Sächsischer Landtag
5. Wahlperiode

DRUCKSACHE 5/7448

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

15. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2009 bis 31. März 2011

Dem Sächsischen Landtag

vorgelegt zum 31. März 2011

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 16. Dezember 2011*

Ausgegeben am: 16. Dezember 2011*

* in der Fassung geändert mit Austauschblatt vom 27. Januar 2012 zu Seite 140

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

Besucheranschrift: Devrientstraße 1
01067 Dresden

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.

AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Art. 3 des Gesetzes vom 1. November 2011 (BGBl. I S. 2131)
AsylbLG	Asylbewerberleistungsgesetz in der Fassung der Bekanntmachung vom 5. August 1997 (BGBl. I S. 2022), zuletzt geändert durch Art. 2e des Gesetzes vom 24. September 2008 (BGBl. I S. 1856)
ATDG	Gesetz zu dem Übereinkommen vom 1. September 1970 über internationale Beförderungen leicht verderblicher Lebensmittel und über die besonderen Beförderungsmittel, die für diese Beförderungen zu verwenden sind (ATP) vom 26. April 1974 (BGBl. 1974 II S. 565)
AZRG	Ausländerzentralregister-Gesetz vom 2. September 1994 (BGBl. I S. 2265), zuletzt geändert durch Art. 4 Abs. 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437)
BABauRaumOG	Gesetz über die Errichtung eines Bundesamtes für Bauwesen und Raumordnung (Art. 1 des Gesetzes über die Errichtung eines Bundesamtes für Bauwesen und Raumordnung sowie zur Änderung besoldungsrechtlicher Vorschriften) vom 15. Dezember 1997 (BGBl. I S. 2902), zuletzt geändert durch Art. 26 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
BaföG	Bundesausbildungsförderungsgesetz in der Fassung der Bekanntmachung vom 7. Dezember 2010 (BGBl. I S. 1952)
BauGB	Baugesetzbuch in der Fassung der Bekanntmachung vom 23. September 2004 (BGBl. I S. 2414), zuletzt geändert durch Art. 1 des Gesetzes vom 22. Juli 2011 (BGBl. I S. 1509)
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen in der Fassung der Bekanntmachung vom 31. Mai 2000 (BayGVBl. S. 414, ber. S. 632, BayRS 2230-1-1-UK), zuletzt geändert durch Gesetz vom 20. Juli 2011 (BayGVBl. S. 313)

BBG	Bundesbeamtengesetz vom 5. Februar 2009 (BGBl. I S. 160), zuletzt geändert durch Art. 13 des Gesetzes vom 28. April 2011 (BGBl. I S. 687)
BBiG	Berufsbildungsgesetz vom 23. März 2005 (BGBl. I S. 931), zuletzt geändert durch Art. 15 Abs. 90 des Gesetzes vom 5. Februar 2009 (BGBl. I S. 160)
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. 16 des Gesetzes vom 1. November 2011 (BGBl. I S. 2131)
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. 1 des Gesetzes vom 27. Juli 2011 (BGBl. I S. 1600)
BOKraft	Verordnung über den Betrieb von Kraftfahrunternehmen im Personenverkehr vom 21. Juni 1975 (BGBl. I S. 1573), zuletzt geändert durch Art. 2 der Verordnung vom 8. November 2007 (BGBl. I S. 2569)
BSO	Verordnung des SMK über die Berufsschule im Freistaat Sachsen (Schulordnung Berufsschule) vom 21. August 2006 (GVBl. S. 446), zuletzt geändert durch Art. 2 der VO vom 27. April 2011 (GVBl. S. 120, 145)
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)
BVerfGG	Bundesverfassungsgerichtsgesetz in der Fassung der Bekanntmachung vom 11. August 1993 (BGBl. I S. 1473), zuletzt geändert durch Art. 11 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2248)

BZRG	Bundeszentralregistergesetz in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 BGBl. I S. 195), zuletzt geändert durch Art. 5 des Gesetzes vom 23. Mai 2011 (BGBl. I S. 898)
DEÜV	Datenerfassungs- und -übermittlungsverordnung in der Fassung der Bekanntmachung vom 23. Januar 2006 (BGBl. I S. 152), zuletzt geändert durch Art. 11 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2309)
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 300-1, bereinigten Fassung, zuletzt geändert durch Art. 21 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586)
FeV	Fahrerlaubnis-Verordnung vom 13. Dezember 2010 (BGBl. I S. 1980), zuletzt geändert durch Art. 1 der Verordnung vom 7. Januar 2011 (BGBl. I S. 3)
GewO	Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), zuletzt geändert durch Art. 1 des Gesetzes vom 11. Juli 2011 (BGBl. I S. 1341)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, zuletzt geändert durch Art. 1 des Gesetzes vom 21. Juli 2010 (BGBl. I S. 944)
GKG	Gerichtskostengesetz vom 5. Mai 2004 (BGBl. I S. 718), zuletzt geändert durch Art. 8 des Gesetzes vom 23. Mai 2011 (BGBl. I S. 898)
GVG	Gerichtsverfassungsgesetz in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), zuletzt geändert durch Art. 3 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2300)
HWO	Handwerksordnung in der Fassung der Bekanntmachung vom 24. September 1998 (BGBl. I S. 3074; 2006 I S. 2095), zuletzt geändert durch Art. 3 des Gesetzes vom 11. Juli 2011 (BGBl. I S. 1341)
IHKG	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern in der im Bundesgesetzblatt Teil III, Gliederungsnummer 701-1, bereinigten Fassung, zuletzt geändert durch Art. 2 des Gesetzes vom 11. Juli 2011 (BGBl. I S. 1341)
KomBekVO	Kommunalbekanntmachungsverordnung vom 19. Dezember 1997 (GVBl. 1998 S. 19)

KOVVfG	Gesetz über das Verwaltungsverfahren der Kriegsopferversorgung in der Fassung der Bekanntmachung vom 6. Mai 1976 (BGBl. I S. 1169), zuletzt geändert durch Art. 20 Abs. 3 des Gesetzes vom 13. Dezember 2007 (BGBl. I S. 2904)
KWG	Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 2 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1126)
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie - Kunsturheberrechtsgesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, bereinigten Fassung (BGBl. I S. 266), zuletzt geändert durch Art. 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266)
LJHG	Landesjugendhilfegesetz vom 4. März 1992 (GVBl. S. 61), zuletzt geändert durch Gesetz vom 11. Juni 2010 (GVBl. S. 182, 184)
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)
OWiZuVO	Verordnung der Sächsischen Staatsregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeiten-Zuständigkeitsverordnung) vom 16. Juli 2008 (GVBl. S. 481), zuletzt geändert durch Art. 2 der Verordnung vom 20. Oktober 2010 (GVBl. S. 299)
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) vom 18. Juni 2009 (BGBl. I S. 1346)
RÄStV	Rundfunkänderungsstaatsvertrag; Fünfzehnter Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge vom 15. Dezember 2010 (LT-Drs. 5/5570)
	danach
RBeitrStV	Rundfunkbeitragsstaatsvertragsentwurf (LT-Drs. 5/7465 zur LT-Drs. 5/5570) vom 17. November 2011
RGebStV	Rundfunkgebührenstaatsvertrag vom 31. August 1991 (GVBl. S. 426) zuletzt geändert durch Art. 6 des Staatsvertrags vom 18. Dezember 2008 (GVBl. 2009 S. 131, 138)
RStV	Rundfunkstaatsvertrag vom 31. August 1991 (GVBl. S. 426), zuletzt geändert durch Art. 1 des Staatsvertrags vom 20. November 2009 (GVBl. 2010 S. 88)

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)
SächsABG	Erstes Gesetz zur Abfallwirtschaft und zum Bodenschutz im Freistaat Sachsen vom 12. August 1991 (GVBl. S. 306), zuletzt geändert durch Art. 16 des Gesetzes vom 15. Dezember 2010 (GVBl. S. 387, 398)
SächsAGSGB	Sächsisches Gesetz zur Ausführung des Sozialgesetzbuches vom 6. Juni 2002 (GVBl. S. 168), zuletzt geändert durch Art. 1 des Gesetzes vom 15. Dezember 2010 (GVBl. S. 387, 388)
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 Art. 1 des Gesetzes vom 19. Juni 2009 (GVBl. S. 382)
SächsBG	Beamtengesetz für den Freistaat Sachsen (Sächsisches Beamtengesetz) vom 17. Dezember 1992 (GVBl. S. 615), zuletzt geändert durch Art. 1 des Gesetzes vom 4. Oktober 2011 (GVBl. S. 380)
SächsDolmG	Sächsisches Gesetz über die staatliche Prüfung, öffentliche Bestellung und allgemeine Beeidigung von Dolmetschern, Übersetzern und Gebärdensprachdolmetschern (Sächsisches Dolmetschergesetz) vom 25. Februar 2008 (GVBl. S. 242), zuletzt geändert durch Art. 2 Abs. 15 des Gesetzes vom 19. Mai 2010 (GVBl. S. 142, 144)
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), geändert durch Art. 6 des Gesetzes vom 8. Dezember 2008 (GVBl. S. 940, 941), zuletzt geändert durch Gesetz vom 14. Juli 2011 (GVBl. S. 270)
SächsEAG	Gesetz über den einheitlichen Ansprechpartner im Freistaat Sachsen vom 13. August 2009 (GVBl. S. 446) zuletzt geändert durch Art. 2 Abs. 7 des Gesetzes vom 19. Mai 2010 (GVBl. S. 142, 143)

SächsGDIG	Gesetz über die Geodateninfrastruktur (Sächsisches Geodateninfrastrukturgesetz) vom 19. Mai 2010 (GVBl. S. 134)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 301), zuletzt geändert durch Art. 2 des Gesetzes vom 26. Juni 2009 (GVBl. S. 323, 325)
SächsHSG	Sächsisches Hochschulgesetz vom 11. Juni 1999 (GVBl. S. 294), zuletzt geändert durch Art. 5 des Gesetzes vom 4. Oktober 2011 (GVBl. S. 380, 391)
SächsJG	Gesetz über die Justiz im Freistaat Sachsen (Sächsisches Justizgesetz) vom 24. November 2000 (GVBl. S. 482, ber. 2001 S. 704), zuletzt geändert durch Gesetz vom 4. März 2011 (GVBl. S. 54)
SächsKAG	Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502), zuletzt geändert durch Art. 2 Abs. 14 des Gesetzes vom 19. Mai 2010 (GVBl. S. 142, 144)
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 11. Juni 2010 (GVBl. S. 182, 184)
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)
SächsÖbVVO	Sächsische Verordnung über Öffentlich bestellte Vermessungsingenieure im Freistaat Sachsen vom 3. März 2009 (GVBl. S. 119)
SächsPBefZuVO	Sächsische Personenbeförderungszuständigkeitsverordnung vom 27. Juni 2008 (GVBl. S. 415)
SächsPersVG	Sächsisches Personalvertretungsgesetz vom 21. Januar 1993 (GVBl. S. 29), zuletzt geändert durch Viertes Gesetz zur Änderung des Gesetzes vom 4. November 2010 (GVBl. S. 290)
SächsPolG	Polizeigesetz des Freistaates Sachsen, Bekanntmachung vom 13. August 1999 (GVBl. S. 466), zuletzt geändert durch Art. 1 des Gesetzes vom 4. Oktober 2011 (GVBl. S. 370)
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)
SächsUIG	Umweltinformationsgesetz für den Freistaat Sachsen (Sächsisches Umweltinformationsgesetz) vom 1. Juni 2006 (GVBl. S. 146)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVermGeoG	Sächsisches Vermessungs- und Geobasisinformationsgesetz vom 29. Januar 2008 (GVBl. S. 138, 148), *gültig bis 4. Juni 2011 (danach SächsVermKatG)*
SächsVermKatG	Gesetz über das amtliche Vermessungswesen und das Liegenschaftskataster im Freistaat Sachsen vom 19. Mai 2011 (GVBl. S. 134)
SächsVerwOrgG	Sächsisches Verwaltungsorganisationsgesetz vom 25. November 2003 (GVBl. S. 899), zuletzt geändert durch Art. 28 des Gesetzes vom 15. Dezember 2010 (GVBl. S. 387, 402)
SächsVwVfZG	Gesetz zur Regelung des Verwaltungsverfahrens- und des Verwaltungszustellungsrechts für den Freistaat Sachsen vom 19. Mai 2010 (GVBl. S. 142)
SächsVwZG	Verwaltungszustellungsgesetz für den Freistaat Sachsen vom 21. April 1993 (GVBl. S 362 ber. in GVBl. 1995 S. 182), zuletzt geändert durch Gesetz vom 10. September 2003 (GBVl. S. 620, ber. in GVBl. S. 913), *gültig bis 4. Juni 2011 (danach SächsVwVfZG)*
SächsWG	Sächsisches Wassergesetz vom 23. Februar 1993 (GVBl. S. 201), zuletzt geändert durch Art. 1 des Gesetzes vom 23. September 2010 (GVBl. S. 270)
SBO	Verordnung des SMK über den Besuch öffentlicher Schulen (Schulbesuchsordnung) vom 12. August 1994 (GVBl. S. 1565), zuletzt geändert durch Verordnung vom 4. Februar 2004 (GVBl. S. 66)
SchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Art. 2 Abs. 10 des Gesetzes vom 19. Mai 2010 (GVBl. S. 142, 144)

SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - (Art. 1 des Gesetzes vom 11. Dezember 1975, BGBl I S. 3015), zuletzt geändert durch Art. 12 Abs. 2a des Gesetzes vom 24. März 2011 (BGBl. I S. 453)
SGB II	Zweites Buch Sozialgesetzbuch - Grundsicherung für Arbeitsuchende - (Art. 1 des Gesetzes vom 24. Dezember 2003, BGBl. I S. 2954), in der Fassung der Bekanntmachung vom 13. Mai 2011 (BGBl. I S. 850 (2094)), zuletzt geändert durch Art. 3a des Gesetzes vom 20. Juni 2011 (BGBl. I S. 1114)
SGB III	Drittes Buch Sozialgesetzbuch - Arbeitsförderung - (Art. 1 des Gesetzes vom 24. März 1997, BGBl. I S. 594), zuletzt geändert durch Art. 2 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1202)
SGB IV	Viertes Buch Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - (Art. 1 des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845), in der Fassung der Bekanntmachung vom 12. November 2009 (BGBl. I S. 3710, 3973; 2011 I S. 363), zuletzt geändert durch Art. 3 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1202)
SGB V	Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung (Art. 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477), zuletzt geändert durch Art. 3 des Gesetzes vom 28. Juli 2011 (BGBl. I S. 1622)
SGB VI	Sechstes Buch Sozialgesetzbuch - Gesetzliche Rentenversicherung - (Art. 1 des Gesetzes vom 18. Dezember 1989, BGBl. I S. 2261, 1990 BGBl. I S. 1337), zuletzt geändert durch Art. 5 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1202)
SGB VII	Siebtes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung - (Art. 1 des Gesetzes vom 7. August 1996, BGBl. I S. 1254), zuletzt geändert durch Art. 6 des Gesetzes vom 22. Juni 2011 (BGBl. I S. 1202)
SGB VIII	Achtes Buch Sozialgesetzbuch - Kinder und Jugendhilfe - (Art. 1 des Gesetzes vom 26. Juni 1990, BGBl. I S. 1163), zuletzt geändert durch Art. 2 des Gesetzes vom 29. Juni 2011 (BGBl. I S. 1306)
SGB IX	Neuntes Buch Sozialgesetzbuch - Rehabilitation und Teilhabe behinderter Menschen - (Art. 1 des Gesetzes vom 19. Juni 2001, BGBl. I S. 1046), zuletzt geändert durch Art. 6 Abs. 8 des Gesetzes vom 20. Juni 2011 (BGBl. I S. 1114)

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. 13 des Gesetzes vom 23. Mai 2011 (BGBl. I S. 898)
SGB XI	Elftes Buch Sozialgesetzbuch - Soziale Pflegeversicherung - (Art. 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014), zuletzt geändert durch Art. 6 des Gesetzes vom 28. Juli 2011 (BGBl. I S. 1622)
SGB XII	Zwölftes Buch Sozialgesetzbuch - Sozialhilfe - (Art. 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022), zuletzt geändert durch Art. 3b des Gesetzes vom 20. Juni 2011 (BGBl. I S. 1114)
SigG	Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 1 des Gesetzes vom 1. November 2011 (BGBl. I S. 2130)
StipG	Stipendienprogramm-Gesetz vom 21. Juli 2010 (BGBl. I S. 957), zuletzt geändert durch Art. 1 des Gesetzes vom 21. Dezember 2010 (BGBl. I S. 2204)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 5 des Gesetzes vom 23. Juni 2011 (BGBl. I S. 1266)
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. 2 des Gesetzes vom 12. Juli 2011 (BGBl. I S. 1378)
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)
StVZO	Straßenverkehrs-Zulassungs-Ordnung vom 28. September 1988 (BGBl. I S. 1793), zuletzt geändert durch Art. 3 der Verordnung vom 21. April 2009 (BGBl. I S. 872)

TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 3 des Gesetzes vom 24. März 2011 (BGBl. I S. 506)
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692)
VersammlG	Versammlungsgesetz in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), zuletzt geändert durch Art. 2 des Gesetzes vom 8. Dezember 2008 (BGBl. I S. 2366)
VwGO	Verwaltungsgerichtsordnung in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), zuletzt geändert durch Art. 9 des Gesetzes vom 22. Dezember 2010 (BGBl. I S. 2248)
VwVDolmetscher	Verwaltungsvorschrift des SMJus zum Sächsischen Dolmetschergesetz vom 29. August 2008 (SächsJMBl. S. 382)
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)
WoGG	Wohngeldgesetz in der Fassung der Bekanntmachung vom 7. Juli 2005 (BGBl. I S. 2029 (2792)), zuletzt geändert durch Art. 12 Abs. 2 des Gesetzes vom 24. März 2011 (BGBl. I S. 453)
ZensG 2011	Zensusgesetz 2011 vom 8. Juli 2009 (BGBl. I S. 1781)
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. 1 des Gesetzes vom 21. Oktober 2011 (BGBl. I S. 2082)

Sonstiges

a. a. O.	am angegebenen Ort
AOK	Allgemeine Ortskrankenkasse
ArbG	Arbeitsgericht
ARGE	Arbeitsgemeinschaft nach SGB II
BBSR	Bundesinstitut für Bau-, Stadt- und Raumforschung

BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BFH	Bundesfinanzhof
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMAS	Bundesministerium für Arbeit und Soziales
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministerium des Innern
BMVBS	Bundesministerium für Verkehr, Bau und Stadtentwicklung
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragter 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
CTI	Computer Telephony Integration

De-Mail	Postfach- und Versanddienst, ist der zentrale Dienst für die zuverlässige und vertrauliche Kommunikation
DNN	Dresdner Neueste Nachrichten (Tageszeitung)
DöV	Die öffentliche Verwaltung, Zeitschrift für öffentliches Recht und Verwaltungswissenschaft
DSK	Datenschutzkonferenz (halbjährlich stattfindende Konferenz der Datenschutzbeauftragten des Bundes und der Länder)
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
EDPS	Europäischer Datenschutzbeauftragter
eGK	Elektronische Gesundheitskarte
ELENA	elektronischer Einkommensnachweis
EPA	Elektronische Patientenakte
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUROJUST	Europäische Einheit für justizielle Zusammenarbeit
EUROPOL	Europäische Polizeibehörde
e. V.	Eingetragener Verein
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
gGmbH	Die gemeinnützige GmbH ist eine Gesellschaft mit beschränkter Haftung, der besondere Steuervergünstigungen gewährt werden. Sie ist keine eigene Gesellschaftsform und unterliegt den Vorschriften des GmbH-Gesetzes
GKI	Gemeinsame Kontrollinstanz Schengen (unabhängiges Gremium, dessen Mitglieder den nationalen Datenschutzbehörden angehören)
GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System

GVBl.	Sächsisches Gesetz- und Verordnungsblatt
HS	Halbsatz
IHK	Industrie- und Handelskammer
IKK	Innungskrankenkasse
IMI	Internal Market Information System, Binnenmarkt-Informationssystem; Die Europäische Kommission hat das IMI für eine sichere Online-Anwendung, die es nationalen, regionalen und lokalen Behörden ermöglicht, schnell und einfach mit Verwaltungen im Ausland zu kommunizieren, entwickelt. Das IMI ist über das Internet zugänglich und erfordert keine zusätzliche Software.
INPOL	Polizeiliches Informationssystem des Bundes u. der Länder
IP-Adresse	Adresse in Computernetzen, wird Geräten zugewiesen, welche an das Netz angebunden sind und macht die Geräte so adressierbar und damit erreichbar. Die IP-Adresse kann einen Empfänger oder eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast). Einem Computer können auch mehrere IP-Adressen zugeordnet sein.
IVO	Integriertes Vorgangsbearbeitungssystem der Sächsischen Polizei
JVA	Justizvollzugsanstalt
JZ	Juristen-Zeitschrift
KBV-Richtlinie	Qualitätssicherungs-Richtlinien der Kassenärztlichen Bundesvereinigung
KKM	Kommunales Kernmelderegister
KV	Krankenversicherung
KV-SafeNet	Anbindungsmöglichkeit an das sichere Netz der Kassenärztlichen Vereinigungen
LfD	Landesbeauftragte(r) für den Datenschutz
LG	Landgericht
LKA	Landeskriminalamt Sachsen
LT-Drs.	Landtags-Drucksache

LPK	Lehr- und Praxis-Kommentar
LRA	Landratsamt
LSG	Landessozialgericht
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MMR	Multimedia und Recht
m. V. a.	mit Verweis auf
m. w. N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZS	Neue Zeitschrift für Sozialrecht
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen
RDV	Zeitschrift Recht der Datenverarbeitung
rSp/lSp	rechte Spalte/linke Spalte
SAKD	Sächsische Anstalt für Kommunale Datenverarbeitung
SächsABl.	Sächsisches Amtsblatt
SächsJMBl.	Sächsisches Justizministerialblatt
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
sc.	sinngemäß: das heißt
SDÜ	Schengener Durchführungsübereinkommen

SG	Sozialgericht
SIS	Schengener Informationssystem
SK	Sächsische Staatskanzlei
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz und für Europa
SMK	Sächsisches Staatsministerium für Kultus und Sport
SMS	Sächsisches Staatsministerium für Soziales und Verbraucherschutz
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft
SMWA	Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SRH	Sächsischer Rechnungshof
SSG	Sächsischer Städte- und Gemeindetag
SVN	Sächsisches Verwaltungsnetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TU	Technische Universität
TV-L	Tarifvertrag für den öffentlichen Dienst der Länder
TVöD	Tarifvertrag für den öffentlichen Dienst
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VwRR	Verwaltungsrechtsreport
VwV	Verwaltungsvorschrift
VwV TK	Verwaltungsvorschrift Telekommunikation
WLAN	Wireless Local Area Network; drahtloses lokales Netzwerk

ZBR	Zeitschrift für Beamtenrecht
ZEVIS	Zentrale Verkehrs-Informationssystem
ZfSH/SGB	Zeitschrift für die sozialrechtliche Praxis

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 Einleitung

Die Verarbeitung von personenbezogenen Informationen ist notwendiger Bestandteil jeglichen staatlichen Gemeinwesens. Dass dies schon in alter Vorzeit so war, wird anschaulich in der Weihnachtsgeschichte des Neuen Testamentes belegt. Der Anlass der Wanderung von Josef und Maria ist die Schätzung des Augustus (Lk 2, 1-3). Der oft verwendete Begriff der Volkszählung ist hier falsch. Es ging nicht um die anonyme Zählung, sondern um die Schaffung eines aktuellen Registers. Jeder Einwohner des Reiches sollte in den Steuerlisten aufgeschrieben (so das griechische Wort απογραφω, das Luther mit „schätzen“ übersetzt) werden. Selbst wenn man die Historizität der Wanderung nach Bethlehem in Frage stellt, ist doch bemerkenswert, wie sich dieses Ereignis in die Erinnerung der Zeitgenossen eingegraben hat. Sowohl der Evangelist als auch seine Zuhörer können etwas mit diesen knappen Worten anfangen. Ohne die Erfassung seiner Bürger war ein Staatsapparat wie der des Römischen Reiches nicht arbeitsfähig, konnten keine Steuern eingetrieben werden, um die öffentliche Infrastruktur zu erhalten, konnten keine Bürger zu Arbeitsleistungen oder zum Militärdienst herangezogen werden, um das Reich vor Feinden zu schützen und Handel und Sicherheit zu gewährleisten.

Allerdings zeigt die Weihnachtsgeschichte eines anderen Evangelisten (Mt 2) auch den Missbrauch staatlicher Macht und der damit verbundenen Informationsverarbeitung. Herodes erfährt durch die Weisen aus dem Morgenland von der Geburt eines Konkurrenten und versucht mit der vorgetäuschten Absicht, diesen auch anzubeten, Informationen zu erlangen. Als das nicht gelingt, lässt er alle Jungen im entsprechenden Alter aus der Gegend von Bethlehem töten, um den Konkurrenten auszuschalten. Diese erste Rasterfahndung wäre nicht möglich gewesen, wenn es keine staatliche Erfassung der Einwohner von Geburt an gegeben hätte. Dass diese auch dem Machterhalt von Autokraten diente, macht die Geschichte drastisch deutlich.

Wenn wir heute über Datenschutz reden, haben wir eine lange Geschichte des Kampfes um Menschenrechte und für eine Form des Gemeinwesens, die diese sichert, hinter uns. Die Demokratie versucht durch ihren institutionellen Aufbau und durch ihren verbrieften Rechtskodex, auf der einen Seite die notwendige Machtausübung und die damit verbundene Verarbeitung von Informationen über ihre Bürger zu sichern, auf der anderen Seite diese auf das notwendige Maß zu begrenzen und Missbrauch zu verhindern. Der Datenschutzbeauftragte und seine Mitarbeiter haben seit neuerer Zeit in diesem System ihren Platz und ihre Aufgabe. Sie kontrollieren und beraten, ob und wie öffentliche Stellen das Recht auf informationelle Selbstbestimmung einhalten bzw. einhalten

können. Auch achten sie mittlerweile darauf, dass gleiche Prinzipien in der Privatwirtschaft gelten. Dies ist nicht immer eine von vornherein klare Sache. Oft tasten sich alle Beteiligten an eine Lösung heran, sind Kompromisse zu finden und Auseinandersetzungen zu führen. Das ist meist langwierig und zäh, manchmal unbefriedigend oder auch störend. Aber das ist Demokratie.

Dieser aktuelle Bericht macht die Bandbreite der Arbeit der Behörde des Sächsischen Datenschutzbeauftragten deutlich. Es geht nicht nur um die im medialen Fokus stehenden Angelegenheiten, sondern um den alltäglichen Gang der Verwaltung und der Wirtschaft. Auch wenn es pathetisch klingt, in allen diesen Feldern hat Demokratie sich zu bewähren. Ich hoffe, der Sächsische Datenschutzbeauftragte trägt seinen Teil dazu bei.

1.2 Behördliche Datenschutzbeauftragte

Wie in 14/15. mitgeteilt, habe ich ein internes Forum unter http://circa.sachsen.de eingerichtet. Der Staatsbetrieb Sächsische Informatik Dienste (SID) als Betreiber des CIRCA-Servers bittet in diesem Zusammenhang darum, dass alle neuen Nutzer bei der Anmeldung folgende Daten mitteilen: Vorname, Nachname, Organisation, E-Mail-Adresse, Telefonnummer, postalische Adresse sowie die Angabe, dass eine Aufnahme in den „AK Behördlicher Datenschutzbeauftragter“ erfolgen soll.

1.3 Verfahrensverzeichnisse

Der Sächsische Datenschutzbeauftragte beabsichtigt, künftig Verfahrensverzeichnisse bürgerfreundlich im Internet zu veröffentlichen. Diese Möglichkeit ergibt sich aus der Begründung des Änderungsantrages der Fraktionen CDU und SPD zum Sächsischen Datenschutzgesetz (LT-Drs. 4/7133). Dies dient der Herstellung von Transparenz über die Datenverarbeitung im öffentlichen Bereich. Neben einer persönlichen Möglichkeit zur Einsichtnahme wird diese heute am besten durch Internet-Veröffentlichungen realisiert. Dies setzt jedoch voraus, dass die Verfahrensverzeichnisse künftig elektronisch übermittelt werden. Hierfür werden geeignete Formulare bereitgestellt werden.

Die Veröffentlichung durch den Sächsischen Datenschutzbeauftragten erfolgt nur im Fall der Nicht-Bestellung eines behördlichen Datenschutzbeauftragten. Aber auch bei der Bestellung eines behördlichen Datenschutzbeauftragten wird der Sächsische Datenschutzbeauftragte den Daten verarbeitenden Stellen ermöglichen, die entsprechende Software für eine Veröffentlichung in ihrem Internetangebot zu nutzen.

2 Parlament

In diesem Berichtszeitraum nicht belegt.

3 Europäische Union / Europäische Gemeinschaft

3.1 EU-Dienstleistungsrichtlinie

Bereits in meinem letzten Tätigkeitsbericht hatte ich über die Umsetzung der EU-Dienstleistungsrichtlinie (RL 2006/123/EG - ABl. L 376, S. 36 vom 27. Dezember 2006) berichtet. Das zuständige Staatsministerium habe ich in datenschutzrechtlichen Fragen beraten und zur Sicherstellung der datenschutzkonformen Umsetzung erforderliche gesetzliche Regelungen gefordert.

Im neuen Berichtszeitraum hat der Sächsische Landtag zur Umsetzung der Vorgaben der Richtlinie im Freistaat Sachsen am 24. Juni 2009 das „Gesetz über den einheitlichen Ansprechpartner im Freistaat Sachsen“ beschlossen, einer Stelle, die Anfragen an Behörden bündeln soll.

Den datenschutzrechtlichen Anforderungen wurde bei der Umsetzung der EU-Dienstleistungsrichtlinie m. E. seitens des Verordnungsgebers bislang jedoch nicht ausreichend Rechnung getragen.

§ 4 SächsEAG ermächtigt das SMWA, durch Rechtsverordnung zu bestimmen, unter welchen Voraussetzungen, in welchem Umfang und mit welcher Dauer personenbezogene Daten durch den einheitlichen Ansprechpartner aufgabenbezogen verarbeitet werden dürfen. Bereits im Gesetzgebungsverfahren zum Gesetz über den einheitlichen Ansprechpartner wurde die Notwendigkeit des Erlasses der Rechtsverordnung meinerseits in Ausschusssitzungen betont. Weder aus dem Gesetz über den einheitlichen Ansprechpartner noch aus §§ 71a bis 71e VwVfG ergibt sich, in welchem Umfang, in welcher Tiefe und in welchem Ausmaß personenbezogene Daten durch den einheitlichen Ansprechpartner verarbeitet werden können sollen. Die formellen Gesetze allein regeln daher nicht hinreichend und abschätzbar die Datenverarbeitung. Unabhängig von diesem Punkt stellt der einheitliche Ansprechpartner eine Behörde mit einer neuartigen Verwaltungsaufgabe dar. Auch aus diesem Grund ist die Schaffung einer Rechtsverordnung zur Regelung der Datenverarbeitung im Rahmen der gesetzlichen Aufgaben des einheitlichen Ansprechpartners notwendig.

Dies und meine Auffassung sind dem SMWA auch bekannt. Seit dem Inkrafttreten des Gesetzes über den einheitlichen Ansprechpartner vertritt das Staatsministerium die Auffassung, dass das Sächsische Datenschutzgesetz ausreichend sei, soweit der einheitliche

Ansprechpartner in seinem gesetzlich zugewiesenen Aufgabenfeld tätig würde und eine Rechtsverordnung nur notwendig sei, wenn diese über klarstellende Regelungen hinaus gehe.

Ich teilte dem SMWA mit, dass ich diese Rechtsauffassung nicht teile. Vielmehr erhoffe ich mir weiterhin eine Rechtsverordnung in der normenklare Datenverarbeitungsbefugnisse und -regeln festgelegt werden. Regelungs- und Klarstellungsbedarf sehe ich im Hinblick auf

- die Erhebung der für die Aufgabenerfüllung des einheitlichen Ansprechpartners unbedingt erforderlichen Daten (abschließende Festlegung),
- die Erforderlichkeit der Kenntnisnahme von Einzeldaten und für die Speicherung von Daten,
- die Datenübermittlungen zwischen dem einheitlichen Ansprechpartner und den zuständigen Behörden,
- die Zweckbindung (einschließlich des grundsätzlichen Verbots personenbezogene Daten aus verschiedenen Verfahren abzugleichen),
- die Verarbeitung sensibler Daten,
- die Löschung und Archivierung (einschließlich Fristen, Zuständigkeiten).

Demgegenüber beharrte das SMWA auf seiner Ansicht, dass das Sächsische Datenschutzgesetz für die öffentlichen Stellen des Freistaates Sachsen die Zulässigkeitsvoraussetzungen für die Datenverarbeitung ausreichend regeln würde. Zudem würden bereichsspezifische Vorschriften im jeweiligen Fachrecht ebenfalls einzuhalten sein.

Ich vertrete eine andere Auffassung. Den Gesetz- bzw. Verordnungsgeber trifft m. E. eine Pflicht, ein breit gefächertes, an genau umschriebenen Verarbeitungszusammenhängen orientiertes Regelungssystem aufzubauen (Simitis in: Simitis, BDSG, Einleitung Rdnr. 48). Nicht ausreichend ist dabei, wenn eine bestimmte Aufgabe beschrieben wird, deren Erfüllung die Kenntnis bestimmter Informationen voraussetzt, ohne dass die Verarbeitung personenbezogener Daten näher geregelt wird. Die Rechtsvorschrift muss vielmehr eine eindeutige Befugnis zur Datenverarbeitung enthalten und zumindest die Art der Daten und den Zweck der Verarbeitung regeln (vgl. dazu Gola/Schomerus, BDSG, § 4 Rdnr. 8).

Im Falle der Datenverarbeitung durch den einheitlichen Ansprechpartner sind wegen der Eingriffsintensität der zur Aufgabenerfüllung notwendigen Datenverarbeitung bereichsspezifische Regelungen erforderlich. So sollen auch Gesundheitsdaten erfasst und übermittelt werden. Ein Rückgriff auf die allgemeinen Regelungen des Sächsischen Datenschutzgesetzes nach den §§ 12 ff. ist bei besonders schutzwürdigen Daten wie

Gesundheitsdaten nicht ohne weiteres - von Einwilligungen abgesehen - zulässig (vgl. dazu Walz in: Simitis, BDSG, § 4 Rdnr. 15). Lediglich bereichsspezifische Rechtsvorschriften erlauben aufgrund ihrer speziellen Regelungsgegenstände Voraussetzungen und Umfang der Verarbeitung personenbezogener Daten klar und für den Bürger erkennbar zu bestimmen (vgl. BVerfGE 65,1).

Vor dem Hintergrund, dass dem einheitlichen Ansprechpartner als neu gebildeter Behörde zur Erfüllung einer neuen Aufgabe eine Vielzahl von personenbezogenen Daten aus unterschiedlichsten Verwaltungsverfahren anvertraut werden, bleibt meine Forderung nach dem Erlass einer Rechtsverordnung, welche normenklar die Datenverarbeitungsbefugnisse und -regeln für diese Stelle mit all ihren Besonderheiten festlegt, bestehen.

Der einheitliche Ansprechpartner im Freistaat Sachsen hat seine Tätigkeit bei der Landesdirektion Leipzig mittlerweile aufgenommen. Die bisherigen Fallzahlen sind noch relativ gering.

3.2 Binnenmarktinformationssystem IMI

In meinem letzten Tätigkeitsbericht hatte ich bereits über das Binnenmarktinformationssystem IMI berichtet. Ich hatte die fehlende Rechtsgrundlage für das Verfahren und den Umstand, dass den nationalen Datenschutzbehörden kein Kontrollrecht im Hinblick auf die Einführung des Verfahrens zugestanden wird, kritisiert, 14/3.2. Bisher ist das Verfahren insbesondere für die Umsetzung der EU-Dienstleistungsrichtlinie vorgesehen, vgl. 3.1.

In Abstimmung mit den Datenschutzbeauftragten des Bundes und der Länder wendete ich mich im letzten Berichtszeitraum an den Europäischen Datenschutzbeauftragten (EDPS) und reklamierte erneut die nicht bestehende Rechtsgrundlage und ein erforderliches Einsichts- und Prüfrecht in die Unterlagen für die Kontrollbehörden und die behördlichen Datenschutzbeauftragten. Behörden und Beauftragte haben, um ihrem gesetzlichen Auftrag nachkommen zu können, u. a. im Rahmen durchzuführender Vorabkontrollen vor dem Einsatz des Verfahrens den Sicherheitsplan von IMI bzw. geeignete Datenschutz- und Datensicherheitskonzepte zu IMI zugrunde zu legen.

Nach dem Ende des Berichtszeitraums wurde ich dahingehend informiert, dass das IMI-Verfahren von EU-Behörden geprüft worden und sicher sei und dass im Übrigen keine weitergehenden Revisionen vorzusehen seien. Auch im Hinblick auf die oben genannten Kontrollmöglichkeiten enthielt die lapidare Belehrung aus Brüssel nichts Neues. Da IMI als Kommunikationsverfahren in Sachsen für andere Verfahren als die der Ausfüh-

rung von EU-Richtlinien in Erwägung gezogen wird, bedeutet dies, dass IMI wegen der nicht ordnungsgemäß durchführbaren Vorabkontrolle für andere Verwaltungsvorgänge - wegen der Unmöglichkeit das Verfahren zu prüfen - zukünftig schlichtweg nicht verwendet werden darf.

Zwischenzeitlich ist mir noch ein Verordnungsentwurf der EU-Kommission zu IMI zugegangen. Wenngleich dieser neue datenschutzrechtliche Fragestellungen aufwirft, wird damit - und das ist positiv - eine gesetzliche Grundlage geschaffen, wie die DSK es gefordert hat.

3.3 Urteil des Europäischen Gerichtshofs zur Veröffentlichung von Empfängern von Agrarbeihilfen im Internet

Das Recht der Europäischen Union wird auch für Sachsen immer wichtiger. Dies betrifft nicht nur die Rechtsetzung durch die Kommission und den Rat, sondern auch die Rechtsprechung des EuGH. Dieser entschied in den vergangenen Jahren immer häufiger zu datenschutzrechtlichen Fällen.

So wurde in einem Fall, der auch viele sächsische Empfänger von Agrarbeihilfen betrifft und in dem sich ein Petent mit einer gleichgelagerten Problematik an mich gewandt hatte, entschieden, dass u. a. eine nicht nach Zeiträumen, Häufigkeit sowie Art und Umfang von Subventionen differenzierte Veröffentlichung natürlicher Personen im Internet als Subventionsempfänger gegen den Grundsatz der Verhältnismäßigkeit verstößt (EuGH, Urt. v. 9. November 2010 - C-92/09 und C-93/09). Das Gericht urteilte, dass entsprechende Veröffentlichungen die durch Art. 7 der Charta der Grundrechte der Europäischen Union geschützte Achtung des Privat- und Familienlebens sowie das durch Art. 8 der Charta anerkannte Recht auf Datenschutz verletzen (Rdnr. 64) und der Rat und die Kommission beim Erlass der zugrundeliegenden Vorschriften den Grundsatz der Verhältnismäßigkeit verletzt haben, indem sie nicht geprüft haben, ob nicht auch eine eingeschränkte namentliche Veröffentlichung ausreichend gewesen wäre, die Transparenz der Mittelvergabe zu gewährleisten (Rdnr. 83 ff.).

Damit hat das Gericht nicht zuletzt den EU-Gesetzgeber ermahnt, in seiner Gesetzgebung zur Verarbeitung personenbezogener Daten stets den Grundsatz der Verhältnismäßigkeit zu beachten. Auch Subventionsempfänger dürfen nicht nur deshalb, weil sie staatliche Gelder erhalten, undifferenziert im Internet bekannt gemacht werden. Der Gerichtshof hat deutlich gemacht, dass es den „gläsernen Subventionsempfänger“ nicht geben darf. Dies ist eine Erkenntnis, die ich nur begrüßen kann.

3.4 Datenschutz im Schengener Informationssystem

Im Berichtszeitraum erhielt ich eine Anfrage des BfDI bezüglich eines Petenten, dessen Daten im Schengener Informationssystem (SIS) erfasst worden waren. Dabei stellte sich die Frage nach den Gründen für die Speicherung.

Das SIS ist ein automatisiertes Personen- und Sachfahndungssystem innerhalb der EU. Aufgrund der Aufhebung der Grenzkontrollen im Binnenraum der EU wurde mit dem Schengener Übereinkommen das Prinzip der einmaligen Kontrolle bei der Einreise in das Schengen-Gebiet eingeführt. Diese Maßnahme wurde 1995 begleitet durch die Errichtung des Schengener Informationssystem. Am SIS nehmen alle EU-Mitgliedsstaaten außer dem Vereinigten Königreich, Irland und Zypern teil. Ferner sind Island, Norwegen und die Schweiz angeschlossen.

In dem System können unter anderem Daten zu folgenden Personen erfasst werden:

- Personen, die von der Polizei gesucht oder überwacht werden,
- vermisste Personen oder Personen, die in Gewahrsam zu nehmen sind, insbesondere Minderjährige,
- Personen, die nicht die Staatsangehörigkeit einer Schengener Vertragspartei haben und denen die Einreise in das Schengener Hoheitsgebiet zu verweigern ist.

Das SIS ist aus der Sicht des Datenschutzes u. a. problematisch, weil kaum nachzuvollziehen ist, welche beteiligten Stellen was wissen und wie nutzen. Kontrolliert wird das System in jedem einzelnen Staat durch eine nationale Instanz, welche jede Vertragspartei mit der unabhängigen Kontrolle zu beauftragen hat. Dem steht allerdings entgegen, dass der Datenschutz nicht in allen Schengen-Mitgliedsstaaten gleich gut entwickelt ist. Dies führt zu unterschiedlichen Einschätzungen bezüglich des gleichen Sachverhaltes.

Dem Datenschutz des Einzelnen wird zumindest durch ein bestehendes Auskunftsrecht etwas Rechnung getragen. So kann jedermann bei jeder zuständigen nationalen Instanz Auskunft beantragen. Soweit das nationale Recht des Staates, in dem der Auskunftsantrag gestellt wurde, dies vorsieht, können die betreffenden Daten mitgeteilt werden. Unter bestimmten Voraussetzungen kann eine Auskunft auch verweigert werden. Gegebenenfalls besteht ein Recht auf Berichtigung der zur eigenen Person gespeicherten Daten, auf Erhebung einer Klage auf Berichtigung, Löschung, Auskunftserteilung oder Schadensersatz sowie auf Überprüfung der Daten. Für Betroffene in Deutschland besteht die Möglichkeit, sich an das BKA, die nationale Kontrollinstanz, den BfDI oder auch an den jeweiligen Landesbeauftragten für Datenschutz zu wenden.

Auf Nachfrage bei der Behörde, welche die Eintragung veranlasst hatte, erfuhr ich, dass der Petent trotz Abschiebung mehrfach unberechtigt nach Deutschland eingereist war. Auf dieser Grundlage wurde der Petent gemäß Art. 96 Abs. 3 des Schengener Durchführungsübereinkommens (SDÜ) in das SIS aufgenommen. Danach dürfen Drittausländer in das System eingetragen werden, wenn sie zuvor ausgewiesen, zurückgewiesen oder abgeschoben worden sind, wobei die Maßnahme nicht aufgeschoben oder aufgehoben worden sein darf, ein Verbot der Einreise oder des Aufenthalts enthalten oder davon begleitet sein muss und auf der Nichtbeachtung des nationalen Rechts über die Einreise oder den Aufenthalt von Ausländern beruhen muss.

Diese Voraussetzungen waren hier gegeben. Dies habe ich dem BfDI mitgeteilt, welcher dann den Petenten informiert hat.

4 Medien

4.1 Rundfunkbeitragsstaatsvertrag

Ich begrüße grundsätzlich, dass mit dem vorgelegten Rundfunkbeitragsstaatsvertrag die Leistung eines Rundfunkbeitrags nicht mehr von dem problematischen Begriff des „Bereithaltens eines Rundfunkgeräts“ abhängig gemacht wird. Leider wurde dabei die Chance, mit der Neuregelung der Finanzierung des öffentlich-rechtlichen Rundfunks in Deutschland ein datensparsames und unbürokratisches Verfahren einzuführen, nicht wahrgenommen. Bereits seit Jahren fordern die Datenschutzbeauftragten des Bundes und der Länder das Prinzip von Datenvermeidung und Datensparsamkeit in verstärktem Maße zu berücksichtigen.

Der Rundfunkbeitragsstaatsvertrag führt jedoch im Gegenteil nicht zur Verringerung der Datenmengen, sondern nur zur Umschichtung der Datenerhebungen; ein Verzicht auf den Einsatz von den verwaltungsrechtlich als problematisch anzusehenden externen und auf Erfolgsprovisionsbasis agierenden Rundfunkgebührenbeauftragten zur Teilnehmerermittlung ist ebenso wenig erkennbar wie die Aufgabe des derzeit praktizierten Adressankaufs. Mit dem vorgesehenen Staatsvertrag, der unter anderem an den Wohnungsbegriff anknüpft, würde eine, gemessen am Zweck, unmaßstäbliche und riesige Datenbank geschaffen, die insoweit über die Melderegister hinausgeht, indem sie neben der gesamten Wohnungsbelegung von Deutschland unternehmensbezogene Datenbestände aus verschiedenen Registern (z. B. Vereins- und Handelsregistern) enthielte.

Insbesondere möchte ich folgende Punkte hervorheben:

1. In § 11 Abs. 4 RBeitrStV werden die Landesrundfunkanstalten ermächtigt, für die Beitragserhebung notwendige Daten ohne Kenntnis des Betroffenen bei öffentlichen und nicht-öffentlichen Stellen zu erheben. Dies geht noch über § 8 Abs. 4 des zu ersetzenden Rundfunkgebührenstaatsvertrags hinaus.

   Zum einen ermöglicht die letztgenannte Vorschrift gerade keine Datenerhebung bei allen öffentlichen Stellen; sie ist gemäß § 4 Abs. 6 bzw. § 8 Abs. 4 RGebStV vielmehr auf Meldebehörden beschränkt. Soweit behauptet wird, dass unter öffentlichen Stellen auch künftig nur Meldebehörden zu verstehen seien, so stellt sich die Frage nach der Notwendigkeit der Ausweitung der Erhebungsbefugnis auf alle öffentlichen Stellen.

   Zum anderen ist der bisher auf dieser Grundlage praktizierte Einkauf von Adressdaten aus privaten Quellen nach der Umstellung auf eine Wohnungsabgabe (erst recht) nicht mehr erforderlich. Aber auch bei gegenteiliger Auffassung ist es nicht

nachvollziehbar, dass für eine behauptete ausschließlich vorgesehene Erhebung von Adressdaten eine derart weitgehende Erhebungsbefugnis bei allen nicht-öffentlichen Stellen vorgesehen wird, die auch eine Erhebung beispielsweise bei Arbeitgebern und Versicherungen ermöglichen könnte.

Nicht ersichtlich ist schließlich auch, warum die Verpflichtung zur Löschung derart erhobener Daten „bei Feststellung des *Nichtbestehens oder Bestehens* eines Rundfunkteilnehmerverhältnisses“ (so noch § 8 Abs. 4 RGebStV) auf eine Pflicht zur Löschung bei Feststellung, „dass eine Beitragspflicht … *nicht besteht*“ reduziert werden soll.

Im Ergebnis ist zu konstatieren, dass es dem Rundfunkbeitragsstaatsvertrag sogar noch mehr als bereits dem bisherigen Rundfunkgebührenstaatsvertrag an einer Präzisierung der Erhebungsbefugnisse und damit an Normenklarheit mangelt.

2. In § 10 Abs. 7 RBeitrStV ist vorgesehen, dass die Landesrundfunkanstalten ermächtigt sind, einzelne Tätigkeiten bei der Durchführung des Beitragseinzugs und der Ermittlung von Beitragsschuldnern ganz oder teilweise auf Dritte zu übertragen. Nachdem sich hierfür bereits „einer im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebenen Stelle“ (der heutigen GEZ) bedient wird, sollte diese in der Lage sein, auch ohne externe Hilfe die Aufgabe zu erfüllen, die ihre Existenzberechtigung ausmacht. Oder sollen z. B. Inkassodienstleister an dem Beitragseinzug beteiligt werden? Nach dem Wortlaut ist jedenfalls vieles gesetzlich umsetzbar.

3. Nachdem § 8 Abs. 3 RGebStV noch vorsah, dass nur „im Einzelfall“ Rundfunkteilnehmerdaten durch andere Landesrundfunkanstalten abgerufen werden konnten, ist diese Einschränkung ohne ersichtliche Notwendigkeit in § 11 Abs. 3 RBeitrStV entfallen, so dass auch listenweise Teilnehmerdaten von anderen Rundfunkanstalten bezogen und abgeglichen werden könnten.

Begrüßt hätte ich einen wirklichen Systemwechsel, insbesondere wenn man bei der Beitragserhebung an eine schon bestehende Datenverarbeitung angeknüpft hätte. Vereinzelt ist schon der Vorschlag gemacht worden, die Erhebung der Gelder für den öffentlich-rechtlichen Rundfunk im Zuge des Lohn- und Einkommenssteuerverfahrens sicherzustellen. So bleibt der Reformstau erhalten und die in ihrem Grundrecht betroffenen Bürger gucken weiterhin in die Röhre.

5 Inneres

5.1 Personalwesen

5.1.1 Mobiltelefone mit GPS-Funktion

Eine sächsische Kommune bat mich um eine datenschutzrechtliche Bewertung des vorgesehenen Einsatzes von „GPS-Smartphones“ durch Mitarbeiter des städtischen Dienstleistungsunternehmens, um deren Position während des Winterdienstes bestimmen zu können. Dies habe mehrere Vorteile. Zum einen könne die Fahrtroute und -geschwindigkeit belegt werden. Dies schaffe Rechtssicherheit und entspräche den zunehmenden Dokumentationsnotwendigkeiten. Zum anderen ließe sich die Arbeitszeit mit dem Ort der Verrichtung belegen, was einen Nachweis beispielsweise bei Dienstunfällen ermögliche. Schließlich könne auch im Falle eines Unfalles die Position des Mitarbeiters schneller ermittelt und dieser schneller geborgen werden.

Ich wies zunächst darauf hin, dass nach § 77 Nr. 4 SächsPersVG ein Mitwirkungsrecht des Personalrates besteht (vgl. dazu auch Beschluss des ArbG Kaiserslautern vom 27. August 2008 - Az. 1 BVGa 5/08) und regte an, eine entsprechende Dienstvereinbarung abzuschließen.

Eine Nutzung der GPS-Funktion und damit die Standortbestimmung stellt eine Verarbeitung von Beschäftigtendaten dar. Diese war vorliegend gemäß § 37 SächsDSG dann zulässig, soweit dies zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich war.

Für die Erforderlichkeit ist es dabei keinesfalls ausreichend, dass die GPS-Ortung über „Vorteile“ verfügt. Es wäre vielmehr beispielsweise darzulegen, dass eine Dokumentation der Fahrtroute notwendig und anders nicht möglich ist. Alternativ würde ich es mittragen, dass die GPS-Daten auf Grundlage einer schriftlichen Einwilligung der betroffenen Beschäftigten gemäß § 4 Abs. 1 Nr. 2, Abs. 3 SächsDSG verarbeitet werden. Diese hat jedoch freiwillig zu erfolgen. Eine Versagung der Einwilligung hat für die Beschäftigten dabei folgenlos zu bleiben. Nur so kann eine Freiwilligkeit gewährleistet werden. Es ist daher seitens der Dienststellenleitung unbedingt sicherzustellen und am besten in einer Dienstvereinbarung zuzusichern, dass Beschäftigten, die eine derartige Einwilligung verweigern, daraus keine Nachteile entstehen.

5.1.2 Datenschutzgerechter Personalbogen

In 6/5.1.1 berichtete ich über meine Beteiligung beim Entwurf der Verwaltungsvorschrift zur Begründung und Beendigung des Beamtenverhältnisses vom 11. August

1997 (SächsABl. S. 1060) und den in der Anlage enthaltenen Personalbogen (abgedruckt unter 6/16.2.1). Ich regte gegenüber dem SMI an, diesen wegen geänderter Rahmenbedingungen zu überprüfen.

Zum einen ist fraglich, ob die unter Feldnummer 16 zu machenden Angaben zum Wehr- oder Zivildienst erforderlich sind oder eine entsprechende Datenerhebung im Ergebnis nicht vielmehr einen Verstoß gegen die Vorschriften des Allgemeinen Gleichbehandlungsgesetzes zur Folge hätte. Fraglich ist zum anderen auch, ob ein Lichtbild in jedem Fall erforderlich ist. Das SMI sicherte mir zu, diese beiden Punkte bei der notwendigen Aktualisierung der Verwaltungsvorschrift zu prüfen.

Ich wies weiterhin darauf hin, dass das Erheben der Kinderdaten (Feldnummer 11) nur erforderlich und zulässig ist, sofern die Kinder noch im Haushalt des Bewerbers/ Bediensteten leben und soweit sich die Angaben auf Kindergeld und Familienzuschlag auswirken. Zum einen spiegelt sich diese Einschränkung in der entsprechenden Fußnote 4 nur bedingt wider („Angaben nur erforderlich, sofern Unterhaltspflicht besteht“), zum anderen kann das Kindergeld auch in Gänze an den Elternteil ausgezahlt werden, der nicht für eine öffentliche Stelle tätig ist. Es ist ebenfalls zu berücksichtigen, dass bei den Tarifverträgen nach dem TV-L und nach dem TVöD eine entsprechende Gehaltszulage nicht mehr vorgesehen ist.

5.1.3 Erhebung von Führerscheindaten bei Nutzung von Dienst-Kfz

Ich erhalte häufiger Anfragen von Beschäftigten, inwieweit die Erhebung von Führerscheindaten durch den jeweiligen Dienstherrn als Voraussetzung für die Nutzung von Dienst-Kfz datenschutzrechtlich zulässig sei. In einem Fall sollte ein Vordruck der Deutschen Rentenversicherung Mitteldeutschland für die Datenverarbeitung Verwendung finden.

Das entsprechende Formular enthielt Hinweise auf Rechtsvorschriften, die die Angabe personenbezogener Daten der Beschäftigten begründen sollten. Die Angabe der Daten war auch als Voraussetzung für die Nutzung eines Dienst-Kfz dargestellt. Datenschutzrechtlich ist zu beachten, dass sich das Erfordernis des Fahrzeughalters zur Verarbeitung spezieller Personaldaten für die Nutzung von Dienst-Kfz lediglich mittelbar aus § 31 Abs. 2 StVZO ergibt. In der arbeits- und verwaltungsgerichtlichen Rechtsprechung ist die erforderliche Datenverarbeitung aber hergeleitet und herausgearbeitet worden. Nach meiner Prüfung konnte der Dienstherr als Fahrzeughalter nach den angegebenen straßenverkehrsrechtlichen Bestimmungen und auf Grundlage von § 37 SächsDSG die für die Kraftfahrzeugzuteilung erforderlichen Daten der Beschäftigten erheben. Einen Da-

tenschutzverstoß konnte ich nicht feststellen. Das entsprechende Formular konnte auch so Verwendung finden.

Das Verfahren nach § 80 Abs. 3 Nr. 8 SächsPersVG bei Beschäftigten mit vorgesehener ständiger Nutzung eines Dienst-Kfz ist mitbestimmungspflichtig. Zwar schreibt § 80 Abs. 3 SächsPersVG den Abschluss einer Dienstvereinbarung nicht zwingend vor. Wegen der gebotenen Transparenz und Überprüfbarkeit der speziellen Datenverarbeitung und der Erfüllung datenschutzrechtlicher Anforderungen bei der konkreten Ausgestaltung der Personaldatenverarbeitung ist eine entsprechende Dienstvereinbarung jedoch sehr zu empfehlen.

Das Formular zur Führerscheinkontrolle - es handelte sich nicht um eine automatisierte Datenverarbeitung - ist allgemein als personenbezogene Sachakte des betroffenen Beschäftigten zu führen. Soweit aus praktischen Erwägungen eine Aufbewahrung beim Fuhrpark erfolgen soll, ist die Benennung der verantwortlichen Mitarbeiter für die Kontrolle und Aufbewahrung sowie deren Vertreter namentlich oder mit der Funktionsbezeichnung zu regeln. Die Aufbewahrung der Formulare beim Fuhrpark sollte wegen möglicherweise eingetragener Beschränkungen auf dem Führerschein nach § 25 Abs. 3 FeV und den dadurch gegebenenfalls miterhobenen Gesundheitsdaten nach § 37 Abs. 1 i. V. m. § 4 Abs. 2 SächsDSG verschlossen erfolgen, vergleichbar der Verwahrung von Personalakten. Die für die Kontrolle und Aufbewahrung der Formulare verantwortlichen Mitarbeiter des Fuhrparks sollten neben der Verpflichtung auf das Datengeheimnis nach § 6 SächsDSG gesondert über die Vertraulichkeit im Umgang mit Personaldaten belehrt sein.

5.1.4 Betriebliches Eingliederungsmanagement und Datenschutz

Nach § 84 Abs. 2 SGB IX sind die Arbeitgeber zur Durchführung des betrieblichen Eingliederungsmanagements verpflichtet. Die Regelung besteht seit 2004. Immer wieder erhalte ich Nachfragen zum datenschutzgerechten Umgang mit Daten, die im Verfahren des betrieblichen Eingliederungsmanagements erhoben worden sind bzw. wie eine Dienstvereinbarung zum betrieblichen Eingliederungsmanagement aussehen sollte.

Das Verfahren ist anzubieten, sobald ein Beschäftigter innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig ist. Es ist bei sämtlichen Beschäftigten durchzuführen, nicht nur bei schwerbehinderten Bediensteten. Ziel der Maßnahme ist die Wiederherstellung, Erhaltung und Förderung der Arbeitsfähigkeit. Es geht um gesundheitsbezogene Informationen, mithin also auch um besonders schutzwürdige Daten im Sinne von § 4 Abs. 2 SächsDSG.

Am Anfang des Verfahrens steht eine den Beschäftigten betreffende Datenerhebung. Der Dienstherr und Arbeitgeber ist verpflichtet, auf Art und Umfang der im Zusammenhang mit dem betrieblichen Eingliederungsmanagement erhobenen und verwendeten Daten hinzuweisen. Die Betroffenen können hierzu freiwillig ihre Einwilligung abgeben, § 84 Abs. 2 SGB IX. Ohne die Einwilligung kann das Verfahren nicht durchgeführt werden. Bei der Einwilligungserklärung erhält der Beschäftigte die Möglichkeit, zu erklären, dass er mit der Durchführung des betrieblichen Eingliederungsmanagements einverstanden ist. Darüber hinaus ist ihm die Möglichkeit zu geben, auszuwählen, ob er die Beteiligung des Personalrats wünscht oder ablehnt. Optional ist auch die Beteiligung weiterer Beauftragter, wie der Schwerbehindertenvertretung und der Frauenbeauftragten vorstellbar.

Bereits bei der Einwilligung haben Inhalt, Umfang und Ausmaß der Datenverarbeitung festzustehen. Hierzu benötigt die Dienststelle Festlegungen, die am besten in einer Dienstvereinbarung geregelt sein sollten, so dass der betroffene Bedienstete die Entscheidung über die Teilnahme an dem Verfahren auf Grundlage solider Informationen vornehmen kann. Deklaratorisch sollte festgehalten werden, dass die Verwendung der erhobenen Daten datenschutzrechtlich strikt zweckgebunden zu erfolgen, d. h., dass die Datenverarbeitung ausschließlich zum Erhalt und Bestand eines gesundheitsbedingt gefährdeten Arbeitsverhältnisses stattzufinden hat. Die für die Zwecke des Verfahrens erhobenen und gespeicherten Daten dürfen insbesondere nicht ohne Weiteres für sonstige arbeitsvertragsrechtliche Zwecke verwendet werden. Die Nutzung der Daten etwa für ein Kündigungsverfahren wegen der gesundheitlichen Konstitution des Beschäftigten würde eine unzulässige Zweckänderung bedeuten. Damit im Zusammenhang steht, dass datenschutzorganisatorisch die eigentliche Akte zum betrieblichen Eingliederungsmanagement von der Personalakte getrennt bleiben muss. In die Personalakte gehören nur äußere Informationen, also Nachweise für die ordnungsgemäße Durchführung des betrieblichen Eingliederungsmanagements, wie ein Abdruck der Einladung zu einem Gespräch zum betrieblichen Eingliederungsmanagement, die Antwort des Beschäftigten auf diese Einladung bzw. einen Vermerk über die Nichtantwort, ein Vermerk über die Beendigung des Verfahrens oder die Ablehnung des Verfahrens durch den Beschäftigten zu Dokumentationszwecken. Die inhaltlichen Informationen sind in der Dienststelle außerhalb der Personalverwaltung zu erheben und aufzubewahren. Es empfiehlt sich dabei, die für ein betriebliches Eingliederungsmanagement erforderlichen Daten von einer besonderen Organisationseinheit, einer Ad-hoc-Kommission zu erheben, die informationell abgeschottet agiert und Vertraulichkeit gewährleisten kann und muss. Diese kann aus Vertretern des Arbeitgebers und den unterschiedlichen in § 84 Abs. 2 SGB IX genannten Interessenvertretungen bestehen. Von einer Beteiligung von Bediensteten aus dem Bereich der Personalverwaltung wird bereits aus Akzeptanzgründen, aber in erster

Linie wegen der datenschutzorganisatorischen Probleme, das Wissen aus dem Verfahren gegenüber der Personalverwaltung geheim zu halten, abzuraten sein. Anfragen bei meiner Behörde lassen den Rückschluss zu, dass Betroffene das betriebliche Eingliederungsmanagement nicht wahrnehmen, da sie es zu vermeiden suchen, sich Teilen der Personalverwaltung gegenüber zu offenbaren. Sollte eine Beteiligung von Bediensteten der Personalverwaltung doch vorgesehen sein, sollte dies auch in der Dienstvereinbarung aus Transparenzgründen konkret so erwähnt und nicht z. B. mit „Vertreter des Arbeitgebers“ umschrieben werden, so dass die Beschäftigten auch wissen, auf was sie sich einlassen. Vorstellbar ist auch, die Daten bei einem Betriebsarzt zu erheben, da dieser gegebenenfalls ohnehin Einblick in die Gesundheitsumstände betroffener Beschäftigter hat und eine Beteiligung fachlich zweckmäßig erscheint. Unabhängig davon könnte ein Betriebsarzt auch die im Verfahren anfallenden Informationen inhaltlicher Art in der Akte aufbewahren.

Die Aufgabe der Überwachung des Verfahrens ist dem Personalrat durch den Gesetzgeber zugewiesen worden, § 84 Abs. 2 Satz 1 SGB IX. Daneben wird auch dem behördlichen Datenschutzbeauftragten nach § 11 SächsDSG bei der datenschutzrechtlichen Umsetzung eine wichtige Rolle zukommen. Rechtsgrundlage für das Tätigwerden des Personalrats ist § 73 Abs. 1 Nr. 2 SächsPersVG. Der Personalrat ist dabei auch personenbezogene Informationen zu beziehen berechtigt, so die Namen der für das betriebliche Eingliederungsmanagement in Betracht kommenden Beschäftigten bzw. einen Abdruck des sogenannten Unterrichtungsschreibens der Personalverwaltung nach § 84 Abs. 2 Satz 3 SGB IX an die betroffenen Beschäftigten. Hierfür bedarf es nicht der vorherigen Zustimmung der jeweils Betroffenen. Weitere Informationen dürfen den Personalratsmitgliedern nur mit Einwilligung der Betroffenen gegeben werden (vgl. Beschluss des BVerwG v. 23. Juni 2010 - 6 P 8.09 - 23 FB 17/06).

Weitere häufige datenschutzrechtliche Fragen betreffen letztendlich die Aufbewahrungsdauer der Daten, die beim betrieblichen Eingliederungsmanagement erhoben wurden. Orientiert am Zweck der Maßnahme, der Wiederherstellung der Arbeitsfähigkeit, werden bei dauerhafter Zweckerreichung die erhobenen Daten wieder gelöscht werden können. Entscheidend wird hier sein, ob die Langzeiterkrankung überwunden und das Dienst- und Arbeitsverhältnis bestimmungsgerecht fortgesetzt werden kann. Nach wenigen Jahren wird eine Aufbewahrung der Unterlagen zum Verfahren nicht mehr erforderlich sein. Verschiedentlich wird eine Aufbewahrungsdauer von drei Jahren empfohlen. Generell sollte auch die Dienstvereinbarung zum betrieblichen Eingliederungsmanagement Festlegungen zur Speicherdauer enthalten. Im Falle eines Widerrufs der Teilnahme am betrieblichen Eingliederungsmanagement durch den Beschäftigten - die jederzeit möglich ist - während des Verfahrens sind die Daten ohnehin zu löschen.

Darüber hinaus sollte sich die bei einigen Behörden als „Integrationsvereinbarung“ betitelte Dienstvereinbarung mit ihren Regelungen auch auf die übrige Datenverarbeitung erstrecken. So sollten der Umfang der zu erhebenden Daten, die Zusammensetzung der zu bildenden Kommission und die Art und Weise der Speicherung der erhobenen Daten - wie oben beschrieben - darin normenklar geregelt sein.

5.1.5 Soziale Netzwerke - Was darf der Dienstherr vorgeben und kontrollieren?

Die zunehmende und schon weit verbreitete Nutzung sozialer Netzwerkdienste im Internet kann für den Einzelnen folgenreich und für Personal verwaltende Stellen von Interesse sein. Die gilt selbst dann, wenn die Dienste in geschlossenen Nutzerkreisen im Rahmen der privaten Lebensgestaltung genutzt werden.

Beschäftigte können sich dabei im Internet als solche darstellen und nicht selten werden durch diese selbst Bezüge zur dienstlichen Tätigkeit offenbart. So können z. B. Fotoaufnahmen in Uniform oder Abbildungen aus dem Dienstbetrieb vom Dienstherrn unerwünscht sein. Darüber hinaus wird bei der Kommunikation in sozialen Netzwerken seitens der Beschäftigten insbesondere darauf zu achten sein, dass jederzeit die gesetzlichen und angeordneteten Verschwiegenheitspflichten gewahrt bleiben. Im Hinblick auf bestimmte Behörden und deren Beschäftigte empfiehlt es sich sogar, wegen der hoheitlichen Tätigkeit oder dem Grad, in dem die Beschäftigten in der Öffentlichkeit und im Ansehen stehen, einen Verhaltenskodex aufzuerlegen, um negativen Eindrücken in der Öffentlichkeit über soziale Netzwerke vorzubeugen.

Darüber hinaus ist es, selbst wenn Informationen als allgemein zugänglich betrachtet werden können, nicht ohne weiteres erforderlich und statthaft, ohne Anlass im Internet zu Beschäftigten zu recherchieren, Nachforschungen anzustellen und Daten von Dritten ohne Kenntnis der Betroffenen zu beziehen. So enthält § 37 SächsDSG keine besondere diesbezügliche Befugnis und die allgemeinen Datenverarbeitungsbestimmungen gehen vom Direkterhebungsgrundsatz aus (§ 12 Abs. 2 Satz 1 SächsDSG). Danach dürfen nicht allgemein zugängliche personenbezogene Daten nur beim Betroffenen mit seiner Kenntnis erhoben werden. Bei sozialen Netzwerken wird davon auszugehen sein, dass es sich nicht um allgemein zugängliche Informationen handelt, wenn für den Informationsbezug und die Teilhabe eine Registrierung oder Anmeldung erforderlich ist. Darüber hinaus ist auf die Unterrichtungspflicht nach § 12 Abs. 6 SächsDSG hinzuweisen. Im Übrigen gilt auch bei allgemein zugänglichen Daten der Erforderlichkeitsgrundsatz, § 37 Abs. 1 Satz 1 SächsDSG. Die Personalverwaltung hat sich demgemäß zu beschränken. Soweit Behörden Derartiges durch interne Verwaltungsvorschriften und Richtlinien festlegen, ist dies zu begrüßen.

Auch bei Bewerbern stellt sich die Frage, ob Internet-Recherchen durchgeführt werden dürfen. Dazu wird es auf die Umstände ankommen: Soweit der Bewerber selbst auf seine oder andere Internetpräsenzen im Zusammenhang mit seiner Bewerbung oder seinen Qualifikationen hinweist, kann dies als Aufforderung zu verstehen sein, ergänzende Informationen über die angegebene Quelle zu beziehen. Das Problem dabei wird allerdings sein, dass in diesem Fall Angaben über den Bewerber, die für das Bewerbungsverfahren ohne Bedeutung sind, evtl. auch besonders sensible Bezüge im Sinne von § 4 Abs. 2 SächsDSG, von der ausschreibenden Personal verwaltenden Stelle mit zur Kenntnis genommen werden.

Im Hinblick auf mögliche Recherchen zu Bewerbern gilt wiederum der Erforderlichkeitsgrundsatz des § 37 SächsDSG. Zusätzlich ist auch zu berücksichtigen, dass nicht selten Informationen über Betroffene ohne deren Kenntnis oder Einwilligung in das Internet eingestellt werden und überhaupt Zweifel im Hinblick auf die Richtigkeit von Daten auf privaten Internetpräsenzen bestehen und eine Geeignetheit des Bezugs der Informationen regelmäßig nicht bejaht werden kann.

5.1.6 Bildung einer zentralen Reisekostenstelle

Im Geschäftsbereich des SMF wurde dem Landesamt für Steuern und Finanzen per Erlass des Staatsministeriums für den Geschäftsbereich die Aufgabe einer zentralen Reisekostenstelle übertragen. Im Sächsischen Verwaltungsorganisationsgesetz war die Aufgabenübertragung nicht festgelegt worden. Die Behörde wird auch nach außen tätig und bescheidet die Antragsteller; es handelt sich also nicht nur um eine innerorganisatorische Maßnahme.

Das Landesamt und das Staatsministerium wies ich auf die Notwendigkeit hin, die Aufgabe des Landesamtes wegen der damit einhergehenden personenbezogenen Datenverarbeitung durch eine Rechtsvorschrift zu regeln, § 4 Abs. 1 Nr. 1 SächsDSG.

Meine Bemühungen zur Herstellung eines rechtmäßigen Zustandes waren bisher nicht erfolgreich.

5.2 Personalvertretung

5.2.1 Datenerhebung durch die Personalvertretung im Überblick

Eine Pflicht zur rechtzeitigen und umfassenden Unterrichtung des Personalrats ergibt sich aus § 73 Abs. 2 SächsPersVG. Die Überwachungsaufgabe des Personalrats ist in § 73 Abs. 1 Nr. 2 SächsPersVG festgelegt. In diesem Zusammenhang, weniger bei den ausdrücklich normierten und den Mitbestimmungs- und Beteiligungstatbeständen, zeigen sich immer wieder Unsicherheiten, welche personenbezogenen Unterlagen den Per-

sonalvertretungen zur Information und zu Überwachungszwecken zur Verfügung zu stellen sind. Es ist jedenfalls nicht durch eine Dienstvereinbarung regelbar, auf welche Weise der Personalrat zu unterrichten ist (vgl. VG Frankfurt am Main - 31. Mai 2010 - 23 K 500/10).

Klargestellt hat der Gesetzgeber, dass die Personalakte nur mit Einwilligung der Beschäftigten eingesehen werden darf, § 73 Abs. 2 Satz 3 SächsPersVG, (vgl. 1/5.2.1). Auch die materiellrechtlich als Personalakten zu qualifizierenden Disziplinarvorgänge können damit ohne die Zustimmung des betroffenen Beamten nicht eingesehen werden. Der Personalrat hat nach ständiger Rechtsprechung auch keinen Anspruch auf Vorlage dienstlicher Beurteilungen (13/5.2.1). Hingegen sind dem Personalrat auf Verlangen Bewerbungsunterlagen von zur Einstellung vorgesehenen Bewerbern vorzulegen, soweit es sich dabei noch nicht um Personalakten handelt (vgl. 2/5.2.3). Die Pflicht zur Anhörung des Personalrats ergibt sich bei einschneidenden Personalmaßnahmen aus § 73 Abs. 6 SächsPersVG. Sie setzt die Kenntnisnahme der hierfür entscheidenden Informationen durch die Personalvertretung voraus.

Auch das Zur-Verfügung-Stellen von Übersichten, z. B. Stellenplänen (vgl. 4/5.2.4), die nach der Rechtsprechung des Bundesverwaltungsgerichts auch nicht materiellrechtlich als Personalakten angesehen werden und auch personenbezogen verlangt werden können, ist zulässig und ggf. erforderlich. Dies gilt wiederum nicht, wenn materiellrechtlich Einzelheiten zu Personalaktenvorgängen verlangt werden, so z. B. im Hinblick auf Antragsteller von sozialen Unterstützungen oder ähnlichen sensiblen Inhalten. Bei Leistungszulagen dagegen hat das Bundesverwaltungsgericht entschieden, dass es sich hierbei nicht um Bestandteile der Personalakten handeln soll, sondern um den Personalakten vergleichbar schutzwürdig anzusehende Listen, bei denen aber eine Zustimmung der betroffenen Beschäftigten in die Einsichtnahme durch den Personalrat nicht erforderlich sei (BVerwG - 22. Dezember 1993 - 6 P 15.92). Auch die Einsichtnahme in Gehaltslisten wird als zur Aufgabenerfüllung erforderlich angesehen (vgl. BVerwG - 22. April 1998 - 6 P 4.97). Die Personenbeziehbarkeit kann aber grundrechtsschonend eingeschränkt werden, z. B. durch Pseudonymisierung, wenn die Kenntnis der Identität zur Wahrnehmung der gesetzlichen Überwachungspflichten nicht erforderlich ist (vgl. VGH Mannheim - 25. November 2008 - PL 15 S 2634/07). Ähnlich entschied das OVG Münster im Hinblick auf Übersichtslisten zur Einhaltung der Arbeitszeitschutzbestimmungen, wonach die einzelnen Beschäftigtennamen durch feste Kennziffern ersetzt werden sollten (vgl. OVG Münster - 4. November 2005 - 1 A 4935/04). Insgesamt ist den Dienststellen daher zu raten, mit der Personalvertretung möglichst datensparsame Informationsflüsse zu vereinbaren. Ggf. kann der behördliche Datenschutzbeauftragte um eine Empfehlung ersucht werden.

Die Informationsansprüche der Personalvertretung sind auf die Bekanntgabe der für die Wahrnehmung der personalvertretungsrechtlichen Aufgaben erforderlichen Angaben beschränkt. Diese Aufgaben sind dem Grunde nach kollektiv ausgerichtet. Ein Anspruch auf Unterrichtung besteht insoweit nicht ohne Weiteres, wenn es um die Wahrnehmung individueller Rechte einzelner Beschäftigter geht, es sei denn, diese haben die Personalvertretung angerufen.

Mehrfach haben Gerichte entschieden, dass die Personalvertretung keinen Anspruch auf die im Wege eines automatisierten Abrufs bzw. eines Online-Zugriffs von der Dienststelle verarbeiteten Daten oder ganze Computerprogramme hat (z. B. VG Frankfurt am Main - 31. Mai 2010 - 23 K 500/10). Dagegen bestehen Informationsrechte der Mitarbeitervertretung im Hinblick auf eingesetzte automatisierte Verfahren und der Datenverarbeitung allgemein, nicht nur in Fällen der Mitbestimmung und der Mitwirkung sowie unabhängig von konkreten Maßnahmen der Dienststelle (vgl. BVerwG, DVBl. 1988, 74). Nach der Rechtsprechung kann die Personalvertretung zur Wahrnehmung ihrer Überwachungsfunktionen u. a. Auskünfte zu der personenbezogenen Beschäftigtendatenverarbeitung in der Dienststelle - z. B. mittels Dateiübersichten - und zu den datenschutzorganisatorischen Maßnahmen und Verfahrensabläufen - z. B. mit Hilfe von Verfahrensbeschreibungen - verlangen.

5.3 Einwohnermeldewesen

5.3.1 Bezug von Meldedaten aus dem KKM im Wege des automatisierten Abrufverfahrens durch unbefugte Mitarbeiter

Bei einer Routinekontrolle eines sächsischen Vermessungsbüros nach § 27 SächsDSG i. V. m. § 22 Abs. 4 SächsMeldVO stellte ich fest, dass der öffentlich bestellte Vermessungsingenieur Mitarbeiter mit der Abfrage von Melderegisterdaten aus dem Kommunalen Kernmelderegister auf Grundlage von § 8 SächsÖbVVO beauftragt hatte. Das KKM stellt ein Landesmelderegister dar. Behörden erhalten nach der Sächsischen Meldeverordnung im Wege des automatisierten Abrufs landesweiten Zugriff auf Meldedaten in Sachsen. Meine datenschutzrechtliche Prüfung ergab, dass die Beauftragung von Mitarbeitern mit der Abfrage von Melderegisterdaten aus dem KKM auf Grundlage von § 8 SächsÖbVVO rechtlich unzulässig ist.

Die regelmäßige Datenübermittlung im Wege des automatisierten Abrufs von Daten ist unter den gesetzlich geregelten Voraussetzungen nur für Behörden und Gerichte des Freistaates Sachsen, seiner Aufsicht unterstehende juristische Personen des öffentlichen Rechts sowie für öffentlich bestellte Vermessungsingenieure mit Amtssitz im Freistaat Sachsen zulässig (§ 29 Abs. 5 SächsMG, § 36 Nr. 4b SächsMG i. V. m. §§ 22, 34 SächsMeldVO).

Nur der öffentlich bestellte Vermessungsingenieur *selbst*, als Beliehener, ist damit rechtlich befugt, die Meldedaten im Wege des automatisierten Abrufs über das Internet abzurufen. Vergleichbar mit dieser Regelung ist das Verfahren zur Kostenerhebung nach § 24 SächsVermGeoG (seit 5. Juni 2010 SächsVermKatG).

In meiner abschließenden Stellungnahme an den kontrollierten öffentlich bestellten Vermessungsingenieur forderte ich diesen auf, entsprechend der Rechtslage die Meldedaten zukünftig selbst abzurufen.

Das zuständige Staatsministerium habe ich gebeten, diese Information an die betreffenden Stellen der Vermessungsverwaltung in geeigneter Form weiterzugeben und diese Thematik als weiteren Prüfpunkt in die reguläre Fachprüfung der öffentlich bestellten Vermessungsingenieure mit aufzunehmen. Daneben bat ich die SAKD, als die für die Einrichtung des Abrufes zuständige Stelle, um Berücksichtigung.

5.3.2 Fehlende Verpflichtung auf das Meldegeheimnis

Wer bei einer Meldebehörde oder einer Stelle, die im Auftrag der Meldebehörde handelt, beschäftigt ist, darf nach den Regelungen des Sächsischen Meldegesetzes personenbezogene Daten nicht unbefugt verarbeiten oder sonst verwenden. Zur Wahrung des sogenannten „Meldegeheimnisses“ werden deshalb alle Beschäftigten, die in der Meldebehörde tätig sind und die Personen, die im Auftrag der Meldebehörde handeln, nach § 9 SächsMG schriftlich auf das Meldegeheimnis verpflichtet.

Die Verpflichtung auf das Meldegeheimnis nach § 9 Abs. 2 SächsMG ist ein förmlicher Akt zu Beginn des Dienst-, Arbeits- oder Auftragsverhältnisses. Sie wird durch den Leiter der öffentlichen Stelle, den Arbeitgeber oder jeweils einen Beauftragten durchgeführt. Sie schließt die wichtige vorhergehende Unterrichtung des Bediensteten oder des Auftragnehmers über das Meldegeheimnis nach § 9 Abs. 1 SächsMG „sowie die sonstigen bei (seiner) Tätigkeit zu beachtenden Vorschriften über den Datenschutz“ ab und hat schriftlich bei Dienstantritt zu erfolgen. Die Urkunde ist in der Personalakte zu verwahren.

Bei routinemäßig durchgeführten anlasslosen Kontrollen von sächsischen Meldebehörden fiel mir auf, dass Bedienstete, die in der Meldebehörde tätig waren, gar nicht auf das Meldegeheimnis nach § 9 SächsMG verpflichtet worden waren bzw. z. T. ohne dass dies schriftlich erfolgt oder dokumentiert war. In der Praxis fanden sich zudem häufig nur Verpflichtungen der Beschäftigten auf das Datengeheimnis gemäß § 6 SächsDSG. Man war der Auffassung, dass man damit den Gesetzmäßigkeiten Rechnung getragen habe. § 9 SächsMG normiert das Meldegeheimnis jedoch als besonderes spezielles Datengeheimnis, das für den Bereich des Meldewesens die Anwendung der Vorschriften

über das allgemeine Datengeheimnis ausschließt, § 4 Abs. 2 SächsDSG, so dass eine Verpflichtung auf bereichsspezifischer gesetzlicher Grundlage nicht unterlassen werden darf. Darüber hinaus wird man geeigneterweise, da im Hinblick auf die Geschäftsabläufe der Beschäftigten der Meldebehörde erwartet werden kann, dass auch personenbezogene Daten, die nicht Meldedaten sind, verarbeitet und zur Kenntnis genommen werden, zusätzlich eine Verpflichtung auf das Datengeheimnis durchzuführen haben. Auch diese Verpflichtung hat formgebunden schriftlich zu erfolgen, § 6 Abs. 2 SächsDSG.

Ich habe die Erkenntnis, dass in diesem Bereich der meldebehördlichen Praxis Beratungsbedarf besteht, zum Anlass genommen, ein Muster für die Verpflichtung auf das Meldegeheimnis nach § 9 SächsMG (siehe 17.2.3) und ein erläuterndes Merkblatt zur Verpflichtung auf das Meldegeheimnis (siehe 17.2.4) zu entwerfen. Beide Hilfen biete ich auch auf meinem Internetauftritt an.

5.3.3 Unzulässig erteilte „einfache Melderegisterauskunft“ nach § 32 Abs. 1 SächsMG

Im Berichtszeitraum wandte sich ein Bürger mit der Bitte um Prüfung der Rechtmäßigkeit der durch eine Meldebehörde erteilten einfachen Melderegisterauskünfte zu seiner Person an mich. Nach dem Sächsischen Meldegesetz darf die Meldebehörde an private Personen eine Auskunft über Vor- und Familiennamen, Doktorgrad und gegenwärtige Anschriften einzelner bestimmter Einwohner übermitteln (einfache Melderegisterauskunft).

Der Bürger schilderte zwei Fälle der Auskunftserteilung, in denen die Gemeinde jeweils über seine Meldedaten Auskunft erteilt habe, obwohl sich die Anfrage auf eine andere männliche Person, zwar mit gleichem Vor- und Zunamen, aber anderer Anschrift, bezogen hätte.

Ich bat die betroffene Gemeinde um Stellungnahme zum Sachverhalt. Diese teilte mir mit, dass die Recherche mit dem Vor- und Zunamen zu dem anfragenden Bürger zu einem eindeutigen Treffer im Melderegister geführt habe. Die Meldebehörde habe wegen der Eindeutigkeit des Treffers die Auskunft zur Person des anfragenden Bürgers trotz der abweichenden Anschrift erteilt.

Die Überprüfung des Vorganges ergab, dass von einem datenschutzrechtlichen Verstoß im Zusammenhang mit den durch die Gemeinde zur Person des anfragenden Bürgers erteilten einfachen Melderegisterauskünften auszugehen ist.

Die Gemeinde hatte irrtümlich angenommen, dass die Erteilung der einfachen Melderegisterauskunft ohne jegliche Prüfung in einem vereinfachten Verfahren möglich wäre.

Sie wies in ihrer Stellungnahme an mich darauf hin, dass die Meldebehörde bei der Erteilung der einfachen Melderegisterauskunft ein berechtigtes Interesse des Anfragenden nicht prüfen müsse. In diesem Punkt habe ich der Gemeinde Recht gegeben.

Von der Prüfung des berechtigten Interesses allerdings völlig unabhängig regelt § 32 Abs. 2 Satz 1 SächsMG, dass eine Meldebehörde die einfache Melderegisterauskunft ausschließlich über die Daten „einzelner *bestimmter* Einwohner“ erteilen darf.

Als Voraussetzung für die rechtmäßige Erteilung der einfachen Melderegisterauskunft muss die Person, auf die sich die Auskunft beziehen soll, also individuell und eindeutig bestimmt sein.

Das ist nicht der Fall, wenn ein Auskunftsersuchen im Melderegister aufgrund einer Namensübereinstimmung zu einem Treffer führt, die übersandte Adresse (als sogenanntes Individualisierungskriterium) aber mit den im Melderegister zu dieser Person gespeicherten (auch früheren) Adressen nicht übereinstimmt. In diesen Fällen ist die Person, auf die sich die Auskunft beziehen soll, im Sinne des § 32 Abs. 1 Satz 1 SächsMG *nicht eindeutig bestimmt*.

Eine Auskunftserteilung ist in diesen Fällen nicht zulässig.

Wurden der Meldebehörde von Seiten des Auskunftsersuchenden keine weiteren Informationen (z. B. Geburtstag) zur gesuchten Person übersandt, kann sich die Meldebehörde zu deren Beschaffung wieder an den Auskunftsersuchenden wenden.

Ich habe die Gemeinde aufgefordert, das Verfahren der Erteilung der einfachen Melderegisterauskunft nach § 32 Abs. 1 SächsMG durch das Einwohnermeldeamt zukünftig rechtmäßig durchzuführen.

5.3.4 Anlasslose Kontrollen bei Sächsischen Meldebehörden

Im Berichtszeitraum führte ich erneut routinemäßig anlasslose Kontrollen bei sächsischen Meldebehörden durch. Hierbei traten immer wieder ähnliche Probleme auf. Beispielhaft seien die informationelle Auftrennung der Meldebehörde bei Posteingängen (vgl. die zurückliegenden Beiträge 1/5.3.9; 13/5.3.3) oder die fehlende Verpflichtung der Mitarbeiter der Meldebehörde auf das Meldegeheimnis nach § 9 SächsMG genannt (vgl. 5.3.2).

Hinweisen möchte ich aus gegebenem Anlass auf den aus melde- und datenschutzrechtlicher Sicht wichtigen Bereich der Aufbewahrung und Vernichtung von Meldescheinen,

die Löschung und gesonderte Aufbewahrung von Meldedaten und die Übernahme von Daten in das zuständige kommunale Archiv.

1) Aufbewahrung und Vernichtung von Meldescheinen nach § 18 SächsMeldVO:

Die Fristen für die Aufbewahrung und Vernichtung der Meldescheine sind in § 18 SächsMeldVO geregelt. Die Meldescheine und die Mitteilungen über die Änderung der Hauptwohnung sind nach den Festlegungen der Verordnung mindestens bis zum Ablauf des ersten, längstens jedoch bis zum Ablauf des dritten auf die Abgabe des Meldescheins oder der Mitteilung folgenden Kalenderjahres gesondert aufzubewahren und danach zu vernichten.

In einer Vielzahl der kontrollierten Meldebehörden wurden die Meldescheine nicht nach der in der Sächsischen Meldeverordnung geregelten Frist vernichtet. In einigen Meldebehörden lagerten noch Anmeldescheine aus den 90er Jahren.

Ich habe die betreffenden Meldebehörden jeweils aufgefordert, den Bestand der Meldescheine zu überprüfen und die gemäß § 18 SächsMeldVO zu lange aufbewahrten Meldescheine zu vernichten.

2) Löschung und gesonderte Aufbewahrung von Meldedaten (§ 26 SächsMG):

Nach § 26 Abs. 1 Nr. 2 SächsMG hat die Meldebehörde die Daten zu löschen, wenn ihre Kenntnis zur Erfüllung der der Meldebehörde obliegenden Aufgaben nicht mehr erforderlich ist. Eine große Anzahl von Meldebehörden erfüllt die Vorgaben zur Löschung und gesonderten Aufbewahrung von Meldedaten nach meiner Erfahrung jedoch nicht. Ich wies deswegen bei meinen Besuchen die Stellen darauf hin, dass § 26 SächsMG die Löschung und gesonderte Aufbewahrung der gesetzlich nicht mehr erforderlichen Meldedaten in einem dreistufigen Verfahren vorsieht. Diese zwingenden gesetzlichen Vorgaben gelten sowohl für die in Papierform als auch für die elektronisch gespeicherten Daten. Teilweise gaben die Meldebehörden bei den Kontrollen an, dass die eingesetzten IT-Verfahren (Einwohnermeldeverfahren) sie nicht in die Lage versetzten, die gesetzlichen Vorgaben zur Löschung und gesonderten Aufbewahrung von Meldedaten gemäß § 26 SächsMG zu erfüllen. Unabhängig von der Befähigung der beauftragten IT-Dienstleister und Verfahrensanbieter bleiben rechtlich die Meldebehörden als Daten verarbeitende Stellen verpflichtet, den ordnungsgemäßen Umgang mit den Meldedaten sicherzustellen (§ 5 i. V. m. § 26 SächsMG). Insofern ist die öffentliche Stelle aufgefordert, ggf. mit dem Anbieter des Einwohnermeldeverfahrens Kontakt aufzunehmen und eine gesetzeskonforme Umsetzung des Vertrags sicherzustellen bzw. das IT-Verfahren entsprechend anzupassen.

3) Übernahme von Daten in das zuständige kommunale Archiv, § 27 SächsMG:

Bei meinen Kontrollbesuchen musste ich auch darauf hinweisen, dass gemäß § 27 SächsMG vor Löschung der Daten oder nach Ablauf der in § 26 Abs. 4 Satz 1 SächsMG bestimmten Frist die Daten dem zuständigen kommunalen Archiv zur Übernahme anzubieten sind. Zu diesem Zweck sollte die Meldebehörde dem zuständigen Archiv eine Aufstellung aller Arten von Dokumenten und Daten (unter Beifügung von Beispielen) zur Entscheidung, ob eine Übernahme durch das Archiv beabsichtigt ist, vorlegen. Gemäß der zu dokumentierenden Entscheidung des Archivs sind die Daten dann dem Archiv zu übergeben. Nicht vom Archiv übernommene Daten sind zu löschen.

5.3.5 Keine Datenverarbeitung ohne Aufgabe - Datenübermittlung des Einwohnermeldeamtes aus Anlass der Einführung einer Zweitwohnungssteuer

Ein Betroffener teilte mir im Berichtszeitraum mit, dass die Meldebehörde seines Zweitwohnsitzes im Zusammenhang mit der Erhebung einer Zweitwohnungssteuer Meldedaten an die städtische Steuer- und Kassenverwaltung übermittelt habe. Er unterbreitete mir, dass diese Datenübermittlung wohl noch vor dem Inkrafttreten der Zweitwohnungssteuersatzung stattgefunden habe und bat mich um datenschutzrechtliche Überprüfung des Vorganges.

Die von mir zur Stellungnahme aufgeforderte Stadtverwaltung bestätigte in ihrer Erwiderung, dass die Übermittlung der Meldedaten vor dem Inkrafttreten der Zweitwohnungssteuersatzung der Gemeinde stattgefunden habe. Die Stadt glaubte sich in ihrer Stellungnahme damit zu entlasten, dass die Datenübermittlung des Einwohnermeldeamtes bereits vor Inkrafttreten der Zweitwohnungssteuersatzung gemäß § 29 Abs. 1 i. V. m. § 29 Abs. 7 SächsMG rechtlich zulässig gewesen sei.

Die datenschutzrechtliche Überprüfung des Vorgangs ergab hingegen, dass die vorbereitende Datenübermittlung der Meldebehörde an die Steuer- und Kassenverwaltung in Erwartung der Satzung unzulässig gewesen war.

§ 29 Abs. 1 SächsMG bestimmt, dass die Meldebehörde einer anderen Behörde oder sonstigen öffentlichen Stelle in der Bundesrepublik Deutschland aus dem Melderegister Daten von Einwohnern übermitteln darf, wenn dies zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. § 29 Abs. 7 SächsMG bestimmt, dass dieser Absatz auch für die Weitergabe von Daten und das Bereithalten von Daten zur Einsichtnahme innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, entsprechend gilt.

Die Datenübermittlung nach § 29 SächsMG ist demnach nur zulässig, wenn diese zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. Diese rechtlich zwingende Voraussetzung war zum Zeitpunkt der Datenübermittlung jedoch nicht erfüllt. Auch wenn, wie im mir zur Kenntnis gelangten Vorgang, der Stadtrat der Stadt die Satzung bereits vor der Übermittlung beschlossen hatte und diese auch bereits im Amtsblatt veröffentlicht wurde, entfaltete die Satzung ihre Rechtskraft erst mit ihrem Inkrafttreten.

Erst ab Wirksamwerden der Satzung war es Aufgabe der Stadt i. S. d. § 29 SächsMG gewesen, eine Zweitwohnungssteuer für das Innehaben einer Zweitwohnung im gesamten Stadtgebiet zu erheben. Wäre eine Datenübermittlung der Meldebehörde an die städtische Steuer- und Kassenverwaltung im Zusammenhang mit der Erhebung der Zweitwohnungssteuer zu einem früheren Zeitpunkt beabsichtigt gewesen, hätte dieser Vorgriff in der Satzung und ein Inkrafttreten davor geregelt sein müssen.

Im Hinblick auf das zeitnah auf die Datenübermittlung folgende Wirksamwerden der Satzung als Rechtsgrundlage für die Datenübermittlung und die Tatsache, dass die Daten relativ bald nach der erfolgten Übermittlung gemäß der einschlägigen Vorschrift der Satzung in zulässiger Weise hätten erhoben werden können, verzichtete ich darauf, die Stadtverwaltung zur Löschung der rechtswidrig übermittelten Daten aufzufordern. Die Stadtverwaltung und der Betroffene wurden abschließend schriftlich über die Rechtswidrigkeit der erfolgten Datenübermittlung informiert.

5.4 Personenstandswesen

5.4.1 Hinterlegungsverbot des Personalausweises

Durch eine Petition nach § 24 SächsDSG wurde ich im Berichtszeitraum darauf aufmerksam gemacht, dass in einem staatlichen Museumsbereich bei der Ausleihe eines sog. „Audio-Guide“ die Hinterlegung des Personalausweises gefordert werde.

Seit dem 1. November 2010 gilt das geänderte Personalausweisgesetz. In § 1 Abs. 1 Satz 3 PAuswG ist geregelt, dass vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Entsprechend dieser Regelung wäre die Hinterlegung des Personalausweises als Pfand für die Leihe eines „Audio-Guide“ rechtswidrig.

Ich bat die zuständige Daten verarbeitende Stelle um Stellungnahme zum Sachverhalt. Diese teilte mir mit, dass sie die gesetzlichen Regelungen beachten würde und dass der beschriebene Sachverhalt das Verhalten eines privaten Dienstleisters betreffen würde. Sie habe anlässlich meines Schreibens den Dienstleister aufgefordert, die Beachtung der

gesetzlichen Vorschriften sicherzustellen und dies schriftlich zu bestätigen. Weiter versicherte mir die Museumsleitung in ihrem Schreiben, dass auch vor der gesetzlichen Änderung keine Datensammlung stattgefunden hätte. Die Ausweise seien, wie andere vergleichbare Pfänder, nur aufbewahrt und nach Abgabe der „Audio-Guide“-Geräte wieder an die Besucher ausgegeben worden. Eine Registrierung oder eine sonstige Erfassung der Ausweisinhalte habe nicht stattgefunden.

Mittlerweile liegt mir eine schriftliche Erklärung des Dienstleisters vor, wonach die Besucher nicht mehr um die Abgabe von Personalausweisen gebeten werden. Ich gehe daher davon aus, dass die Ausweishinterlegung als Pfand für die Entleihe eines „Audio-Guide“-Gerätes nicht mehr praktiziert wird.

5.5 Kommunale Selbstverwaltung

5.5.1 Unzulässige Übermittlung von persönlichen Angaben einer Vertrauensperson bei einem Einwohnerantrag - Unverschlüsselte E-Mail-Kommunikation

Auf die Anfrage eines Landratsamtes hin beriet ich die Behörde bei der Prüfung einer Dienstaufsichtsbeschwerde eines Gemeinderatsmitglieds wegen eines vorgeblichen Datenschutzverstoßes durch einen Bürgermeister.

Dem Vorgang lag folgender Sachverhalt zugrunde: Der Bürgermeister übermittelte ein Schreiben zu einem Einwohnerantrag zur Aufhebung einer Straßenausbausatzung mit der Bitte um vertrauliche Behandlung per E-Mail als Kopie parallel an alle Mitglieder des Gemeinderates. Das Schreiben, das an den als Vertrauensperson zu dem Einwohnerantrag benannten Gemeinderat gerichtet war, enthielt über allgemeine Einzelheiten zu dem Antragsgegenstand hinaus Details über private Mietschulden des Gemeinderatsmitglieds beim Eigenbetrieb Immobilienwirtschaft der Gemeinde. Der betroffene Gemeinderat wurde in dem Schreiben konkret als langjähriger und fortwährender Mietschuldner mit einem Mietrückstand von mehr als zwei Monatsmieten bei mehrfach nicht eingehaltenen Ratenzahlungsvereinbarungen bezeichnet. Das Schriftstück der Gemeinde war als Eingangsbescheid für den Einwohnerantrag (§ 23 SächsGemO) zu bewerten, enthielt jedoch keine Hinweise auf die rechtlich vorgeschriebenen und durch die Gemeinde vorzunehmenden Verfahrenshandlungen.

Die Übermittlung des Schreibens an die Gemeinderäte und ihre Kenntnisnahme der weitergehenden Angaben über den Gemeinderat im Hinblick auf Mietschulden erfährt im Einwohnerantragsverfahren keine rechtliche Stütze. Unerheblich war in diesem Zusammenhang auch der Einwand des sich verteidigenden Bürgermeisters, er habe an anderer Gelegenheit in seiner Eigenschaft als Betriebsleiter des Eigenbetriebes den Ge-

meinderat in nichtöffentlicher Sitzung über Mietrückstände und Mahnverfahren bereits informiert; der Gemeinderat habe zu den Betroffenen gehört und dass die Tatsachenbehauptung wahr gewesen sein mag. In dem geregelten Einwohnerantragsverfahren dürfen weitergehende Informationen zu Antragstellern und Vertrauenspersonen, soweit sie für den Sachgegenstand nicht von Bedeutung sind, auch wenn die Gemeindeverwaltung hier über Spezialwissen verfügt, natürlich nicht weitergegeben werden. Denn wie sich aus der grundlegenden gesetzlichen Festlegung des § 4 Abs. 1 SächsDSG ergibt, ist die Verarbeitung personenbezogener Daten bei nicht vorliegender Einwilligung des Betroffenen nur zulässig, wenn die Regelungen des Sächsischen Datenschutzgesetzes oder andere Rechtsvorschriften dies erlauben. Für die Übermittlung der personenbezogenen Daten des als Vertrauensperson fungierenden Gemeinderates durch die E-Mail mit dem Betreff „Einwohnerantrag“ an die Gemeinderäte lag eine Rechtsgrundlage nicht vor, weder bereichsspezifisch, d. h. kommunalrechtlich, noch nach dem Sächsischen Datenschutzgesetz. Durch die Datenübermittlung des Bürgermeisters wurde aufgrund der persönlichen und ansehensrelevanten Angaben des betroffenen Gemeinderatsmitglieds dessen Persönlichkeitsrecht verletzt. Diese Tatsache änderte auch nicht die Feststellung, dass die Datenübermittlung an die (grundsätzlich) berechtigten Gemeinderäte erfolgte. Diese erhielten offenkundig nicht für die Aufgabenerfüllung erforderliche Einzelangaben (erneut) zur Kenntnis und der Betroffene war durch das Eingangsschreiben in einem (anderen) Verfahren mit ihn in negativem Licht erscheinen lassenden sachfremden Einzelheiten aktenkundig belastet.

Zu dem datenschutzrechtlichen kam ein datenschutzorganisatorischer Verstoß hinzu, nämlich dahingehend, dass bei einer Nutzung der E-Mail-Kommunikation durch öffentliche Stellen geeignete Maßnahmen zu treffen sind, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. So ist beim Absender und Adressaten bei der Übermittlung schutzwürdiger personenbezogener Daten durch öffentliche Stellen grundsätzlich eine Verschlüsselungssoftware zu verwenden, um personenbezogene Daten vor unbefugter Kenntnisnahme zu schützen. Es konnte unterstellt werden, dass der Bürgermeister eine Verschlüsselungssoftware bei der Übermittlung der E-Mail an die Gemeinderäte nicht verwendete. Das ist ein allgemein häufig zu beobachtender Missstand bei sächsischen Behörden. Damit erhielt der Datenschutzverstoß wegen der unverschlüsselten Übermittlung der Daten auch einen grundsätzlichen Bezug, denn bei Übermittlungen an eine Vielzahl von privaten E-Mail-Adressen besteht auch eine nicht zu vernachlässigende Wahrscheinlichkeit von unberechtigten Kenntnisnahmen durch unbefugte Dritte. Allgemein bleibt nämlich zu betonen, dass eine Übermittlung von Sitzungsunterlagen zu Gemeinderatsangelegenheiten an die Mitglieder nach § 36 Abs. 3 SächsGemO, die geeignet sind, das öffentliche Wohl oder berechtigte Interessen Einzelner zu gefährden, per E-Mail - auch verschlüsselt - datenschutzrechtlich wegen des

privaten Standortes des PC und des damit verbundenen Mangels an Vertraulichkeit grundsätzlich ungeeignet ist. Auch eine nachträgliche Versicherung der Gemeinderäte, die E-Mail keiner weiteren Person zur Kenntnis gegeben zu haben, konnte - abgesehen von der bereits eingetretenen Kenntnisnahme der Gemeinderäte von den privaten mietvertraglichen Einzelangaben des Betroffenen - den eingetretenen Datenschutzverstoß nicht vollständig kompensieren.

5.5.2 Öffentliche Zustellung über das Internet

Ein Petent teilte mir mit, dass eine öffentliche Zustellung, die gemäß § 15 SächsVwZG (seit 5. Juni 2010 SächsVwVfZG) im Amtsblatt einer Kommune zu erfolgen hatte, durch die Veröffentlichung des Amtsblatts auch im Internet erfolgte. Das um seine Rechtsauffassung gebetene SMI teilte mir dazu mit, dass eine öffentliche Zustellung über das Internet nicht möglich sei. In einem weiteren Schreiben stellte es klar, dass auch archivrechtliche Vorschriften keine Rechtsgrundlage für die Veröffentlichung des Amtsblattes enthielten. Dies entspricht auch meiner Auffassung.

Ich teilte dies der Kommune mit und bat um Löschung der personenbezogenen Daten des Petenten im Internet. Diese verwies in ihren Antworten jedoch nur auf das erste Schreiben des SMI und war der Meinung, dass eine Veröffentlichung der aktuellen Amtsblätter im Internet eine Archivierung darstelle. Diese Ansicht würde im Übrigen auch durch den SSG geteilt, der mich zudem aufgefordert habe, mein Schreiben an die Kommune zu revidieren. Eine derartige Aufforderung des SSG habe ich nicht erhalten.

Leider hat das SMI meiner Bitte um Klarstellung gegenüber der Kommune und dem SSG nicht entsprochen. Es teilte mir vielmehr eine vollkommen neue Rechtsauffassung mit. So sei die Veröffentlichung einer öffentlichen Zustellung im Internet durch eine Kommune keine öffentliche Zustellung und daher unabhängig von der Frage, ob eine Archivierung vorliege, zulässig. Eine Rechtsgrundlage für derartige Veröffentlichungen wurde in diesem Schreiben freilich nicht benannt.

Da die Kommune letztendlich doch die personenbezogenen Daten des Petenten aus ihrer Internetveröffentlichung gelöscht hat, habe ich von einer Beanstandung abgesehen. Ergänzend sei darauf hingewiesen, dass das Verwaltungszustellungsrecht des Freistaates Sachsen in § 4 SächsVwVfZG nunmehr lediglich einen Verweis auf das Verwaltungszustellungsgesetz des Bundes enthält. Der Gesetzentwurf der Staatsregierung (LT-Drs. 5/1326) führt dazu aus: „*Die öffentliche Zustellung wird den Möglichkeiten der elektronischen Kommunikation angepasst. Bislang war eine Bekanntmachung über das Internet (Website) aufgrund der Formulierung („Aushang“) nicht möglich*“. Seit Inkrafttreten dieser Änderung vom 19. Mai 2010 ist die öffentliche Zustellung auch in

einem „elektronischen Amtsblatt“ zulässig, soweit dies durch die Behörde hierfür allgemein bestimmt ist.

Grundsätzlich ist darauf hinzuweisen, dass die vorgenannte Veröffentlichungsbefugnis nur für öffentliche Zustellungen *nach* Inkrafttreten des Sächsischen Verwaltungsverfahrenszustellungsgesetzes gilt. Es ist also nicht rückwirkend zulässig, personenbezogene Daten aus früheren Amtsblättern im Internet zu veröffentlichen.

5.5.3 Datenschutz bei Stadtratsvorlagen

Bei der Vorbereitung von Gemeinderatssitzungen sind nicht selten Unsicherheiten festzustellen, die den erforderlichen Schutz personenbezogener Daten in Beschlussvorlagen betreffen (vgl. auch 12/5.5.6, 5.5.9 und 14/5.5.4). Gegenstand einer an mich gerichteten Beschwerde war, dass über eine Beschlussvorlage der Verwaltung im Hinblick auf einen Antrag eines Einwohners auf sanierungsrechtliche Genehmigung einer Grundschuldbestellung in öffentlicher Sitzung des Stadtrates entschieden werden sollte.

Wegen der Eilbedürftigkeit, wie es in der Stellungnahme hieß, sei die Vorlage nicht, wie es die Hauptsatzung eigentlich vorschrieb, in den Technischen Ausschuss überwiesen worden, sondern als öffentlich zu behandelnde Vorlage an alle Stadtratsmitglieder verteilt worden.

Die vorgesehene Behandlung der Vorlage in öffentlicher Stadtratssitzung ließ unbeachtet, dass die allgemeinen Vorschriften für städtebauliche Sanierungsmaßnahmen den Schutz personenbezogener Daten begründen. Die in § 138 BauGB enthaltenen Vorgaben zur Auskunftspflicht des Betroffenen über seine persönlichen Lebensverhältnisse im wirtschaftlichen und sozialen Bereich und Sanktionsmöglichkeiten bei Verweigerung gehen einher mit einer strikten Zweckbindung der Daten und einem Löschungsgebot nach Aufhebung der förmlichen Festlegung des Sanierungsgebietes. Eine Übermittlungsbefugnis für personenbezogene Daten ist stark eingeschränkt und zweckgebunden. Die mit der Verarbeitung dieser Daten Beauftragten sind entsprechend zu verpflichten.

Ich habe der Stadt mitgeteilt, dass die vorgenannten Regeln des Baugesetzbuches zwingend die Anwendung der datenschutzrechtlichen Vorschriften der §§ 36 Abs. 3 Satz 1, 37 Abs. 1 Satz 1 SächsGemO bedingen, die eine Behandlung von Beschlussvorlagen in öffentlicher Sitzung bei entgegenstehenden berechtigten Interessen Einzelner untersagen. Da die Vorlage bereits öffentlich und an alle Stadtratsmitglieder ausgereicht war, erwies sich die Mitteilung der Stadt über die Absetzung der Vorlage von der Tagesordnung der Stadtratssitzung für den festgestellten Datenschutzverstoß als unerheblich. Im Ergebnis meiner Prüfung wurde im Büro des Stadtrates die Vorlage gegen-

ständlich vernichtet und die Begründung im Sitzungsprogramm gelöscht. Die Mitglieder des Stadtrats wurden auf ihre Verschwiegenheitspflicht hingewiesen und die Vorlage wurde eingezogen. Auf eine förmliche Beanstandung habe ich daher verzichtet.

5.5.4 Öffentlichkeitsgrundsatz der Gemeinderatssitzungen und Bekanntgabe von Grundstücksverkäufen der Gemeinde

Mehrfach habe ich mich in der Vergangenheit (vgl. 1/5.5.2, 7/5.5.7, 13/5.5.1 und insbesondere 12/5.5.9) zu verschiedenen Fragestellungen zur Beachtung des Öffentlichkeitsgebots für Sitzungen des Gemeinderats nach § 37 Abs. 1 SächsGemO geäußert. Anfragen hierzu erhalte ich häufig. In einem erneuten Fall betraf dies die Zulässigkeit der Veröffentlichung einer Mitteilung über den öffentlich gefassten Beschluss des Gemeinderats zum Verkauf eines kommunalen Grundstücks unter Nennung des Kaufpreises sowie des Namens und der Adresse des Käufers im Amtsblatt.

Der Öffentlichkeitsgrundsatz bei Sitzungen des Gemeinderats nach der Sächsischen Gemeindeordnung wird lediglich durchbrochen, wenn das öffentliche Wohl oder berechtigte Interessen Einzelner eine nichtöffentliche Verhandlung erfordern. Grundstücksverkaufsangelegenheiten sind nach § 37 SächsGemO grundsätzlich öffentlich zu behandeln. Bei Veräußerungsgeschäften der Gemeinde treten die berechtigten Interessen Einzelner regelmäßig zurück. Veräußerungen der Gemeinde sind von der Interessenlage, was die öffentliche Stelle und den Käufer angeht, als Leistungsaustauschbeziehung wie Ausschreibungen zu sehen. Für die Öffentlichkeit sind daher der Kaufpreis und auch die wesentlichen Verkaufsmodalitäten sowie behördliche Auflagen von Interesse. Die Transparenz soll den Vergleich durch die Gemeindeöffentlichkeit ermöglichen und so eine ordnungsgemäße Behandlung durch die Verwaltung sicherstellen, Begünstigungen, Benachteiligungen und Vetternwirtschaft ausschließen helfen.

Rechtsgrundlage für öffentliche Bekanntmachungen der Gemeinde ist, soweit nicht besondere bundes- oder landesrechtliche Vorschriften anzuwenden sind, die Bekanntmachungsverordnung. Öffentliche Bekanntmachungen im Sinne der Verordnung sind die Verkündung von Rechtsverordnungen, die öffentliche Bekanntmachung von Satzungen und sonstige durch Rechtsvorschrift vorgeschriebene öffentliche Bekanntmachungen und öffentliche Bekanntgaben. Soweit durch Rechtsvorschrift die ortsübliche Bekanntmachung oder die ortsübliche Bekanntgabe vorgeschrieben ist, kann diese auch nach den Bestimmungen der Bekanntmachungsverordnung erfolgen (§ 1 KomBekVO). Die Gemeinde hat die Form der Bekanntmachung (z. B. Amtsblatt) durch Satzungsbeschluss zu regeln (§ 6 KomBekVO). Durch eigene Rechtsvorschrift (§ 36 Abs. 4 SächsGemO) sind beispielsweise Zeit, Ort und Tagesordnung der öffentlichen Sitzung ortsüblich bekanntzugeben.

Eine Bekanntgabe über den Kauf eines kommunalen Grundstücks unter Nennung des Kaufpreises sowie Name und Adresse des Käufers im Gemeindeblatt unter Wahrung datenschutzrechtlicher Vorgaben ist nur dann zulässig, wenn die Bekanntmachungssatzung der Gemeinde vorsieht, öffentlich gefasste Beschlüsse generell im Amtsblatt zu veröffentlichen. Im Übrigen sollten dabei nur die erfolgreichen Bieter genannt werden. Darüber hinausgehende Veröffentlichungen, z. B. was unterlegene Bieter betrifft, sind nicht erforderlich und daher unzulässig. Bei den Vergabeverfahren sowie bei der Vorbereitung der Beschlüsse und textlichen Fassung der Beschlussvorlagen ist dies bereits zu berücksichtigen. Vorlagen sind im Übrigen gemeinderechtlich nicht zu veröffentlichen.

Die Bekanntmachungssatzung sollte darüber hinaus - sofern dies für erforderlich angesehen wird - die Veröffentlichung im Gemeindeblatt bzw. von Beschlüssen über das Internet vorsehen. Dieses Medium erlangt auch im Hinblick auf die Information der Einwohner immer mehr Bedeutung. Lediglich die in der Satzung vorgesehene Veröffentlichung im Gemeindeblatt bzw. der gesetzliche Umstand, dass Sitzungen öffentlich stattzufinden oder stattgefunden haben, bietet noch keine normenklare Rechtsgrundlage, um personenbezogene Daten im *World Wide Web* zu veröffentlichen (vgl. auch 5.5.2 zur öffentlichen Zustellung über das Internet). Leider erhalte ich auch in Bezug auf die Veröffentlichung von Gemeindeblättern und der damit einhergehenden Preisgabe personenbezogener Daten im Internet immer mehr berechtigte Eingaben von Betroffenen. Dabei ist die Löschung von einmal im Internet veröffentlichten personenbezogenen Daten schwierig zu bewerkstelligen und aufgrund der Vervielfältigungsmöglichkeiten und wegen der Suchmaschineninhalte im Internet manchmal auch nicht möglich. Persönlichkeitsrechtsverletzungen werden damit häufig irreparabel. Dessen und der damit verbundenen Verantwortung sollten sich die Behördenverantwortlichen stets bewusst sein.

5.5.5 Übermittlung von Grundstückseigentümerdaten an öffentlich-rechtliche Entsorgungsträger

Die kreisfreien Städte, die Landkreise und die Abfallverbände sind gesetzlich öffentlich-rechtliche Entsorgungsträger. Zum Einzug der Abfallgebühren benötigen sie die Anschriften der Gebührenschuldner. Zwar dürfen die öffentlich-rechtlichen Entsorgungsträger nach § 12b SächsABG u. a. bei Behörden und sonstigen öffentlichen Stellen des Freistaates Sachsen sowie bei Landkreisen und Gemeinden die erforderlichen Daten erheben und die so gewonnenen Daten weiterverarbeiten. Außerdem dürfen die Meldebehörden nach § 3a Abs. 4 SächsABG den öffentlich-rechtlichen Entsorgungsträgern die für die Heranziehung des Gebührenschuldners erforderlichen Daten übermitteln. In der Praxis erreichen mich jedoch in einigen Fällen Nachfragen zu Übermittlungsbefugnissen, die sich nicht direkt aus dem Sächsischen Abfallswirtschafts- und Bodenschutzgesetz und der jeweiligen zugrunde zu legenden abfallwirtschaftlichen Sat-

zung ableiten lassen. Das betrifft insbesondere Nachfragen zur Übermittlungsbefugnis von „Alt-Datenbeständen“ bei einer Aufgabenübertragung bzw. der Neugründung von Abfallverbänden sowie die Ermittlung der Gebührenschuldner bei Gewerbegrundstücken.

Zur Rechtslage: Das Kommunalabgabengesetz bestimmt, dass die Vorschriften über das Steuergeheimnis (§ 30 AO) auf Kommunalabgaben sinngemäß anzuwenden sind (§ 3 Abs. 1 Nr. 1 Ziff. c SächsKAG). Nach § 7 Abs. 3 SächsKAG obliegt die Festsetzung und Erhebung der Realsteuern (Grundsteuer) den Gemeinden. Die für die Verwaltung der Grundsteuer zuständigen Behörden sind nach § 31 Abs. 3 AO berechtigt, die nach dem Steuergeheimnis geschützten Namen und Anschriften von Grundstückseigentümern, die bei der Verwaltung der Grundsteuer bekannt geworden sind, zur Verwaltung anderer Aufgaben sowie zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden oder den hierfür zuständigen Gerichten, Behörden oder juristischen Personen des öffentlichen Rechts auf Ersuchen mitzuteilen, soweit nicht überwiegende Interessen des Betroffenen entgegenstehen.

Die öffentlich-rechtlichen Entsorgungsträger, die allgemein über eine Erhebungsbefugnis im Hinblick auf Namen und Anschriften der Grundstückseigentümer verfügen, können sich daher an die zuständigen Grundsteuerbehörden, die Gemeinden, wenden. Die Gemeinden wiederum sind nach § 31 Abs. 3 AO zur Offenbarung bzw. Übermittlung der Daten befugt.

Gewerbedaten unterliegen nach § 11 Abs. 4 GewO einer strengen Zweckbindung. Unabhängig von einer jederzeit möglichen Übermittlung der Grunddaten des Gewerbetreibenden, wozu Name, betriebliche Anschrift und angezeigte Tätigkeit gehören, wäre jedoch eine anlassbezogene fallweise Übermittlung weiterer Daten aus dem Gewerberegister an eine öffentlich-rechtliche Stelle zulässig, soweit diese nicht als öffentlich-rechtliches Unternehmen am Wettbewerb teilnimmt (§ 14 Abs. 7 Nr. 3 GewO). Aber auch an öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, dürfen der Zweckbindung unterliegende Daten übermittelt werden, nämlich dann, wenn diese Datenempfänger ein rechtliches Interesse an der Kenntnis der übermittelten Daten geltend machen und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Gewerbetreibenden überwiegt (§ 14 Abs. 8 GewO). Die Vorschrift kann bei im Auftrag des Entsorgungsträgers handelnden Eigenbetrieben Anwendung finden.

Soweit von den öffentlich-rechtlichen Entsorgungsträgern wegen einer hohen Anzahl von unzustellbaren Gebührenbescheiden eine regelmäßige jährliche Übermittlung der Grundstückseigentümerdaten durch die Steuerämter der Gemeinden gefordert wird, würde sich der überwiegende Teil dieser Daten auf bereits bekannte Daten beziehen und

die Übermittlung des Gesamtdatenbestandes wäre auch als unverhältnismäßig einzuordnen. Bei Unzustellbarkeit eines Gebührenbescheides - z. B. bei Missachtung der Anzeigepflicht bei einer Adressenänderung des Gebührenschuldners - ist zur Ermittlung der Anschrift des Gebührenschuldners zunächst eine entsprechende Anfrage an die zuständige Meldebehörde (§ 3a Abs. 4 SächsABG i. V. m. § 29 SächsMG) zu richten. Gegebenenfalls kann eine Auskunft aus dem Gewerberegister zulässig sein.

Bei den Daten empfangenden öffentlich-rechtlichen und privaten Entsorgungsunternehmen, die am Wettbewerb teilnehmen, ist für Datenübermittlungen an diese, soweit bereichsspezifische Bestimmungen nicht greifen, die Vorschrift des § 16 Abs. 1 SächsDSG maßgeblich. Die Übermittlung muss nach § 16 Abs. 1 Nr. 1 SächsDSG zur Aufgabenerfüllung der übermittelnden Stelle (kreisfreie Stadt bzw. Landkreis) erforderlich sein und es muss geprüft werden, ob die Voraussetzungen vorliegen, die eine Datennutzung zu anderen Zwecken nach § 13 Abs. 1 bis 4 SächsDSG zulassen würden. Nicht selten werden die tatbestandlichen Bedingungen erfüllt sein, insbesondere dann, wenn die Übermittlung von Grundstückseigentümerdaten letztendlich für Zwecke erfolgen kann, für die die Daten bereits erhoben worden sind, § 13 Abs. 1 Nr. 2 SächsDSG. Bei etwaigen Auskünften aus dem Gewerberegister kann nach § 14 Abs. 8 GewO übermittelt werden, s. o. Eine entsprechende Regelung findet sich für andere Datenbestände, soweit keine spezielleren Vorschriften einschlägig sind, in § 16 Abs. 1 Nr. 2 SächsDSG.

Übermittelte Daten an öffentlich-rechtliche Stellen, die am Wettbewerb teilnehmen, dürfen von diesen nicht zu anderen Zwecken weiterverarbeitet werden, § 16 Abs. 4 SächsDSG. Die Übermittlung kann nach Absatz 5 mit Auflagen versehen werden. Nachweise der Datennutzung und der Einhaltung von Löschfristen können z. B. geeignet sein. Von dieser Möglichkeit machen Daten übermittelnde öffentliche Stellen noch zu wenig Gebrauch.

5.5.6 Behandlung von personenbezogenen Angaben in Beschlussvorlagen und Unterlagen bzw. Niederschriften öffentlicher Stadtratssitzungen - Ein positives Beispiel

Bereits in Tätigkeitsberichten zuvor hatte ich mich zu Fragen der Veröffentlichung und des Schutzes personenbezogener Daten in Unterlagen oder Protokollen öffentlicher Stadtratssitzungen geäußert (vgl. 12/5.5.9, 13/5.5.1, 14/5.5.4).

Im aktuellen Berichtszeitraum wandte sich eine Stadtverwaltung mit der Frage an mich, wie mit personenbezogenen Daten im Zusammenhang mit der Vor- und Nachbereitung von öffentlichen Sitzungen zu verfahren sei. Besonders im Umgang mit Beschlussvorlagen sowie Unterlagen bzw. Protokollen öffentlicher Stadtratssitzungen bestand Un-

sicherheit zur Frage der (Un-)Zulässigkeit der namentlichen Nennung der Antragsteller in Angelegenheiten zum Beispiel zur Vergabe öffentlicher Aufträge, Bauvorhaben bzw. der Vergabe von Fördermitteln. Die Anfrage stand auch im Zusammenhang mit dem von der Stadt betriebenen und über das Internet veröffentlichten Ratssystem.

Für eine bessere Abstimmung mit meiner Behörde übersandte mir die Stadt die von ihr zu dieser Thematik vertretenen Standpunkte. Die Gemeinde vertrat darin unter anderem die Auffassung, dass bei Stadtratssitzungen nur die für die Aufgabenerfüllung erforderlichen Daten in die Beschlussvorlagen aufzunehmen seien. Dabei sollte auf Detailangaben weitgehend verzichtet werden. Beispielsweise würde von der betroffenen Person statt der Angabe der Adresse nur der Wohnort, statt des genauen Geburtsdatums nur das Alter in Jahren oder wenn benötigt, statt der Angabe des genauen Familienstandes die Angabe „verheiratet/nicht verheiratet“ angegeben werden. Die Vorabübersendung von Unterlagen in Vorbereitung einer Sitzung sollte nur dann personenbezogene Daten enthalten, wenn dies zwingend erforderlich wäre. In diesem Fall sollten die Unterlagen auf das erforderliche Minimum reduziert, in einem verschlossenen Umschlag versandt und der Umschlag mit dem Schriftzug „vertraulich“ besonders gekennzeichnet werden. Sitzungsunterlagen mit personenbezogenen Daten seien nur den Mitgliedern des Gremiums zuzuleiten, dass für die Beratung und Entscheidung in dieser Angelegenheit zuständig sei.

Sensible Daten, die für eine sachgemäße Entscheidung des Stadtrates unverzichtbar seien, aber nicht in Vorbereitung der Sitzung an die Stadträte übersandt worden sind, sollten als Tischvorlagen nur vor und nach der Sitzung zur Verfügung gestellt und anschließend vernichtet werden.

Die mir von der Stadt vorgeschlagenen Handlungsweisen befanden sich im Einklang mit den geltenden datenschutzrechtlichen Normen bzw. deckten sich mit meinen Vorstellungen (vgl. 14/5.5.4), so dass ich lediglich ein paar ergänzende Erläuterungen hinzufügte.

Generelle Aussagen hinsichtlich der Zulässigkeit der Nennung personenbezogener Daten in Beschlussfassungen, Protokollen oder Sitzungsunterlagen sind auf der Grundlage der Sächsischen Gemeindeordnung aber weiterhin schwer möglich. Es gilt der Öffentlichkeitsgrundsatz in Sitzungen (§ 37 SächsGemO). Der sächsische Gesetzgeber lässt im Unterschied zu anderen Ländern allgemeine Einschränkungen des Öffentlichkeitsgrundsatzes auf Grundlage kommunaler Satzungen nicht zu, sondern nur nach dem Gesetz, wenn das öffentliche Wohl oder berechtigte Interessen Einzelner eine nichtöffentliche Verhandlung erfordern. Dementsprechend ist die Entscheidung, ob und welche personenbezogenen Daten in Unterlagen erscheinen dürfen, jeweils eine Einzelfallent-

scheidung. Die Sächsische Gemeindeordnung schreibt vor, dass der Bürgermeister den Gemeinderat schriftlich mit angemessener Frist einberuft und den Gemeinderatsmitgliedern rechtzeitig die einzelnen Verhandlungsgegenstände mitteilt. Dabei sind die für die Sitzung erforderlichen Unterlagen beizufügen, soweit nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Die Gemeinderäte sollen sich mit Hilfe der Unterlagen mit den Beratungsgegenständen vertraut machen und auf die Sitzung vorbereiten können. Ich empfehle den Gemeinden regelmäßig, bereits bei der Zusammenstellung der Sitzungsunterlagen jeden Personenbezug - soweit dieser nicht erforderlich ist - zu vermeiden. Diese Vorgehensweise bietet neben dem Schutz des Einzelnen den Vorteil, dass Mehrfertigungen solcher Vorlagen ohne Weiteres, d. h. ohne größeren Aufwand, im Sitzungsraum für die Zuhörer und für die Presse bereitgehalten werden können. Auch die Unterlagen, die den Gemeindevertretern selbst für die Beratungen zur Verfügung gestellt werden, dürfen einen Personenbezug nur enthalten, soweit dies erforderlich ist.

In der Praxis wird sich nicht immer vermeiden lassen, dass z. B. Einwendungen gegen Vorhaben den Mitgliedern der Gremien personenbezogen vorzustellen sind, weil anders die Bedenken und die Betroffenheit der einzelnen Einwohner und Einwender nicht beurteilt werden können. Das informationelle Selbstbestimmungsrecht dieser Betroffenen ist in diesen Fällen auch durch die Pflichten der Gemeindevertreter als ehrenamtlich tätige Bürger nach § 19 SächsGemO geschützt. Stadträte sind zur Verschwiegenheit über alle Angelegenheiten verpflichtet, deren Geheimhaltung gesetzlich vorgeschrieben, besonders angeordnet oder ihrer Natur nach erforderlich ist. Ein Gemeinderatsmitglied darf die Kenntnis von geheim zuhaltenden Angelegenheiten nicht unbefugt verwerten. Die Geheimhaltung kann nur aus Gründen des öffentlichen Wohls oder zum Schutz berechtigter Interessen Einzelner angeordnet werden. Zu den berechtigten Belangen Einzelner zählen alle rechtlich geschützten oder anerkannten Interessen, die der Persönlichkeitssphäre zuzurechnen sind, z. B. Personal- oder Grundsteuerangelegenheiten oder allgemein persönliche Umstände, die sich negativ auf die Wertschätzung durch Dritte oder die berufliche Stellung auswirken können (vgl. Menke/Arens, Gemeindeordnung für den Freistaat Sachsen, § 37 Rdnr. 4). Da es für ehrenamtlich Tätige in den Räten nicht immer leicht zu erkennen sein wird, welche Angelegenheiten ihrer Natur nach unter die Verschwiegenheitspflicht fallen, empfiehlt es sich, die Geheimhaltung nach Möglichkeit besonders anzuordnen.

Gegenstand der Verständigungen zwischen mir und der Stadtverwaltung waren letztendlich auch die Bedingungen für eine Veröffentlichung personenbezogener Daten im Ratsinformationssystem der Stadt. Beispielsweise wurde entschieden, dass Einwohner, die sich bei öffentlichen Sitzungen äußern, zukünftig hinsichtlich der Einwilligung zur

Veröffentlichung ihrer personenbezogenen Daten befragt werden sollen. Die Stadtverwaltung sagte in diesem Zusammenhang den Entwurf eines geeigneten Formulars zu, in dem die Einwohner in die Veröffentlichung ihrer personenbezogenen Daten, z. B. des Namens, einzuwilligen in der Lage sind. Die namentliche Nennung sollte danach nur erfolgen, wenn der Betroffene seine Einwilligung erteilt hat.

Bei einer ein halbes Jahr nach meiner Beratung durchgeführten routinemäßigen Kontrolle der Stadtverwaltung zeigte sich, dass die abgestimmten datenschutzrechtlichen Vorgaben eingehalten wurden. Ich hatte die Stadt auch darum gebeten, mir Einwillligungen der Einwohner zu übersenden, deren personenbezogene Daten und die in öffentlichen Sitzungen dargelegten Positionen im Ratsinformationssystem veröffentlicht wurden. Die Erklärungen wurden mir vollständig übersandt und nur in den Fällen, in denen die Betroffenen der Veröffentlichung zugestimmt hatten, wurden die Namen der Betroffenen in den Niederschriften erwähnt.

Das Beispiel der Stadtverwaltung zeigt, dass entgegen häufig geäußerten Behauptungen ein bürgerfreundliches und effektives Ratsinformationssystem und die Beachtung der datenschutzrechtlichen Belange in Einklang gebracht werden können. Ein planmäßiges Vorgehen und die bewusste Berücksichtigung der datenschutzrechtlichen Fragen bei der Ausgestaltung des Ratsinformationssystems sichert die Rechtssicherheit des Internetangebots der Gemeinde ab.

5.5.7 Betrieb von Webcams durch Kommunen

Immer mehr sächsische Städte und Gemeinden stellen den Nutzern ihrer Internetseiten Bilder eigener Webcams zur Verfügung. Marktansichten, Brunnen oder Einkaufsstraßen werden live in das Internet übertragen, damit sich potentielle Gäste oder auch die eigenen Einwohner aus der Ferne ein Bild vom Ort, den touristischen Einrichtungen oder von der aktuellen Wetterlage machen können. Nicht selten sind die Abbildungen zeitlich durch Zeitstempel einzuordnen. Je nach gewählter Einstellung werden die im Internet gezeigten Bilder in bestimmten Zeitabständen, die zwischen wenigen Sekunden und einigen Minuten liegen können, aktualisiert. Zum Teil handelt es sich aber auch um sogenannte „Live-Streams“, d. h. um die ununterbrochene Übertragung von bewegten Bildern in Echtzeit.

Bei den vorgenannten Übertragungen können u. U. neben der aufgenommenen Örtlichkeit auch einzelne Personen erkennbar abgebildet werden. Dies hängt von den Einstellungen und der Bildauflösung der Webcam im Einzelfall ab. In den Fällen, in denen meine Überprüfung ergab, dass die Bilder zumindest personenbeziehbar (§ 3 Abs. 1 SächsDSG) sind, bat ich die Kommunen, unverzüglich sicherzustellen, dass eine Identi-

fizierung von Personen für die Zukunft ausgeschlossen wird. Bei schwenk- und zoombaren Kameras forderte ich zudem, sicherzustellen, dass keine Aufnahmen durch Fenster oder Türen in das Gebäudeinnere möglich sind.

Zum Teil mochten einige Kommunen meine Bitten zunächst nicht nachvollziehen. Grund für meine Forderungen war jedoch, dass jede Überwachung des öffentlichen Raumes mit optisch-elektronischen Einrichtungen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen darstellt. Das gilt auch für die Webcams und deren weltweite Bildübertragungen, auch wenn damit „nur“ in einer örtlichen Öffentlichkeit sich abspielende Geschehnisse und damit „ohnehin“ öffentliche Dinge übermittelt werden. Deshalb bedürfen auch bei Webcams beide Datenverarbeitungsschritte - die Erhebung der Bilddaten und die Übermittlung der Bilddaten an einen unbestimmten Empfängerkreis - einer gesetzlichen Grundlage. Zunächst muss auch der Webcam-Einsatz als Beobachtung öffentlich zugänglicher Räume zur Aufgabenerfüllung der Stelle erforderlich sein (§ 33 Abs. 1 SächsDSG). Keine der um Stellungnahme ersuchten Kommunen konnte mir jedoch die Erforderlichkeit der Datenerhebung durch eine kommunale Webcam zur Aufgabenerfüllung belegen.

Sodann fehlt es an einem gesetzlichen Erlaubnistatbestand für die Übermittlung der personenbezogenen Bilddaten. Auch liegt keine Einwilligung der Betroffenen vor.

Gesetzlich ist zudem eine Übermittlung von personenbezogenen Abbildungen für öffentliche Stellen auch nicht vorgesehen und eine Herstellung einer Zulässigkeit anhand von Einwilligungen ist angesichts des nicht bestimmbaren Personenkreises potentiell Betroffener und der fehlenden Freiwilligkeit ausgeschlossen. Zu beachten ist auch, dass bei dem Präsentieren der Aufnahmen über das Internet, einem weiteren Datenverarbeitungsvorgang, der bei der Überwachung mit herkömmlichen Videokameras in aller Regel fehlt, auch dann schon ein Personenbezug gegeben sein kann, wenn z. B. Internetnutzer die betroffenen Personen anhand ihrer Kleidung, wegen mitgeführter Gegenstände oder wegen eines Fahrzeugs oder eines Kfz-Kennzeichens identifizieren können. Letztendlich können in das Internet eingestellte Abbildungen und Videoabschnitte die Betroffenen unabhängig von dem Zusammenhang persönlichkeitsrechtlich beeinträchtigen. Dabei ist bei einer Übermittlung der Informationen über das Internet die Verbreitung und Nutzung für die Daten verarbeitende Stelle nicht mehr steuerbar. Webcams und die Übertragung im Internet können in der Konsequenz damit auch für die öffentliche Stelle ein unkalkulierbares Risiko darstellen, namentlich dann, wenn Betroffene aufgrund der Veröffentlichungsweise schadensrechtliche Ansprüche geltend machen. Hingegen werden z. B. bloße Panoramabilder einer Stadt, die Ansichten aus großer Entfernung bieten, wiederum datenschutzrechtlich unbedenklich sein.

Im Berichtszeitraum hat eine Reihe von Kommunen den Betrieb ihrer Webcams vollständig eingestellt oder entsprechend meinen Forderungen angepasst. In den verbleibenden Fällen werde ich weiter auf ein gesetzmäßiges Verhalten der Kommunen hinwirken.

5.5.8 Bildaufnahmen des fließenden Verkehrs zur Überwachung von Geschwindigkeit und Sicherheitsabstand

In einem vielbeachteten Beschluss vom 11. August 2009 bescheinigte das Bundesverfassungsgericht einer norddeutschen Ordnungsbehörde die Rechtswidrigkeit der dort praktizierten Videoüberwachung und -aufzeichnung des Straßenverkehrs zum Zweck der Feststellung von Verkehrsverstößen. Bewertet wurde das anlassunabhängige Erfassen des Straßenverkehrs durch Videoaufzeichnungen, die später auf eventuell abgebildete Straftaten oder Ordnungswidrigkeiten hin ausgewertet werden. Das Gericht stellte fest, dass Videoaufzeichnungen des fließenden Verkehrs, die eine Identifizierung des Fahrzeugs sowie des Fahrers ermöglichen, einen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung darstellen. Einschränkungen dieses Rechts bedürfen einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entspricht und verhältnismäßig ist und ohne die ein solcher Eingriff verfassungswidrig ist. Eingriffe aufgrund einer Verwaltungsvorschrift, z. B. eines ministeriellen Erlasses - wie im zugrunde liegenden Fall geschehen - seien unter keinem rechtlichen Aspekt vertretbar und daher willkürlich. Von zentraler Bedeutung war die Feststellung, dass bei einer anlasslosen und permanenten Aufzeichnung des fließenden Verkehrs eine große Zahl sich rechtskonform verhaltender Personen erfasst und diese Bilder gespeichert würden.

Anders zu bewerten sind Fälle, in denen das Aufzeichnungsverfahren erst dann - automatisch oder manuell - eingeleitet wird, nachdem der Verkehrsverstoß bereits festgestellt wurde oder der Fahrzeugführer, etwa während des Hinterherfahrens, bereits auffällig geworden ist und dieses auffällige Fahrverhalten den Anlass für die Aufzeichnung gibt.

Die Entscheidung des Bundesverfassungsgerichts brachte ein gewisses Maß an Unsicherheit bei Rechtsanwendern und Betroffenen mit sich. Gerichtsurteile widersprachen sich, manche Verkehrsrechtsanwälte stellten sämtliche polizeilichen Maßnahmen im Zusammenhang mit Verkehrsüberwachungen infrage und Petenten wandten sich an mich, weil sie „konventionell“ geblitzt wurden. In der Folgezeit verzeichneten die Gerichte eine erhöhte Anzahl von Verfahren bezüglich der Messergebnisse fest installierter Geschwindigkeitsmessgeräte. Einige Juristen interpretierten die verfassungsgerichtliche Entscheidung dahingehend, dass auch „Blitzerfotos“ einen nicht legitimierten Eingriff in das Recht auf informationelle Selbstbestimmung darstellen.

Auch das Bundesverfassungsgericht sah sich in der Folge mit verschiedenen Interpretationen seiner Entscheidung vom 11. August 2009 konfrontiert. Es stellte aber in einem Nichtannahmebeschluss vom 5. Juli 2010 abschließend klar, dass für Bild- und Videoaufnahmen zur Erfassung einer Geschwindigkeitsübertretung § 100h Abs. 1 Satz 1 Nr. 1 StPO i. V. m. § 46 Abs. 1 OWiG - anders als in dem im August 2009 beurteilten Fall einer anlasslosen, dauerhaften Aufzeichnung - die erforderliche gesetzliche Rechtsgrundlage für entsprechende Eingriffe in das Recht auf informationelle Selbstbestimmung bildet:

Nach § 100h StPO sind Aufzeichnungen zu Zwecken der Verfolgung von Straftaten oder Ordnungswidrigkeiten im Straßenverkehr zulässig, soweit ein hinreichender Anfangsverdacht für einen entsprechenden Regelverstoß vorliegt. Nach dieser Vorschrift dürfen ohne Wissen des Betroffenen außerhalb von Wohnungen Bildaufnahmen hergestellt werden.

Dass ausschließlich Bilder von verdächtigen Sachverhalten aufgezeichnet, gespeichert und zur Beweisführung verwendet werden, ist durch die zuständigen Behörden sicherzustellen. Möglich ist dies durch manuelles, persönliches Auslösen und Anhalten der Aufzeichnung oder mittels entsprechender Technik, die automatisch und rechnergestützt Regelverstöße erkennt bzw. prognostiziert und nur die relevanten Sequenzen aufzeichnet. Unzulässig dagegen sind kontinuierliche Videoaufzeichnungen, die zwangsläufig auch unbeteiligte, sich rechtmäßig verhaltende Fahrzeugführer erfassen.

Für die Fälle des gezielten Filmens oder Fotografierens zu schnell fahrender oder zu dicht auffahrender Autofahrer mit stationären oder mobilen Aufzeichnungsgeräten durch Polizei oder Ordnungsbehörde ist der Beschluss des Bundesverfassungsgerichts vom 11. August 2009 also ohne Bedeutung.

Das SMI versicherte mir auf meine Nachfrage, dass in Sachsen zum Zweck der Feststellung von Verkehrsverstößen keine anlasslosen Videoaufzeichnungen angefertigt werden.

5.6 Baurecht; Wohnungswesen

In diesem Berichtszeitraum nicht belegt.

5.7 Statistikwesen

5.7.1 Volkszählung „Zensus 2011“

Die Volkszählung, die unter der Bezeichnung „Zensus 2011“ auf der Grundlage des *Gesetzes über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011 - ZensG*

2011, vom 8. Juli 2009, BGBl. I S. 1781) stattfindet, ist eine von der EU angeordnete Statistik (vgl. § 1 Abs. 3 Nr. 3 ZensG 2011). Das Neue gegenüber früheren Volkszählungen ist, dass die Statistikbehörden die in die Statistik eingehenden Daten weitgehend nicht unmittelbar beim Betroffenen (durch Befragung) erheben, sondern aus Daten, die ohnehin in Verwaltungsbehörden aufgrund von deren Verwaltungshandeln rechtmäßig angefallen und - gespeichert - vorhanden sind. Das ist es, was mit der Bezeichnung der Volkszählung als „registergestützt“ gemeint ist. Direkterhebungen finden nur in Gestalt einer Befragung einer 10 %-igen Stichprobe von Haushalten (§ 7 ZensG 2011) und einer Totalerhebung bei Eigentümern hinsichtlich Wohngebäuden (§ 6 ZensG 2011) statt.

Gegen das Erhebungsprogramm, also den Katalog der abgefragten oder auf andere Weise beschafften - zunächst personenbezogenen - Daten gibt es unter datenschutzrechtlichen Gesichtspunkten gegen das Zensusgesetz 2011 keine Einwände. Der Katalog der Erhebungsmerkmale bei der Haushaltebefragung ist wesentlich weniger umfangreich als derjenige beim sogenannten Mikrozensus, insbesondere werden keine Angaben zu Einkommen oder Vermögen erhoben. Ohnehin sind bis auf das Datum „rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft“ sowie das, ausnahmsweise, ohne Auskunftspflicht erhobene Datum „Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung“ (§ 7 Abs. 4 Nr. 18 und Nr. 19, § 18 Abs. 1 Satz 2 ZensG 2011) alle Erhebungsmerkmale EU-rechtlich vorgeschrieben, und insoweit findet bekanntlich nach der Rechtsprechung des Bundesverfassungsgerichts (zuletzt BVerfG 19. Juli 2011 - 1 BvR 1916/09, NJW 2011, 3428, 3429 Rdnr. 53) eine verfassungsrechtliche Kontrolle am Maßstab des Grundgesetzes in Deutschland faktisch nicht statt.

Allerdings habe ich in einzelnen anderen Punkten Einwände gegen die Art und Weise der Durchführung des Zensus 2011 geltend gemacht. Es handelt sich vor allem um Folgendes:

(1) Der erste Einwand betrifft die vom Freistaat Sachsen, zusammen mit drei anderen Bundesländern, vorgenommene Betrauung von Privat-Unternehmen mit Teilen der Durchführung der Volkszählung (als amtlicher Statistik), vor allem die Übertragung des elektronischen *Einlesens* („Scannens“) der ausgefüllten Erhebungsbögen auf ein Privat-Unternehmen. Dergleichen halte ich, wie schon seit längerem von mir insbesondere auch gegenüber dem SMI erklärt[1], für nach geltendem Recht nicht vom Gesetz erlaubt

[1] Leider hat das SMI in dem mit mir geführten Schriftwechsel sich diesbezüglich in einer Weise geäußert, die geeignet ist, bei unbefangenen Dritten den irrigen Eindruck zu erwecken, dass ich die Aufgabe des von mir, in der Tat, in meinen 4. TB im Jahre 1996, in Abschnitt 5.7.3, dazu eingenommenen gegenteiligen Rechtsstandpunktes nicht schon seit vielen Jahren, nämlich seit 2003, dem SMI, wie auch (seit 2004) Stellen des Bundes sowie der anderen Bundesländer bekanntgegeben hätte. Im 12. TB habe ich meine geänderte Auffassung in Abschnitt 5.7.2 ausführlich dargelegt.

und daher rechtswidrig, weil das insoweit meiner Auffassung nach maßgebliche Bundesstatistikgesetz eine Vorschrift, die eine derartige Fremd-Vergabe von Behördentätigkeit (namentlich „Datenverarbeitung im Auftrag“) erlaubte, nicht enthält.

Diese Auffassung habe ich auch in der Öffentlichkeit mit Nachdruck vertreten. Allerdings wird diese meine Rechtsauffassung, bei der es auf die grundsätzliche Einordnung des Rechtsinstitutes der *Datenverarbeitung im Auftrag* in das System des Datenschutzrechtes ankommt, nicht von allen Landesdatenschutzbeauftragten geteilt.

Zusätzlich habe ich in diesem Zusammenhang gegenüber dem SMI, als dem insoweit weisungsbefugten und verantwortlichen Staatsministerium (§ 3 Abs. 1 Satz 1 SächsStatG), geltend gemacht, dass unabhängig von der Frage, inwieweit das Statistikrecht eine Einschaltung privater Auftragsdatenverarbeiter durch die Statistikbehörden in die Ausführung einer Bundesstatistik erlaubt, die Auswahl des privaten Dienstleisters für den *Druck und Versand* der „personalisierten“, also an die bestimmten Auskunftspflichtigen namentlich adressierten, Erhebungsunterlagen bedenklich gewesen ist: Ich habe die Vergabe der Versendung der Erhebungsbögen an die Deutsche Post AG als eine Verletzung der Pflicht zur sorgfältigen Auswahl des Auftragsdatenverarbeiters angesehen. Diese Sorgfaltspflicht, positiviert etwa in § 7 Abs. 2 Satz 1 SächsDSG, ergibt sich aus dem inneren Grund der datenschutzrechtlichen Privilegierung der Weitergabe an einen Auftragsdatenverarbeiter. Als Auftragsdatenverarbeiter darf nicht herangezogen werden, wer selbst aufgrund seines schon vor der Auftragserteilung nachhaltig betriebenen Geschäftsmodells ein ausgeprägtes Interesse daran hat, gerade diejenigen Daten, die ihm zur Auftragserfüllung überlassen werden, zweckentfremdend selbst für auftragsfremde Zwecke nutzen zu können. Auch wenn der Deutschen Post AG eine solche Zweckentfremdung nach dem mit ihr geschlossenen Vertrag ausdrücklich verboten war, lässt sich die Einhaltung dieser Pflicht, also die vollständige Unterlassung einer Abzweigung der Daten durch Herstellung einer Kopie, in der Praxis nicht kontrollieren, weil sich ein Kopiervorgang - zumindest nach dem gegenwärtigen Stand der Technik - nicht sicher nachweisen lässt. Bekanntlich zählen die Deutsche Post AG selbst oder doch zumindest ihre konzernverbundenen Unternehmen zu den bedeutensten Adressmittlern (Adressvermietern, Listbrokern) in Deutschland, falls sie nicht überhaupt den Spitzenplatz einnehmen. Die Deutsche Post AG hat also ein extremes Interesse daran, ihre Adressdateien mithilfe der ihr aus der Statistik-Durchführung übermittelten Adressdateien (sämtlich[e] Eigentümer von Wohnraum!) zu aktualisieren.

Diesen Gesichtspunkt der sorgfältigen Auswahl des Auftragsdatenverarbeiters im Hinblick auf dessen die Wahrung der Zweckbindung gefährdendes Eigeninteresse habe ich seinerzeit bereits in 6/5.7.5 (1998), auf S. 79, angesprochen.

Im Fall der Auftragsdatenverarbeitung im Hinblick auf die Durchführung amtlicher Statistiken ist in diesem Falle hinzugekommen, dass bei Adressdaten die Gefahr besteht, dass die Daten in den Verwaltungsvollzug gelangen; denn bekanntlich ist die GEZ berechtigt, bei privaten Adresshändlern wie der Deutschen Post AG bzw. deren Konzerntöchtern Adressdaten zu erwerben. Der Rückfluss personenbezogener Daten aus der amtlichen Statistik in den Verwaltungsvollzug - hier der GEZ als öffentlicher Stelle - ist jedoch unter dem Gesichtspunkt der Zweckbindung bekanntlich nach dem Volkszählungsurteil höchst problematisch. (Das Urteil legt sich insoweit nicht vollständig auf ein von Verfassungs wegen bestehendes Verbot fest, aber es stellt höchste Ansprüche an die Klarheit diesbezüglicher gesetzlicher Regelungen - die aber eben vollständig fehlen.)

Was die Auslagerung der *Beleglesung* auf ein - anderes, in Süddeutschland tätiges - Privat-Unternehmen betrifft, von der der Freistaat Thüringen wegen (gerade von mir geäußerter) rechtlicher Bedenken, im Unterschied zu Sachsen, Sachsen-Anhalt und Hessen, vorsorglich Abstand genommen hat, ist in diesen drei Bundesländern zunächst geplant gewesen, die vorgedruckten Briefbögen für die Rücksendung der ausgefüllten Fragebögen (der Gebäude- und Wohnungszählung) in einer Weise zu beschriften, dass nicht erkennbar würde, dass sie postalisch gerade nicht an das betreffende (in der Anschriftenbezeichnung irreführenderweise ausschließlich genannte) Statistische Landesamt, sondern (was den tatsächlichen postalischen Lieferweg betraf) unmittelbar an das private Belegleseunternehmen adressiert waren. Gegen anfänglich heftiges Widerstreben auch des SMI habe ich, wie auch meine Kollegen in Hessen und Sachsen-Anhalt, erreicht, dass die vorgedruckte Angabe des Empfängers der zurückzusendenden Fragebögen korrekt mit „*Beleglesezentrum systemform MediaCard GmbH, 96081 Bamberg*“ angegeben worden ist, mit dem Zusatz *im Auftrag des Statistischen Landesamtes des Freistaates Sachsen*.

Diese Offenlegung des Weges, den die Daten nehmen würden, hat, wie mir vom Statistischen Landesamt im Zusammenhang mit einer Kontrolle mitgeteilt worden ist, immerhin dazu geführt, dass eine große Anzahl der bei der Gebäude- und Wohnungszählung Befragten ihre Fragebögen stattdessen bewusst an das Statistische Landesamt versandt haben, welches dann die betreffenden Unterlagen zu dem Privatunternehmen in Bamberg hat transportieren müssen. Nach Einschätzung des Statistischen Landesamtes hat sich hier der von mir in meinem Internauftritt gegebene Hinweis ausgewirkt, dass selbstverständlich jeder den Umschlag, in dem der Erhebungsbogen zurückzusenden ist, an das Statistische Landesamt des Freistaates Sachsen *umadressieren* könne.

(2) Darüber hinaus habe ich auch Zweifel an der *Verfassungsmäßigkeit* der Übertragung einzelner in der Volkszählung 2011 anfallender Aufgaben für alle Bundesländer auf ein bestimmtes einzelnes Bundesland, wie sie in § 12 Abs. 7 Satz 3 ZensG 2011 vorgesehen

ist. Diese verfassungsrechtlichen Bedenken sind nicht spezifisch datenschutzrechtlicher Natur, sondern folgen aus Grundregeln für die Verteilung der Verwaltungsaufgaben-Zuständigkeit im Bundesstaat; aber eine Verarbeitung personenbezogener Daten durch eine - hier m. E. eben aus verfassungsrechtlichen Gründen - unzuständige Stelle ist immer rechtswidrig, also ein Datenschutzverstoß (vgl. BVerwG 9. März 2005 - 6 C 3/04, NJW 2005, 2330 = DVBl. 2005, 1234 = DöV 2005, 873, sogar im Falle, dass es lediglich an der *instanziellen* Zuständigkeit fehlt).

(3) Außerdem habe ich, zuerst im Zusammenhang mit der parlamentarischen Behandlung des Sächsischen Ausführungsgesetzes zum Zensusgesetz[2], Einwände hinsichtlich der nach dem Gesetz beabsichtigten bleibenden, also fortdauernden, Ortsbezogenheit der Speicherung der im Rahmen der Volkszählung erhobenen Daten geltend gemacht. Dabei geht es um Folgendes: Die Hilfsmerkmale, also Name und Anschrift, müssen, sobald sie nicht mehr benötigt werden, allerspätestens nach vier Jahren (§ 19 Abs. 1 Satz 3 ZensG 2011) restlos beseitigt (gelöscht) werden. Denn wenn die Daten einmal hinreichend auf Vollständigkeit und Plausibilität geprüft sind - was zunächst nur maschinell erfolgt -, dann wird für die statistischen Zwecke jede Information darüber, um welche Person es sich eigentlich bei den Angaben handelt, die gespeichert werden, nicht mehr benötigt - weswegen der Name und die Anschrift eben gelöscht werden müssen. Das entspricht dem Gebot der frühestmöglichen statistikunschädlichen Beseitigung des Personenbezuges, also des Bezuges auf eine erkennbare Person, mithin einer Umgestaltung der statistischen Daten in dem Sinne, dass die einzelnen Datensätze sich zwar jeweils auf eine einzelne existente (genauer: zum Berichtszeitpunkt 9. Mai 2011 [§ 1 Abs. 1 ZensG2011] existent gewesene) einzelne Person beziehen, diese Person jedoch nicht bekannt ist und auch nicht festgestellt werden kann, so dass die Daten folglich nicht mehr im datenschutzrechtlichen Sinne personenbezogen sind. Dieses Gebot der frühestmöglichen statistikunschädlichen Anonymisierung ist wiederum ein Ausfluss des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes.

Aber die geplante Fortdauer der Speicherung von *Blockseitenangaben* (vgl. § 3 Satz 3 Nr. 6 SächsZensGAG) *könnte*, nämlich dann, wenn die Blockseite, d. h. der Abschnitt einer Straßenseite zwischen zwei Straßeneinmündungen, zu klein ist - genauer gesagt: zu wenige Einwohner aufweist -, und die Speicherung von Geokoordinaten (§ 4 Abs. 1 Nr. 8 ZensVorbG 2011[3]) *müsste* (außer bei Hochhäusern) *notwendig* einen fortdauernden Personenbezug herstellen (ermöglichen[4]), der für die Durchführung der Statistik

[2] Gesetz zur Ausführung des Zensusgesetzes 2011 im Freistaat Sachsen (Sächsisches Zensusausführungsgesetz - SächsZensGAG) vom 23. September 2010 (GVBl. S. 254).
[3] Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011 (Zensusvorbereitungsgesetz 2011 - ZensVorbG 2011) vom 8. Dezember 2007 (BGBl. I S. 2808).
[4] Über Dateien, die Geokoordinaten mit etwa einem halben Meter Genauigkeit Anschriften zuordnen und die man ohne Weiteres käuflich erwerben kann.

nicht erforderlich und daher vor dem Verhältnismäßigkeitsgrundsatz nicht zu rechtfertigen ist. Diese Überlegung hat verfassungsrechtliche Qualität, stellt also die Gültigkeit der betreffenden gesetzlichen Vorschriften in Frage.

Diese Fragen einer fortlaufenden Speicherung des Ortsbezuges sind, im Unterschied zur Überlassung der Fragebögen an Privat-Unternehmen zur Digitalisierung nicht ein Problem der Anfangsphase der Durchführung der Direkterhebungen innerhalb der Volkszählung 2011, sondern ein noch in der Zukunft zu klärendes Problem.

Es ist keineswegs ausgeschlossen, dass diese Fragen noch in gerichtlichen Entscheidungen zur Volkszählung eine Rolle spielen werden. Zwar sind bisher gemachte Anträge und Klagen gegen den Zensus 2011 bei den Gerichten gescheitert, aber, soweit bekannt, eben nicht aus im Bereich statistik-datenschutzrechtlicher Überlegungen liegenden Gründen. Auch hat es in der juristischen Fachliteratur nur wenig Kritik gegeben (vgl. Stepputat DöV 2011, 111). Aber es scheint eine nicht ganz geringe Anzahl von Verweigerern zu geben, deren Fälle zu Verfahren vor den Gerichten führen könnten.

Die von mir im Hinblick auf die Durchführung der Volkszählung vorgenommenen Kontrollen behördlicher Abläufe haben in den Erhebungsstellen keine hier erwähnenswerten und im Statistischen Landesamt keine volkszählungsspezifischen grundlegenden Probleme zutage gefördert; die Auswertungen - zusammen mit den betroffenen bzw. zu beteiligenden Behörden, also Statistisches Landesamt und SMI - sind insoweit noch nicht abgeschlossen.

5.7.2 Beteiligung des Sächsischen Datenschutzbeauftragten beim Erlass von Statistiksatzungen nach § 9 Abs. 6 Satz 3 SächsStatG

Eine große Kreisstadt hat folgendes grundsätzliches Problem aufgeworfen:

Nach § 8 Abs. 1 SächsStatG sind Gemeinden ermächtigt, Kommunalstatistiken durch Satzung anzuordnen, bei deren Vorbereitung nach Absatz 3 der Vorschrift der Sächsische Datenschutzbeauftragte zwingend zu beteiligen ist. Die Durchführung von Kommunalstatistiken obliegt nach § 9 Abs. 1 SächsStatG der kommunalen Statistikstelle der Gemeinde. Nach § 9 Abs. 6 SächsStatG dürfen für ausschließlich statistische Zwecke an die kommunale Statistikstelle Daten, die im Geschäftsgang anderer Verwaltungsstellen der Gemeinden angefallen sind, unter bestimmten Voraussetzungen anonymisiert weitergegeben werden, wobei regelmäßige Weitergaben nur aufgrund einer Satzung zulässig sind.

Die Frage lautete nun: Ist der Sächsische Datenschutzbeauftragte auch bei Satzungen nach § 9 Abs. 6 SächsStatG aufgrund § 8 Abs. 3 SächsStatG zu beteiligen?

Der Begründung zum Gesetzentwurf der Staatsregierung zum Sächsischen Statistikgesetz vom 29. Juni 1992 (LT-Drs. 1/2063) ist hierzu nichts zu entnehmen. Zur Frage der Anwendbarkeit des § 8 Abs. 3 SächsStatG im Rahmen der Anordnung von Statistiken nach § 9 Abs. 6 SächsStatG habe ich daher Folgendes mitgeteilt:

Wie § 9 Abs. 6 Satz 4 SächsStatG zu entnehmen ist, sind nach § 9 Abs. 6 Satz 3 SächsStatG durchgeführte Statistiken nicht „Kommunalstatistiken“ im technischen Sinne des § 8 SächsStatG, denn sonst wäre die unmittelbare Verweisung auf § 6 Abs. 6 SächsStatG wegen § 8 Abs. 1 Satz 2, 2. HS SächsStatG überflüssig, ebenso die entsprechende Geltung des § 8 Abs. 2 SächsStatG nach § 9 Abs. 6 Satz 2 SächsStatG. Somit entfällt eine Beteiligung des Sächsischen Datenschutzbeauftragten nach § 8 Abs. 3 SächsStatG.

Offensichtlich ist nach dem Gesetz § 9 Abs. 6 Satz 3 SächsStatG die ausschließliche Ermächtigung, Statistiken dieser Art durch Satzung anzuordnen, § 8 Abs. 1 Satz 2 SächsStatG ist es eben gerade nicht.

Hintergrund für die gesetzlich nicht zwingend vorgeschriebene Beteiligung des Datenschutzbeauftragten in den Fällen des § 9 Abs. 6 Satz 3 SächsStatG dürfte meines Erachtens sein, dass man die Anrufung des Datenschutzbeauftragten hier für entbehrlich hält, da es sich dabei nicht um die Durchführung von sogenannten Primärstatistiken wie nach § 8 Abs. 1 SächsStatG handelt, bei denen die Statistik aus völlig neu erhobenen Daten erstellt wird und wofür die betroffenen Bürger einer direkten Befragung ausgesetzt werden, sondern nur um die Weitergabe bereits in der Gemeindeverwaltung vorhandener Daten im Verwaltungsvollzug.

5.7.3 Nichtanwendbarkeit des Sächsischen Statistikgesetzes auf eine von vornherein vollständig anonymisiert durchgeführte Umfrage

Im Rahmen einer vom SMS beim Statistischen Landesamt in Auftrag gegebenen Evaluation des Sächsischen Landeserziehungsgeldgesetzes haben sich Eltern an mich gewandt, die zur Teilnahme an der Befragung einen Fragebogen erhalten haben. Darin wurden die Anzahl und die Vornamen der Familienmitglieder, Geburtsmonat und Geburtsjahr sowie der Familienstand seitens des Statistischen Landesamts erfragt.

Ich bin bei meiner datenschutzrechtlichen Prüfung zu dem Ergebnis gekommen, dass es sich bei einer solchen Befragung von Eltern durch das Statistische Landesamt zwar um eine Statistik im Rechtssinne, nämlich die Sammlung usw. von Daten über Massenerscheinungen zu Planungszwecken (vgl. § 1 Abs. 1 Satz 1 SächsStatG) handelt, das Sächsische Statistikgesetz jedoch auf Befragungen in dieser Form keine Anwendung findet.

Dies ergibt sich aus Folgendem:

Der Begriff der Einzelangabe im Statistikrecht (§ 1 Abs. 3 SächsStatG) ist weiter als der datenschutzrechtliche Grundbegriff des personenbezogenen Datums nach § 3 Abs. 1 SächsDSG. Das Statistikrecht erfasst immer auch Datenerhebungen mit von vornherein äußerst hohem Anonymisierungsgrad. Unter dem Gesichtspunkt des Grundrechtsschutzes ist es jedoch insoweit nicht erforderlich, Datenerhebungen den Anforderungen des Statistikrechts zu unterwerfen, als es sich um Datenerhebungen handelt, die sich von Anfang an nicht auf eine feststellbare einzelne natürliche oder juristische Person beziehen. Die Beschaffung von Einzelangaben, hinsichtlich deren von vornherein bestehender vollständiger Anonymität irgendwelche Zweifel nicht begründet sind, ist nicht Gegenstand des Statistikrechts. Die Erhebung von Massendaten in der Form der Sofortaggregierung fällt daher nicht unter das Sächsische Statistikgesetz (siehe bereits 5./5.7.3). Denn in einem solchen Fall ist von anfänglicher, d. h. von vornherein bestehender, hinreichender Anonymität der Erhebung von Massenerscheinungen auszugehen, die die Anwendung des Statistikrechts ausschließt.

Eine entsprechende „Ausnahme“ von den Anforderungen des sächsischen Statistikrechts erscheint mir auch bei Umfragen gegeben, wenn wie hier lediglich die Anzahl und die Vornamen der Familienmitglieder, Geburtsmonat und Geburtsjahr sowie der Familienstand seitens des Statistischen Landesamts erhoben werden, so dass auch in diesen Fällen von einer von vornherein bestehenden vollständigen Anonymität der an der Befragung teilnehmenden Eltern und deren Kinder ausgegangen werden kann.

Die im Rahmen einer derart ausgestalteten Befragung erfolgenden Datenerhebungen des Statistischen Landesamts können im Ergebnis nicht als personenbezogen qualifiziert werden, so dass Datenschutzbelange der an der Befragung teilnehmenden Familienmitglieder nicht betroffen sind und es aus Sicht des Datenschutzes in diesem Fall einer gesetzlichen Erlaubnis hierzu nicht bedarf.

5.7.4 Vorsicht bei Datenanforderungen zu Statistikzwecken: Rechtswidrige Datenanforderung des Statistischen Bundesamtes bei sächsischen Hochschulen zwecks Durchführung einer Statistik zu Promotionsverfahren

Der sehr aufmerksame persönliche Referent des Rektors einer kleineren sächsischen Hochschule war zu der Einschätzung gelangt, dass das an alle Hochschulen in Deutschland gerichtete Ansinnen des Statistischen Bundesamtes, ihm - wie es ausdrücklich im Betreff von dessen Schreiben hieß, zum „Aufbau einer Adressdatenbank“, die „alle Professorinnen und Professoren in Deutschland“ umfassen sollte - im Hinblick auf alle an der Hochschule tätigen promotionsberechtigten Lehrkräfte Namen, Institutsbezeich-

nung, Telefonnummer, Anschrift für herkömmliche sowie für E-Post mitzuteilen, doch rechtlich höchst bedenklich sei. Er hat sich deswegen an mich gewandt. Seine Einschätzung ist richtig gewesen.

Der Sachverhalt hat sich folgendermaßen abgespielt:

(1) Im Juni 2010 war das Statistische Bundesamt an die Hochschulen mit Promotionsrecht herangetreten und hatte unter Nennung des erwähnten Zweckes des *Aufbaus einer Adressdatenbank mit allen Professorinnen und Professoren in Deutschland* die betreffenden Daten verlangt. Eine deutliche Aussage darüber, inwieweit die Datenlieferung für die Hochschulen freiwillig sein sollte, hat das betreffende Schreiben nicht enthalten, wenngleich es ganz eindeutig auch keine Auskunftspflicht geltend gemacht hat. Die künftige Beantwortung von Fragen durch die vom Bundesamt im zweiten Arbeitsschritt anzuschreibenden Professoren, die dann Angaben über ihre Doktoranden machen sollten, waren allerdings ausdrücklich als freiwillig gekennzeichnet. Eine Rechtsgrundlage für die Durchführung der in dem Schreiben genannten Promotionsverfahrens-Statistik hatte das Schreiben nicht genannt. Ebenso wenig hatte es sich zu der Frage verhalten, inwieweit die angeschriebenen Hochschulen als an Landes-Recht gebundene Stellen berechtigt sein könnten, die betreffenden Daten an die Statistik-Behörde zu übermitteln. Ende August 2010 habe ich daraufhin an alle Hochschulen mit Promotionsrecht im Freistaat Sachsen die Aufforderung gerichtet, dem Verlangen des Statistischen Bundesamtes nach Übermittlung personenbezogener Daten von Lehrkräften zur Erstellung einer Adressdatenbank zwecks späterer Erhebung von Daten zu Promotionsverfahren nicht stattzugeben sowie auch die - datenschutzrechtlich weniger schwerwiegende und sich anbietende - Beschränkung auf die Daten*nutzung* im Wege der Durchführung eines Adressmittlungsverfahrens zu unterlassen und dies auch im Einzelnen begründet sowie das SMWK und den BfDI unterrichtet.

(2) Die Begründung, warum es keine Rechtsvorschrift gab (und gibt), die es der Hochschule erlaubt hätte, dem Statistischen Bundesamt für den Zweck des Aufbaus einer derartigen Adressdatenbank bzw. die Durchführung einer solchen Promotionsverfahrens-Statistik personenbezogene Daten der an der Hochschule tätigen haupt- und nebenberuflichen Professoren (ohne deren Mitwirkung) zu übermitteln, und damit dafür, dass eine solche Datenübermittlung durch die Hochschule an das Statistische Bundesamt wie auch eine Datennutzung zugunsten des Erhebungsvorhabens des Statistischen Bundesamtes rechtswidrig gewesen wäre, ergab sich im Einzelnen aus Folgendem: Die Hochschule betreffend müsste sich eine entsprechende Nutzungs- und Übermittlungsbefugnis aus § 14 Abs. 1 SächsHSG ergeben, da das Sächsische Hochschulgesetz eine namentlich auch gegenüber § 37 SächsDSG (und zumindest bei beamteten Hochschullehrern sicherlich auch gegenüber § 32 BDSG) abschließende Regelung darstellt. Der in § 14

Abs. 1 Satz 1 SächsHSG abschließend bestimmte Aufgabenkatalog umfasst eine Mitwirkung der Hochschule am Aufbau einer Adressdatenbank durch das Statistische Bundesamt zur Durchführung einer entsprechenden freiwilligen Befragung sächsischer Hochschulprofessoren über deren Doktoranden *nicht*. (Auf das Fehlen einer Rechtsverordnung nach § 14 Abs. 3 SächsHSG ist es daher nicht angekommen.)

Es war und ist auch nicht ersichtlich, dass das Bundes-Statistikrecht eine Pflicht der Hochschulen, die gewünschte Datennutzung und Datenübermittlung vorzunehmen, enthielte (anders ausgedrückt: es gibt im Bundesrecht keine Vorschrift, die dem neuen § 4 Abs. 2 Satz 3 StipG, BGBl. I 2010 S. 957, entspräche).

Auch die bloße Datennutzung, auf die sich die Datenverarbeitung durch die Hochschule im Falle der Durchführung eines bloßen Adressmittlungsverfahrens beschränkt hätte, fällt unter den Begriff der Verarbeitung im Sinne des § 14 Abs. 1 SächsHSG.

(3) Ungefähr zur selben Zeit hat das Statistische Bundesamt an - zumindest sächsische - Hochschulen ein weiteres Schreiben in der Angelegenheit gerichtet. Dieses Schreiben war an Hochschulen gerichtet, die, offenbar schon vor meiner diesbezüglichen Unterlassens-Aufforderung, das Datenverlangen kritisch gesehen und das Statistische Bundesamt auf das sogenannte Adressmittlungsverfahren verwiesen hatten, die also das Datenanforderungsschreiben der Behörde an die Dozenten weitergegeben und somit die Datenverarbeitung auf eine *Nutzung* von Lehrkräftedaten durch die Hochschule beschränkt und damit die Daten*übermittlung* (sc. der Dozentendaten an das Statistische Bundesamt) abgelehnt hatten. In diesem Schreiben hat das Statistische Bundesamt zum ersten Mal eine Rechtsgrundlage für die von ihm betriebene Datenerhebung angegeben, nämlich § 7 Abs. 1 BStatG, die Befragung als insgesamt freiwillig bezeichnet und das BMBF als Auftraggeber genannt sowie die Möglichkeit der Einschaltung des jeweiligen Statistischen Landesamtes (vgl. § 7 Abs. 3 BStatG) erwähnt. (Das Statistische Landesamt hatte die Beteiligung an der Durchführung der Statistik - klugerweise - abgelehnt.)

(4) Hochschulen, die überhaupt nicht auf das Schreiben vom Juni reagiert hatten, haben Ende August ein anderes Schreiben des Statistischen Bundesamts bekommen, welches neben § 7 Abs. 1 BStatG als Rechtsgrundlage *für die Abfrage und den Aufbau einer Adressdatenbank der Professoren* § 6 Abs. 1 Nr. 1 BStatG genannt und hilfsweise angeboten hat, sich auf eine Adressmittlung durch die Hochschule einzulassen, sowie erklärt hat, höchst hilfsweise davon auszugehen, dass die Hochschule damit einverstanden sei, dass das Statistische Bundesamt ersatzweise sich die Namen und die Anschriften der Lehrkräfte aus öffentlich zugänglichen Quellen beschaffen werde (dass der letzteren Bemerkung rechtliche Vorstellungen zugrunde liegen könnten, die auch nur ansatzweise

mit geltendem Recht vereinbar sein könnten, hat ohnehin als ausgeschlossen gelten können!).

Beide Varianten der Schreiben vom Ende August 2010 haben zudem Angaben über die beabsichtigte Erhebung von Daten durch das Statistische Bundesamt bei den Lehrkräften gemacht: Es solle zu jedem einzelnen Doktoranden ein Datensatz mit *sozio-demografischen Merkmalen, dem Studienfach, dem Promotionsbeginn, der Promotionsart und dem vorhandenen Hochschulabschluss*, erhoben werden, sowie lehrkraftbezogen die Anzahl der von dem betreffenden Hochschullehrer betreuten Doktoranden.

(5) Nachdem dem Statistischem Bundesamt bekannt geworden war, dass ich mitgeteilt hatte, dass die sächsischen Hochschulen nach Landesrecht nicht befugt seien, die betreffenden Daten zu übermitteln oder auch nur für die Durchführung eines Adressmittlungsverfahrens zu nutzen, hat das Statistische Bundesamt mich dann im Dezember 2010 angeschrieben. Dabei hat die Behörde die Erhebung auf „§ 7“ - ohne Absatz-Angabe - BStatG gestützt und erläutert, zunächst bei den Professoren bezogen auf diese die Anzahl der von ihnen betreuten Doktoranden, deren Promotionsart sowie deren Geschlecht zu erheben. Daran angeschlossen solle eine weitere auf § 7 BStatG zu stützende Erhebung bei den einzelnen Doktoranden stattfinden, wobei das Schreiben nichts darüber ausgesagt hat, in welcher Weise das Statistische Bundesamt an die einzelnen Doktoranden heranzutreten plante und inwieweit es dabei unmittelbare, natürliche Identifikatoren (der Doktoranden) als Hilfsmerkmale zu erheben gedachte. Dem Schreiben des Statistischen Bundesamtes war in keiner Weise zu entnehmen, dass die Zulässigkeitsvoraussetzungen des § 7 Abs. 1 BStatG erfüllt sein könnten.

(6) Ich habe daraufhin dem Statistischen Bundesamt erwidert, dass gänzlich unabhängig davon, inwieweit die Erhebungs- und Weiterverarbeitungs-Handlungen des Statistischen Bundesamtes insoweit (nach Bundesrecht) zulässig seien, es auf der Seite der Hochschulverwaltungen und der Hochschul-Lehrkräfte einer Daten-Nutzungs- und Daten-Übermittlungsbefugnis nach Landesrecht bedürfe, für die Beurteilung dieser Rechtsfrage für Sachsen meine Behörde zuständig sei und dass das Bundesamt mir mitteilen möge, wenn es von mir die diesbezügliche Begründung (der Rechtswidrigkeit der vom Amt gewünschten landesrechtlich zu beurteilenden Verarbeitungshandlungen) erfahren wolle; für eine Änderung der von mir den sächsischen Hochschulen mitgeteilten Rechtsauffassung biete sein Schreiben keine Veranlassung. Da das Amt mich aber angeschrieben hatte, erlaubte ich mir - und zwar aus Zuständigkeitsgründen für das Statistische Bundesamt völlig unmaßgeblich! - mich auch zu dem Versuch des Statistischen Bundesamtes zu äußern, die Statistik, die es durchzuführen sich anschicke, auf eine Rechtsgrundlage im Bundes-Statistikrecht zu stützen: Das Amt sehe die Erlaubnisgrundlage seiner Statistik anscheinend im Absatz 1 des von ihm genannten § 7 BStatG.

Jedoch gehe aus keinem der mir vorliegenden Schreiben des Amtes hervor, inwiefern Auslöser der Statistik, wie von der Vorschrift gefordert, ein *kurzfristig auftretender Datenbedarf* sei und inwiefern dieser Datenbedarf im Hinblick auf die *Vorbereitung und Begründung einer anstehenden Entscheidung einer obersten Bundesbehörde* bestehe. Namentlich habe das Amt nicht angegeben, um welche Entscheidung welcher obersten Bundesbehörde es sich handeln könnte und inwieweit die zu erhebenden Daten dafür tatsächlich *benötigt* würden, also *zumindest nützlich* wären. Zu bedenken sei ja immerhin, dass der Bund keine Zuständigkeit im Promotions-Recht habe. Wenn sich das Statistische Bundesamt demgegenüber auf den Bedarf für *internationale Bildungsberichterstattung* (wohl als bundes-staatliche Aufgabe begriffen) und auf allgemeinen *gesellschaftlichen Wissensbedarf* berufe, so sei dem auch nicht ansatzweise eine Erfüllung der Zulässigkeitsvoraussetzungen des § 7 Abs. 1 BStatG zu entnehmen. Das einzige Tatbestandsmerkmal des § 7 Abs. 1 BStatG, dessen Erfüllung man den Angaben der Behörde bisher entnehmen könne, sei die Anforderung durch eine oberste Bundesbehörde, was jedoch für die rechtliche Zulässigkeit des Handelns des Statistischen Bundesamts entschieden zu wenig sei. Mithin handele das Amt insoweit soweit erkennbar rechtswidrig: Es greife in das Grundrecht auf informationelle Selbstbestimmung ein, obwohl es die nach Verfassungsrecht erforderliche gesetzliche Ermächtigung dafür offenbar nicht habe.

(7) Nachdem mir dann eine sächsische Hochschule ein Schreiben der Hochschulrektorenkonferenz (genau: Konferenz der Rektoren und Präsidenten der Hochschulen in der Bundesrepublik Deutschland) zugänglich gemacht hatte, in dem diese „die Rektorinnen und Rektoren, Präsidentinnen und Präsidenten der deutschen Hochschulen mit Promotionsrecht“ aufgefordert hatte, die Promotionsverfahrens-Statistik des Statistischen Bundesamtes zu unterstützen, habe ich die Hochschulrektorenkonferenz gebeten, bei derartigen Unterstützungsaufrufen in Zukunft den Vorbehalt einer landesrechtlichen Erlaubtheit der betreffenden Verarbeitungshandlungen zu erwähnen, weil die Hochschulleitungen sonst juristisch verunsichert, ja fehlgeleitet werden könnten. Ergänzt habe ich diese Bitte um die Mitteilung, dass ich inzwischen bei der insoweit zuständigen Verwaltungsbehörde nach § 36 Abs. 1 Nr. 2 Buchst. b OWiG, dem BMI, eine Anzeige wegen einer mutmaßlichen Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG erstattet hätte, was ich mit Schreiben vom 6. Januar 2011 kurz zuvor getan hatte: Meiner Auffassung nach ist von Bediensteten des Bundesamtes für Statistik der Tatbestand des § 43 Abs. 2 Nr. 1 BDSG erfüllt worden, insofern das Statistische Bundesamt (a) Daten, die nicht allgemein zugänglich waren, erhoben und (weiter-)verarbeitet hat, diese Daten (b) nicht nur statistische Einzelangaben im Sinne des Statistikrechtes, sondern auch personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes, also des allgemeinen Datenschutzrechtes, gewesen sind und außerdem (c) die Erhebungs-Aktion (Durch-

führung der Promotionsverfahrens-Statistik) nicht von einer gesetzlichen Ermächtigung zur Durchführung dieser Statistik gedeckt gewesen ist. Die Durchführung der Bundesstatistik war daher unzulässig, weil für amtliche Statistiken wegen des grundsätzlich nie auszuschließenden Personenbezuges der Vorbehalt des Gesetzes gilt, ganz abgesehen von dem durch das Bundesstatistikgesetz selbst aufgestellten Gesetzeserfordernis (vgl. implizit § 5 Abs. 2 Satz 3, Abs. 4 Satz 2, § 7 Abs. 1, § 15 Abs. 1 Satz 1 BStatG).

Hinzugekommen ist jedoch eine *Beteiligungs-Verantwortlichkeit* der Bediensteten des Statistischen Bundesamtes, und zwar gemäß § 14 OWiG, nämlich insoweit, als das Amt an landesrecht gebundene Stellen aufgefordert hat (Anstiftung), Datenverarbeitungshandlungen durchzuführen, die rechtswidrig gewesen sind bzw. wären: Insofern nämlich, als das Statistische Bundesamt an Landesrecht gebundene sächsische Stellen - und sicherlich auch Stellen in anderen Bundesländern - durch entsprechende Aufforderung im vollen Wissen und Wollen der *Tatumstände* dazu veranlasst hat, nach Landesrecht rechtswidrig Daten von Professoren zu nutzen, in einzelnen Fällen auch zu übermitteln: Dadurch hat sich das Statistische Bundesamt der Anstiftung zu einer Ordnungswidrigkeit nach § 38 Abs. 1 Nr. 1 Buchst. a SächsDSG schuldig gemacht; die Rechtswidrigkeit der Datennutzung und gegebenenfalls -übermittlung durch die angestifteten sächsischen Stellen habe ich oben dargelegt. (Derartige Anstifter-Verantwortlichkeit statuiert übrigens auch das Datenschutzrecht selbst durch die in ihm generell geltende Verantwortungsverteilung bei der auf Ersuchen stattfindenden Übermittlung, vgl. § 15 Abs. 2 Satz 2 BDSG, § 14 Abs. 2 Satz 2 SächsDSG.) Das Statistische Bundesamt hätte allenfalls einen vermeidbaren Verbotsirrtum hinsichtlich der landesrechtlichen Unzulässigkeit der von ihm verlangten Verarbeitungshandlungen geltend machen können. *Bei einer Durchführung einer Statistik ohne Auskunftspflicht ist es jedoch Pflicht der die Statistik durchführenden Statistikbehörde, die von ihr um Auskünfte angegangenen Stellen darauf hinzuweisen, dass diese selbstverständlich eigenständig zu prüfen haben, inwieweit sie zur Erteilung der Auskünfte berechtigt sind*. Das ist in diesem Falle nicht geschehen. Das Statistische Bundesamt hat den von ihm angeschriebenen Hochschulbehörden nicht einmal eine Rechtsgrundlage seiner eigenen Datenerhebungstätigkeit genannt. Es hat die ganze Aktion damit als eine nicht rechtsgebundene erscheinen lassen - die Hochschulen haben gar nicht erst auf den Gedanken kommen sollen, dergleichen müsse rechtlich betrachtet werden. Deswegen lag der Verdacht auf der Hand, dass bundesweit in der Regel die Hochschulen ohne Prüfung ihrer datenschutzrechtlichen Berechtigung zur Datennutzung und Datenübermittlung Daten geliefert haben, und ferner, dass im Anschluss daran auch um Datennutzung und Datenübermittlung angegangene einzelne Hochschullehrer entsprechend rechtswidrig gehandelt haben. Bei allem, was erkennbar gewesen ist, ist es dem Statistischen Bundesamt völlig gleichgültig gewesen,

ob die Datenbereitstellung durch die Länderstellung (Hochschulverwaltungen, Hochschullehrer) - nach Landesrecht - rechtmäßig sein würde oder aber nicht.

(8) Die Reaktion des BMI, das Vorliegen einer Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG, begangen durch eine der Aufsicht des BMI als oberster Statistik-Behörde des Bundes unterliegende Behörde (§ 2 Abs. 1 BStatG), zu verneinen, ist dann nicht unerwartet gekommen: Dass, wie vom BMI geltend gemacht, sämtliche von den Hochschulen übermittelten Daten öffentlich zugänglich gewesen sein könnten, hatte ich von vornherein eingeräumt; dies galt jedoch nicht für die bei den Lehrkräften dann erhobenen Daten. Insoweit hat sich das BMI dann darauf berufen, die nach § 7 Abs. 1 BStatG erforderliche *Entscheidung einer obersten Bundesbehörde* sei der im Frühjahr 2013 (!) durch das Bundeskabinett zu verabschiedende „Bundesbericht wissenschaftlicher Nachwuchs", der *als Grundlage dafür dienen solle, künftig Fördermaßnahmen für den wissenschaftlichen Nachwuchs zielgenauer zu ergreifen*. Abgesehen von der Frage, inwieweit insoweit überhaupt eine Bundes-Zuständigkeit gegeben ist, ist ein *Bericht* keine *Entscheidung*. In welchem zeitlichen Abstand zur Verabschiedung des Berichtes dann eine Entscheidung über Maßnahmen fallen soll - darüber hat die Stellungnahme des BMI wohlweislich geschwiegen. Bei diesen Angaben des BMI zum Zeitplan ist ohnehin klar, dass es sich nicht im Juni 2010 um den, wie § 7 Abs. 1 BStatG voraussetzt, *kurzfristig auftretenden Datenbedarf für Zwecke der Vorbereitung und Begründung der Entscheidung* handelt, wenn die Entscheidung erst in einem unbestimmten zeitlichen Abstand nach dem Frühjahr 2013 getroffen werden soll. Es liegt auf der Hand: Es hat sich um einen Fall von - zurzeit ja vieldiskutierter - Vermeidung der Befassung des Parlamentes (hier: als Gesetzgebers) gehandelt.

Auf die Beteiligten-Verantwortlichkeit, als zweite Variante der Tatbestands-Verwirklichung durch das Statistische Bundesamt, ist das BMI vorsorglich überhaupt nicht eingegangen; anscheinend hat es gemeint, mit dem in die Schreiben an die Hochschullehrer aufgenommenen Hinweise auf die Freiwilligkeit entfalle die Anstifterverantwortlichkeit. Das ist sicherlich unzutreffend: Der klassische Anstifter behauptet bekanntlich ja nicht, dass derjenige, den er anstiftet, verpflichtet sei, das zu tun, wozu er ihn auffordert; vielmehr beschränkt er sich schlicht darauf, dazu aufzufordern, die betreffende Handlung vorzunehmen, und braucht dazu noch nicht einmal zu behaupten, sie sei rechtmäßig.

(9) *Ergebnis*: Für Sachsen hat das Schlimmste wohl verhindert werden können; vom Statistischen Bundesamt ist in der Angelegenheit rechtmäßiges Verhalten nicht zu erwarten, weswegen die sächsischen Hochschulen und die sächsischen Hochschullehrer insoweit weiter auf der Hut sein müssen. Und generell gilt: Das Vertrauen in die amtliche Statistik wird auf diese Weise stark beeinträchtigt. Man kann daraus in Abän-

derung einer bekannten Maxime zum Thema Statistik formulieren: Beteilige dich als Behörde als Datenlieferant für eine Statistik jedenfalls des Statistischen Bundesamtes an dieser Statistik nur, wenn du gründlich geprüft hast, ob du das auch darfst.

5.8 Archivwesen

5.8.1 Ansturm auf im Kreisarchiv aufbewahrte Unterlagen zur Tätigkeit eines prominenten Landespolitikers im Rat des Kreises 1989/1990: Ein Lehrstück

Gemeinhin meint man, ein Archiv sei eine beschaulich tätige Behörde, an der die größeren Ereignisse der Politik vorbeigingen. Dass es auch anders sein kann und dabei (wenn nicht gerade ein Archivgebäude einstürzt) um datenschutzrechtliche Fragen geht, zeigt folgender Fall: Am 19. Juni 2009 - es war Landtagswahlkampf in Sachsen - meldete eine überregionale Tageszeitung im Zusammenhang mit der Berichterstattung über eine noch im Dezember 1989 durch den Rat des Kreises vorgenommene Enteignung eines Hauses in Kamenz im Hinblick auf die Zugehörigkeit des damaligen Ministerpräsidenten des Freistaates Sachsen zum seinerzeitigen Rat des Kreises Kamenz, dass die Staatskanzlei im Herbst des Vorjahres diesbezüglich im Kamenzer Kreisarchiv recherchiert habe, dass sie vom Landratsamt unterrichtet worden sei, als danach auch der Verfasser des Zeitungsberichtes das Archiv benutzt habe, und dass im Archiv Unterlagen zu dem Enteignungsvorgang „verschwunden“ seien, und zwar erst seit Kurzem.

Ich habe mich daraufhin mit entsprechenden Fragen an die SK sowie an das LRA des Landkreises Bautzen, zu dessen Kreisarchiv das alte Kamenzer Kreisarchiv seit der letzten Landkreis-Reform gehört, gewandt. Unabhängig davon erfuhr ich, dass auch ein Landtagsabgeordneter und Buchautor im Kreisarchiv Kamenz Nachforschungen zu der Tätigkeit des Ministerpräsidenten als Mitglied des Rates des Kreises Kamenz in den Jahren 1989/1990 angestellt hatte, ebenso wie wohl ein Journalist eines Nachrichtenmagazins. Alsbald meldete die sächsische Presse, ich ginge der Frage nach, *ob beim Umgang mit Archivmaterial alles mit rechten Dingen zugegangen sei*.

Ich habe, und zwar sehr kurzfristig, daraufhin in der Tat aufwendig sämtliche infrage stehenden Benutzungsvorgänge, genauer gesagt die Einsichtsgewährung und die Überlassung von Ablichtungen von Unterlagen durch Bedienstete des Archivs, einschließlich der betreffenden Weisungsvorgänge im LRA, und die Datenerhebung durch die SK, einschließlich der dortigen diesbezüglichen Weisungsvorgänge, sowie die Übermittlung von Benutzungsgewährungsvorgangs-Daten an die SK und an sonstige Dritte untersucht: Im Hinblick auf die Personenbezogenheit des Inhaltes der dabei zugänglich gemachten Archiv-Unterlagen sowie der begleitenden Informationserteilung, und zwar mittels Aktenkontrolle sowie schriftlicher und mündlicher Befragungen.

Die Benutzungsvorgänge, so hat sich herausgestellt, hatten schon im September 2008 eingesetzt, und auch während der Zeit meiner Kontrolle haben weitere Medienvertreter Benutzungsanträge gestellt.

(1) Das Ergebnis hinsichtlich der Verarbeitung personenbezogener Daten durch die SK im Zusammenhang mit Einsichtnahmen in das Kreisarchiv Kamenz ist Folgendes gewesen:

(1.1) Die SK hat an drei Tagen im November 2008 durch einen damaligen Mitarbeiter ihrer Pressestelle aufgrund eines von ihr gestellten Benutzungsantrages im Kreisarchiv Einsicht in Unterlagen (vor allem Sitzungsprotokolle) des Rates des Kreises des DDR-Landkreises Kamenz aus den Jahren 1987 bis 1989 genommen. Dabei ist in einigen Fällen seitens der Archivbehörde des Landkreises versäumt worden, vereinzelt in den Unterlagen vorkommende Daten zu Privatpersonen von der Akteneinsicht, in geringerem Umfang auch von der dieser folgenden Überlassung von Ablichtungen (an die SK), auszunehmen.

Insoweit bin ich zu der Einschätzung gelangt, dass die SK faktisch das LRA im Ergebnis unter einen Zeitdruck gesetzt hat, der es diesem unmöglich gemacht hat, rechtzeitig vor Beginn der begehrten Akteneinsicht die in den Unterlagen enthaltenen, von der SK gar nicht benötigten Private betreffenden Daten der Einsichtnahme zu entziehen, wie es datenschutzrechtlich geboten gewesen wäre; ich bin auch zu der Meinung gelangt, dass die SK diese hätte erkennen können und berücksichtigen müssen.

Die SK hat sich damit verteidigt, *höchstens einen Hinweis auf die besondere Eilbedürftigkeit* gegeben zu haben. Meiner Auffassung nach verhält es sich insofern so: Die hochgestellte, „mächtige“ SK muss in derartigen Fällen mit übertriebener Eilfertigkeit des LRA rechnen und sich entsprechend zurückhaltend äußern, das „kleine“ LRA darf nicht aus Eilfertigkeit bzw. Aufregung die rechtlich gebotenen Vorkehrungen bei der Durchführung des Benutzungsvorganges vernachlässigen.

(1.2) Von diesen vereinzelten, der archivrechtlichen Schutzfrist (des § 10 Abs. 1 Satz 3 und 4 SächsArchivG) unterliegenden Daten abgesehen hat die SK zu keinerlei Daten Zugang erhalten, zu denen nicht jedermann - und nicht nur der betreffende Politiker oder andere ehemalige Mitglieder des Rates des Kreises Kamenz als Betroffene - Zugang gehabt hätte. Grund für Letzteres ist, dass es sich um Daten über Amtsträger in Ausübung ihres Amtes gehandelt hat, vgl. § 10 Abs. 2 Satz 3 SächsArchivG. (Dies hat übrigens auch Angaben über die Weiterbildung, namentlich auch die „marxistisch-leninistische Weiterbildung der Mitarbeiter des Staatsapparates“ umfasst, und von denen in zwei Beschlüssen des Rates des Kreises die Rede gewesen ist.)

Weitergehende Folgen hat diese Übereilung jedoch nicht gehabt: Bei der Auswertung des erhaltenen Archivgutes in der Staatskanzlei sind die rechtswidrig übermittelten Daten nicht verwendet worden, zu einer Perpetuierung des Datenschutzverstoßes ist es nicht gekommen.

(1.3) Es ist ein nicht der SK anzulastender Datenschutzverstoß gewesen, dass deren Mitarbeiter im Benutzerbuch des Archivs, in das er sich einzutragen aufgefordert worden war, ohne nennenswerten Aufwand Daten über vorangegangene einschlägige Archivbenutzungsvorgänge hat zur Kenntnis nehmen können, die ihm fast haben ins Auge springen müssen.

(1.4) Eindeutig hat sich aus den von mir getroffenen Feststellungen ergeben, dass die SK nicht darauf hingewirkt hat, dass das LRA sie im Juni 2009 über einen nachfolgenden, denselben Unterlagenkomplex betreffenden Benutzungsvorgang unterrichtet hat. Vielmehr hat die Pressestelle der SK, soweit ich habe feststellen können, lediglich die ihr unaufgefordert zugesandten Informationen entgegengenommen.

(1.5) Folgendes hätte in der SK im Zusammenhang mit der Benutzung des Kreisarchivs in dieser Angelegenheit besser gemacht werden müssen bzw. können:

(1.5.1) Die SK hat ihr Archivbenutzungsbegehren durch den Anruf des Pressesprechers gegenüber dem Landrat geäußert, dieser hat daraufhin eine (pauschale) Benutzungserlaubnis erteilt. Auch wenn eine derartige Benutzung des Kreisarchivs durch die SK an und für sich rechtlich zulässig gewesen ist, ist doch der Umfang der erteilten Erlaubnis rechtswidrig gewesen. Dabei hätte eine von Anfang an *schriftliche* Anmeldung des Archivbenutzungsbegehrens die eingetretenen Risiken archiv- bzw. datenschutzrechtswidrigen Handelns, die sich dann im Handeln des LRA verwirklicht haben, ganz erheblich verringert. Der fernmündliche unmittelbare Kontakt eines hochrangigen, mit Verwaltungsvorgängen jedoch wenig vertrauten Bediensteten der SK mit der mit dem Archivrecht nicht vertrauten Spitze der Landkreisverwaltung, und zwar mit der geäußerten und durchgesetzten Erwartung, der SK-Bedienstete könne in etwa zwei bis drei Stunden mit der umfangreichen Archivbenutzung beginnen (so jedenfalls die Angabe des LRA mir gegenüber), hat den Vorgang in einer Weise zu einem faktisch - nicht rechtlich! - außerordentlichen Vorgang gemacht, die dann dazu geführt hat, dass die Angelegenheit aufseiten des LRA, als kommunaler Archivbehörde, nicht mit der üblichen und für die Rechtmäßigkeit des Ablaufes erforderlichen Geschäftsmäßigkeit betrieben worden ist: Dies ist die wesentliche Ursache dafür gewesen, dass dort archiv-datenschutzrechtliche Fehler gemacht, nämlich rechtswidrig personenbezogene Daten (an die SK) übermittelt worden sind.

(1.5.2) Nützlich - wenn auch nicht vorgeschrieben - für einen insgesamt rechtmäßigen Archivbenutzungsvorgang wäre es gewesen, wenn die SK dem LRA gegenüber bei der (formlosen) Kundgabe des Benutzungsbegehrens Angaben zur archivrechtlichen Einordnung der gewünschten Archivunterlageninhalte gemacht, also insbesondere darauf hingewiesen hätte, dass es ihr ausschließlich um Daten über Amtsträger, einschließlich der Tätigkeit im Rahmen der in § 4 Abs. 2 Satz 3 SächsArchivG genannten DDR-Stellen, ging. Denn erst durch den Einsicht nehmenden Mitarbeiter der SK ist auch darauf hingewiesen worden, dass das Interesse sich auf Angaben zur Tätigkeit des Ministerpräsidenten in seiner Tätigkeit als Mitglied des Rates des Kreises gerichtet hat.

(1.5.3) Im Hinblick darauf habe ich der SK sehr dazu geraten, auch im Bereich der Pressestelle für derartige Tätigkeiten, also insbesondere Inanspruchnahme anderer Behörden außerhalb der eigentlichen Landesverwaltung, von vornherein für eine ausreichende Dokumentation der Verwaltungsvorgänge zu sorgen. Im Nachgang ist ein ordnungsgemäßer Verwaltungsvorgang in der SK angelegt worden; sofern personenbezogene Daten verarbeitet werden, ist dies unerlässlich.

(2) Der genannte, in der Öffentlichkeit laut gewordene Vorwurf der *Aktenmanipulation* hat sich bei der Durchsicht der Unterlagen und der Angaben über die Benutzungsvorgänge *nicht* bestätigt; allerdings hat eine archivfachlich gut begründete und in den Unterlagen, ohne weiteres nachverfolgbare Änderung der Aktenzuordnung eines einzelnen Akten-Blattes, mit einem bestimmten Beschluss des Rates des Kreises, die Grundlage für Fehlschlüsse auf Benutzerseite gelegt.

Die in der Öffentlichkeit geäußerte Befürchtung, womöglich könne es im Kamenzer Kreisarchiv zugehen wir unter dem *sprichwörtlichen Sofa bei Hempels*, hat sich nicht bestätigt. Die unterschiedlichen Eindrücke zum Zustand der Akten haben sich durch den unterschiedlichen Kenntnisstand der Beteiligten erklären lassen.

(3) Ein datenschutzrechtliches Fehlverhalten von größerem Gewicht ist auf Seiten des LRA festzustellen gewesen. Das LRA ist noch so gerade eben um eine förmliche Beanstandung durch mich herumgekommen:

(3.1) Zunächst einmal war der vom Landrat persönlich unterzeichnete, ein Aktenzeichen nicht aufweisende Genehmigungs-Bescheid vom 24. November 2008, 12:10 Uhr mit dem Wortlaut

> „*Hiermit genehmige ich den Mitarbeitern der Sächsischen Staatskanzlei uneingeschränkte Akteneinsicht in den Bestand unseres Archivs*."

eine gegen das archivdatenschutzrechtliche Übermittlungsverbot des § 10 Abs. 1 Satz 3 (mit Satz 4) SächsArchivG verstoßende Übermittlungserlaubnis, und zwar aus folgen-

den Gründen: Seinem Wortlaut nach besagte der Bescheid, dass in bestimmtem Zusammenhang von der SK entsandten Bediensteten zumindest im Bereich der den Beteiligten bekannten Thematik sämtliche dafür in Frage kommenden Unterlagen des Archivs im vollen inhaltlichen Umfang, also betreffend namentlich auch alle in ihnen enthaltenen personenbezogenen Daten offengelegt würden.

Mit diesem Inhalt war der Bescheid nicht nur offenkundig rechtswidrig, insofern er personenbezogene Daten, die unter die Schutzfrist des § 10 Abs. 1 Satz 3 (mit Satz 4) SächsArchivG fielen, von der Offenlegung (Übermittlung) nicht ausnahm; vor allem hat er eine Anwendung (der archivdatenschutzrechtlichen Vorschriften) des maßgeblichen Sächsischen Archivgesetzes auch nicht im Ansatz erkennen lassen und hat somit gegen eine datenschutzrechtliche, dem Persönlichkeitsrechtsschutz dienende Vorschrift verstoßen.

Zwar war zugunsten des Landkreises zu berücksichtigen, dass der Landrat sich durch eine sehr kurzfristige fernmündliche Ankündigung des Archivbenutzungsverlangens durch einen hochrangigen Bediensteten der SK, soweit erkennbar mit der geäußerten und eben auch durchgesetzten Erwartung, der SK-Bedienstete könne in etwa zwei bis drei Stunden mit einer umfangreichen Archivbenutzung beginnen, unter Druck gesetzt gesehen hat, was dann wesentlich dazu beigetragen hat, dass die Angelegenheit nicht mit der üblichen und für die Rechtmäßigkeit des Ablaufes erforderlichen Geschäftsmäßigkeit betrieben worden ist. Es muss aber eben von der Spitze eines LRA verlangt werden, dass sie auch einem solchen Verlangen (aus einer mit Verwaltungsvorgängen wenig vertrauten Organisationseinheit) der SK gegenüber die für Rechtmäßigkeit des Ablaufes erforderliche Geschäftsmäßigkeit der Behandlung des Verwaltungsvorganges im LRA gewährleistet.

(3.2) Datenschutzrechtliches Fehlverhalten hat auch insoweit vorgelegen, als das LRA die SK über ein archivrechtliches Auskunftsverlangen eines Journalisten einer überregionalen Zeitung durch Weiterleitung des vollständigen Wortlautes der Presseanfrage an die SK unterrichtet hat, *insoweit* dabei nicht nur die Tatsache einer bevorstehenden Übermittlung von Daten betreffend den derzeitigen Ministerpräsidenten an ein Presseorgan, einschließlich der in der Anfrage genau benannten einzelnen Archivunterlagen, mitgeteilt worden ist, auch unter Nennung des Namens der betreffenden Zeitung bzw. des Verlages, sondern darüber hinaus auch der genaue Wortlaut der Anfrage und der Name des betreffenden Journalisten. In diesem überschießenden Inhalt war der Inhalt der Anfrage ein personenbezogenes Datum des betreffenden Journalisten.

Eine Unterrichtung des Betroffenen, also hier des damaligen Ministerpräsidenten, darüber, dass ihn betreffende Daten an eine Zeitungsredaktion, möglicherweise auch an

welche bestimmte Zeitungsredaktion, von der Archivbehörde herausgegeben worden sind oder sicher demnächst herausgegeben würden, ist im Archivrecht nicht vorgesehen (vgl. § 10 Abs. 4 Satz 2, 1. HS SächsArchivG im Vergleich zu § 16 Abs. 3 SächsDSG - folgerichtigerweise, weil das Zur-Verfügung-Stellen personenbezogener Daten unter Wahrung des archivrechtlichen Datenschutzes gerade zur eigentlichen Aufgabe der Archivbehörde gehört), entspricht jedoch dem datenschutzrechtlichen Grundgedanken (des Volkszählungsurteils), dass jeder wissen können soll, inwieweit die öffentliche Verwaltung Daten über ihn verarbeitet - wobei allerdings erheblich abschwächend zu berücksichtigen ist, dass es sich bei den offenzulegenden bzw. offengelegten Angaben über den Landespolitiker ausschließlich um die Daten eines (seinerzeitigen!) Amtsträgers in Ausübung seiner (seinerzeitigen!) Amtstätigkeit gehandelt hat bzw. handeln würde, für die (aus verfassungsrechtlichen Gründen zwingenderweise) § 10 Abs. 2 Satz 3 SächsArchivG bestimmt, dass insoweit archivrechtlicher Datenschutz gerade nicht stattzufinden hat. (Die Sondervorschrift des § 32a Stasi-Unterlagen-Gesetz hat nicht zur Rechtfertigung der betreffenden Datenübermittlung an die SK herangezogen werden können.)

Die (in dessen mittlerer Leitungsebene getroffene) Entscheidung des LRA, die SK - ohne dass diese das verlangt hätte! - in dieser Weise umfassend zu unterrichten, ist eine Fernwirkung der überstürzten, eine Berücksichtigung der einschlägigen archivdatenschutzrechtlichen Vorschriften des Sächsischen Archivgesetzes nicht erkennen lassenden, von der üblichen Geschäftsmäßigkeit des Verwaltungshandelns abweichenden Verfahrensweise der Spitze des LRA bei der Erteilung der vorstehend erörterten Benutzungsgenehmigung gewesen.

(3.3) Aus den zuletzt genannten Gründen aller Wahrscheinlichkeit noch rechtmäßig ist es gewesen, wenn das LRA mit der genannten Mitteilung die SK - als vom gegenwärtigen Ministerpräsidenten insoweit mit der Wahrnehmung seiner Persönlichkeitsrechtsbelange betraute öffentliche Stelle des Freistaates - *über die Tatsache der beabsichtigten Offenlegung von Unterlagen in dem durch die Anfrage der Zeitung mit ihrer genauen Angabe der Thematik bestimmten Umfang unterrichtet hat.*

Ausreichend und allein sicher zielführend wäre demgegenüber allerdings die bloße Benachrichtigung über eine Übermittlung gewesen, *nachdem* diese durchgeführt worden war und ihr Umfang feststand.

(3.4) Weniger ins Gewicht gefallen sind archivdatenschutzrechtswidrige Übermittlungen personenbezogener Daten durch Unterlassen des Abdeckens einzelner in den Unterlagen (Protokolle des Rates des Kreises) enthaltener personenbezogener Daten - was wohlgemerkt keineswegs nur gegenüber dem Benutzer aus der Staatskanzlei, sondern auch gegenüber anderen Benutzern der Fall gewesen, also offenkundig unbeab-

sichtigt geschehen ist. Überdies habe ich feststellen können, dass die Archivbehörde im Zusammenhang mit einer personellen Verstärkung im Archiv im Laufe der Benutzungsvorgänge dazu übergegangen ist, die vorzulegenden Unterlagen vorher auf die eben ganz vereinzelt vorkommenden Bezugnahmen auf einzelne dem archivrechtlichen persönlichkeitsrechtsschützenden Datenschutz unterliegende Angaben zu überprüfen. Dies betrifft sowohl die Gewährung von Einsichtnahmen wie die Überlassung von Ablichtungen. Für beides habe ich eine wesentliche Verfahrensverbesserung innerhalb der Behörde im Verlauf der Benutzungsvorgänge zwischen September 2008 und Juni 2009 feststellen können.

(3.5) Zu Recht, wie schon oben (1.2) festgestellt, hatte die Archivbehörde auch Angaben über die Weiterbildung von (in den Unterlagen des Rates des Kreises genannten) Amtsträgern, insbesondere Mitgliedern des Rates des Kreises offengelegt, namentlich auch Angaben über die „marxistisch-leninistische Weiterbildung der Mitarbeiter des Staatsapparates“. Es hat sich bei der Teilnahme an derartigen Weiterbildungsveranstaltungen um Fortbildungen im Rahmen der Amtstätigkeit gehandelt, also um Daten über Amtsträger in Ausübung ihres Amtes, vgl. § 10 Abs. 2 Satz 3 SächsArchivG.

(3.6) Zu loben ist gewesen, dass das Kreisarchiv unter den damaligen Bedingungen (Lagerung des Archivgutes in einem in gründlicher Renovierung sich befindenden Gebäude) in ganz erstaunlichem Maße funktionsfähig gewesen ist. Erkennbar gewesen ist auch ein guter Wille und bestes Bemühen des in der Archivbehörde tätigen Personals, mit den genannten im Laufe der Zeit festzustellen gewesenen Verbesserungen der archivdatenschutzrechtlichen Praxis der Behörde.

Als ungünstig für die Einhaltung der archivdatenschutzrechtlichen Vorschriften hat sich die vergleichsweise tiefe hierarchische Staffelung in der Zuständigkeit für die Archivbehörde erwiesen: Zwischen der Dezernentenebene und der unmittelbaren Leitung (ausschließlich) der Archivbehörde (im neuen Groß-Kreis) gab es drei Hierarchieebenen. Das dürfte stark dazu beigetragen haben, dass die Spitze des LRA, die mit dem oben bemängelten Benutzungserlaubnis-Bescheid, genauer gesagt der in diesem zum Ausdruck kommenden Herangehensweise, das Handeln des Archivs stark beeinflusst hat, zu fern vom Archivrecht und der übrigen Archiv-Sachkunde gewesen ist und dass sie den Bescheid erteilt und damit implizit eine gebotene archivdatenschutzrechtliche Überlegungen außer Acht lassende Betrachtungsweise veranlasst hat. Archivrechtliche, und damit namentlich auch archivdatenschutzrechtliche, Sachkunde dürfte erst ab der Ebene der Leitung von Archiv, Registratur und Verwaltungsbibliothek vorhanden gewesen sein, ‚oberhalb’ davon jedoch nicht mehr.

(3.7) Insgesamt hat sich aus dem Vorgang für die Träger kommunaler Archivbehörden die Folgerung und die Lehre ziehen lassen, dass die Aufgabe des Archivars bzw. der Archivbehörde nur mit dem nötigen qualitativen (Sachkunde) und quantitativen personellen Aufwand erfüllt werden kann und dass allen Beteiligten deutlicher bewusst sein muss, dass es sich um eine - hoheitliche - Aufgabe der öffentlichen Gewalt handelt, deren Erfüllung mit Grundrechtseingriffen einhergehen kann und die rechtsgebunden zu erfüllen ist - wie es ja bei Behörden immer der Fall ist. In dem Vorgang ist eine einzelne sächsische kommunale Archivbehörde einer besonderen Belastungsprobe ausgesetzt gewesen, zumal noch unter besonders ungünstigen Bedingungen (Zusammenlegung dreier kommunaler Gebietskörperschaften mit Verteilung der Verwaltungszuständigkeit auf verschiedene voneinander recht weit entfernte Standorte; Gebäudeumbau); aber so einmalig muss der Fall nicht bleiben, woraus die Lehre zu ziehen ist, dass für solche archivdatenschutzrechtlichen Belastungsproben mehr als bisher Vorsorge getroffen werden muss.

5.8.2 Immer wieder: Daten mit latentem Mehrfachbezug betreffend Verwandtschaftsbeziehungen

Jemand, der Anfang 1945 in Ostpreußen geboren und von seiner Mutter unmittelbar danach mit auf die Flucht genommen worden und in einer sächsischen Stadt bei Pflegeeltern aufgewachsen war, hatte sich an das betreffende Stadtarchiv mit der Bitte um Informationen über seine leiblichen Eltern gewandt.

Die Archivbehörde hat die leiblichen Eltern - eine ostpreußische Geburtsurkunde hatte es angesichts der herannahenden Front nicht mehr gegeben - ermitteln können, war sich aber nicht sicher, ob es die Daten der 1915 und 1925 in Ostpreußen Geborenen, mangels Ablaufes der 100-jährigen Schutzfrist gemäß § 10 Abs. 1 SächsArchivG, dem Fragesteller mitteilen dürfte.

In Beibehaltung meiner bisherigen Rechtsauffassung, wie sie in 11/5.8.2 näher dargestellt ist, habe ich dem Archiv erläutert, dass man den datenschutzrechtlichen Auskunftsanspruch in seiner speziellen archivrechtlichen Ausprägung des § 6 Abs. 1 und 3 SächsArchivG auch auf Daten zu beziehen hat, die einen latenten, d. h. nicht in ihrem Wortlaut zum Ausdruck kommenden Bezug auf den Auskunftsbegehrenden haben, die aber aufgrund der Beziehung des Auskunftsbegehrenden zu den Daten der anderen Person bzw. zu dieser anderen Person selbst mittelbar auch als Daten der auskunftbegehrenden Person anzusehen sind - *vorausgesetzt*, die Daten entstammen einer behördlichen Tätigkeit (und damit einem Überlieferungszusammenhang), in der es um die betreffende Beziehung, in diesem Falle also die Abstammungsbeziehung geht. Mit anderen Worten: Der latente Mehrfachbezug eines Datums ist im Hinblick auf die Er-

füllung des Auskunftsanspruches zu berücksichtigen, allerdings begrenzt auf Beziehungen (zwischen der dem Wortlaut der Daten nach vorkommenden Person und der auskunftverlangenden Person), die vom ursprünglichen Speicherungszweck, also dem Verarbeitungszweck der Verwaltungsbehörde, aus deren Tätigkeit die Daten ins Archiv gelangt sind, umfasst sind. Der Auskunftsuchende konnte in diesem Fall also die Daten bekommen.

Im Hinblick auf Abstammungsbeziehungs-Daten ergibt sich dasselbe Ergebnis auch daraus, dass nach der Rechtsprechung des Bundesverfassungsgerichts aus dem allgemeinen Persönlichkeitsrecht ein Anspruch auf die Kenntnis der eigenen Abstammung folgt, der sich insbesondere gegen öffentliche Stellen richtet (vgl. BVerfG, Urt. v. 31. Januar 1989 - 1 BvL 17/87 = E 79, 256 = NJW 1989, 891). Diese Entfaltung des allgemeinen Persönlichkeitsrechtes als Anspruches auf die Kenntnis der eigenen Abstammung soll nach der Rechtsprechung auch ohne Einhaltung der Zweckbindung gelten: So lässt sich die Entscheidung des AG Bonn vom 8. Februar 2011 - 104 C 593/10 -, RDV 2011, 254, verstehen, die einem Kind einen Anspruch gegen ein Telekommunikationsunternehmen auf die Bekanntgabe des Namens und der Anschrift des Inhabers eines Telefonanschlusses (zu einem bestimmten Tag zu einer bestimmten Mobiltelefonnummer) zugesprochen hat. Offensichtlich war es die Mutter eben dieses Kindes gewesen, die am 29. September 2010 vor dem LG Bonn - zum Az.: 1 O 207/10 - ihrerseits mit dem Verlangen gescheitert war, *ihr* Namen und Anschrift des Telefonanschlussinhabers zu nennen, der sich ihr im Zusammenhang mit einem einmaligen sexuellen Kontakt lediglich unter der Bezeichnung „N“ und unter Angabe seiner (von beiden Beteiligten auch verwendeten) Telefonnummer namhaft gemacht hatte; *insoweit* hat die Rechtsprechung insbesondere einen Auskunftsanspruch aus § 242 BGB oder aus dem allgemeinen Persönlichkeitsrecht verneint.

5.8.3 Datenschutzrecht steht der (anonymisierten) Veröffentlichung von Gedächtnisprotokollen 1989 in Dresden Verhafteter nicht entgegen

Unter der Überschrift „Datenschutz spricht gegen Veröffentlichung“ berichteten die „Dresdner Neuesten Nachrichten“ am 9. Oktober 2009, dass die Bemühungen des Autors Günter Hofmann darum, die Gedächtnisprotokolle anonymisiert zu veröffentlichen, die im Oktober 1989 wegen Teilnahme an gewaltsamen wie auch gewaltfreien Demonstrationen Verhaftete und, wie das seinerzeit hieß, „Zugeführte“ über ihre Erlebnisse dem Dresdner Stadtjugendpfarramt der Evangelisch-Lutherischen Landeskirche Sachsen übergeben hatten, damit sie der damaligen Stadtverordnetenversammlung in öffentlicher Sitzung mit der Bitte um Aufklärung übergeben werden sollten (was am 26. Oktober 1989 durch den damaligen Superintendenten Dr. Ziemer gegenüber dem

damaligen Oberbürgermeister Berghofer geschehen ist), „*an datenschutzrechtlichen Gründen gescheitert*“ seien.

Über die Angabe seiner Telefonnummer in dem genannten Zeitungsartikel hat der Autor versucht, Einwilligungen Betroffener in die (anonymisierte) Veröffentlichung des von ihnen seinerzeit abgegebenen Gedächtnisprotokolls einzuholen.

Bei Verdacht einer missbräuchlichen Berufung auf Datenschutzrecht bin ich sehr hellhörig; deswegen habe ich mich von mir aus an den Autor gewandt.

Aus den mir dann von ihm vorgelegten Unterlagen ging hervor, dass seinerzeit der Stadt Kopien überreicht worden sind, die sich im Dresdner Stadtarchiv befinden, und dass diese Behörde dem Autor mitgeteilt hatte, dass ihm eine *Einsicht* in die Gedächtnisprotokolle aus datenschutzrechtlichen Gründen, die sich aus dem Sächsischen Archivgesetz ergäben, verwehrt werden müsse.

Ich habe dem Autor mitgeteilt, dass wegen § 10 Abs. 2 Satz 2 i. V. m. § 4 Abs. 2 Satz 2 SächsArchivG entgegen der Auffassung der Stadtverwaltung die allgemeine 30-jährige Schutzfrist des § 10 Abs. 1 Satz 1 SächsArchivG auf die Gedächtnisprotokoll-Texte des Stadtarchivs nicht anwendbar ist, weil es sich um Unterlagen handelt, die bis zum 2. Oktober 1990 bei einer staatlichen Stelle in der DDR angefallen, nämlich bei ihr als Behörde eingegangen sind, dass allerdings der Hinweis des Datenschutzbeauftragten der Landeshauptstadt auf § 10 Abs. 1 Satz 3 und 4 SächsArchivG, also die dem Persönlichkeitsrechtsschutz dienenden Schutzfristen für personenbezogenes Archivgut, zutreffend sei und dass die Anwendung des § 13 Abs. 2 Nr. 4 SächsDSG (vgl. dazu 12/10.4.1) ausscheide, da die Daten dem Archivrecht als abschließender Regelung unterlägen.

In Anbetracht dessen, so habe ich dem Autor weiter mitgeteilt, bestünden im Hinblick auf die Verwendung der im Stadtarchiv aufbewahrten Kopien der Gedächtnisprotokolle als Quellen für eine - anonymisierte - Veröffentlichung zwei Möglichkeiten:

Entweder komme das Stadtarchiv seiner meiner Auffassung nach aus § 10 Abs. 2 Satz 1 i. V. m. § 4 Abs. 2 Satz 2 SächsArchivG sich ergebenden Aufgabe nach, die zeitnahe Auseinandersetzung mit der SED-Diktatur zu ermöglichen, und stelle durch einen städtischen Bediensteten eine anonymisierte Kopie der Gedächtnisprotokolle für ihn her. Oder aber er müsse sein Vorhaben, möglicherweise mit einer anderen Person zusammen, dahingehend gestalten, dass er einen Text zu den seinerzeitigen Vorgängen verfasst, der als (historisches) Forschungsvorhaben anzuerkennen ist und in dessen Rahmen oder als dessen Anhang die betreffenden Erlebnis-Protokolle in anonymisierter Form *ediert*, also herausgegeben und veröffentlicht werden. In einem solchen Falle, also zu dem Zwecke der Durchführung eines solchen Vorhabens, würde die Archivbehörde

ihm gemäß § 10 Abs. 4 Satz 2 SächsArchivG die unanonymisierten Texte in Kopie zur Verfügung stellen dürfen, verbunden mit der ihn treffenden Pflicht (aus § 10 Abs. 4 Satz 2, 2. HS SächsArchivG), gemäß der von ihm ohnehin schon erteilten Zusicherung, die Erlebnisberichte in der Veröffentlichung *nur anonymisiert* wiederzugeben.

Darüber war aber der Oktober 2009 schon fast verstrichen, das vom Autor im Juni an die Stadtverwaltung herangetragene Vorhaben daher nicht mehr rechtzeitig zum Jahrestag der revolutionären Vorgänge in Dresden durchführbar.

Selbstverständlich hätte das Dresdner Stadtarchiv im Hinblick auf die historische Bedeutung der damaligen Vorgänge einigen Grund gehabt, den Arbeitsaufwand der Herstellung einer anonymisierten Kopie der Gedächtnisprotokolle zu betreiben. Archivbehörden und namentlich die in ihnen stattfindende Speicherung personenbezogener Daten als Grundrechtseingriff sind ja kein Selbstzweck, und der Wille des sächsischen Archivgesetzgebers, der sich aus § 10 Abs. 2 Satz 1 i. V. m. § 4 Abs. 2 Satz 2 SächsArchivG ausdrückt, nämlich eben eine *zeitnahe* und nicht erst in ferner Zukunft stattfindende Auseinandersetzung mit der SED-Diktatur zu ermöglichen, ist eindeutig.

Der Autor hatte sich bei seinem Bemühen um einen Zugang zu den Texten naheliegenderweise auch an die Evangelisch-Lutherische Landeskirche Sachsens gewandt, war aber auch dort (vgl. Dresdner Neueste Nachrichten vom 29. Juli sowie 6./7. August 2011) mit seinem Bemühen abgewiesen worden. Für *kirchliche* Datenschutz- bzw. archivdatenschutzrechtliche Angelegenheiten bin ich nicht zuständig. Im Hinblick auf Ausführungen des Landeskirchenamtes gegenüber dem Autoren zum staatlichen Archivrecht habe ich diesem allerdings mitgeteilt, dass, wie bereits dargelegt, das Sächsische Archivgesetz die 30-jährige allgemeine Schutzfrist für Archivgut, das bei auf dem Gebiet des Freistaates Sachsen staatliche oder quasi-staatliche Funktion ausübenden Stellen bis zum 2. Oktober 1990 entstanden ist, gemäß § 10 Abs. 2 Satz 2 SächsArchivG gerade außer Kraft setzt, eben zu dem Zweck, dass die historische Aufarbeitung der SED-Diktatur ohne Verzögerung ermöglicht werden soll, vorbehaltlich des Schutzes des Persönlichkeitsrechtes von Privatleuten, und dass dieser Rechtsgedanke zwar nicht unmittelbar auf die seinerzeit von Superintendent Dr. Ziemer gesammelten Gedächtnisprotokolle anzuwenden ist, da sie nicht bei staatlichen Stellen entstanden sind, dass aber davon abgesehen der Rechtsgedanke dieser Regelung gerade auch auf diese Unterlagen zutrifft.

Dem Autor ist es dann gelungen, an 25 der 170 seinerzeit übergebenen Protokolle heranzukommen und diese in dem Buch „Vergesst den Oktober 1989 nicht! Würdelos in der Diktatur - Gedächtnisprotokolle aus den Tagen der friedlichen Revolution“, Dresden 2010 - anonymisiert - zu veröffentlichen (vgl. DNN 22. Oktober 2010).

Inzwischen hat die Angelegenheit dadurch noch eine neue Wendung bekommen, dass der Autor an einen von Superintendent Dr. Ziemer und Stadtjugendpfarrer Henker unterzeichneten Vermerk des Evangelisch-Lutherischen Stadt-Jugendpfarramtes Dresden vom 3. November 1989 gelangt ist, in dem es heißt, man habe im Auftrage des Landeskirchenamtes und der „Gruppe der 20“ Erlebnisberichte und Gedächtnisprotokolle Betroffener zu den Ereignissen vom 3. bis 8. Oktober 1989 in Dresden gesammelt, damit eine unabhängige Untersuchungskommission diese Vorgänge aufklären könne, und wegen immer wieder nach Informationen über diese Berichte gestellter Fragen *lege man hiermit zunächst eine erste Auswahl vor. Die Verfasser hätten diese Berichte für die Öffentlichkeit freigegeben*.

Damit greift offenbar doch, was die im Stadtarchiv liegenden Kopien betrifft, zusätzlich auch § 10 Abs. 2 Satz 1 SächsArchivG ein, wonach die nicht dem Persönlichkeitsrechtsschutz (Datenschutz) dienende allgemeine Schutzfrist von 30 Jahren, ab der Entstehung der Unterlagen (§ 10 Abs. 1 Satz 1 SächsArchivG), nicht gilt, weil die Unterlagen *bereits bei ihrer Entstehung zur Veröffentlichung bestimmt waren*. Überdies, und darauf kommt es im Hinblick auf die dem Schutz des Persönlichkeitsrechtes dienende Schutzfristregelung des § 10 Abs. 1 Satz 3 SächsArchivG und damit für die Rechtslage im Ergebnis letztlich an, wird man eine *Einwilligung* der Betroffenen in eine (mit Namen versehene?) Veröffentlichung vor dem 3. November 1989, ja vermutlich sogar dem 26. Oktober 1989 als dem Tag der Übergabe an die Staatsgewalt, und im Wege eines Erst-recht-Schlusses als Einwilligung in eine heutige Offenlegung für die Zwecke einer anonymisierten Veröffentlichung gelten zu lassen haben. Das tatsächliche Vorliegen dieser Einwilligungen müsste sich ohne Weiteres verifizieren lassen.

Vielleicht liegen die Gedächtnisprotokolle ja vollständig zum 25. Jahrestag der Ereignisse von 1989 in Buchform vor.

Gegen Verwendungen des Datenschutzes als vorgeschobenen Grundes mich zu wenden gehört zu meinen Aufgaben - denn dergleichen ist geeignet, den Datenschutz, d. h. das Grundrecht auf informationelle Selbstbestimmung, in der Öffentlichkeit in unbegründeter Weise in Misskredit zu bringen (vgl. etwa 5/11.1 mit 6/11 und 7/11).

5.9 Polizei

5.9.1 Datenübermittlung durch den Polizeivollzugsdienst an private Hilfsorganisationen nach Einschreiten wegen häuslicher Gewalt

Meine Dienststelle wurde im Berichtszeitraum erneut mit der Frage befasst, ob und unter welchen Bedingungen der Polizeivollzugsdienst persönliche Daten von Opfern häus-

licher Gewalt (familiäre Verhältnisse, polizeilicher Sachverhalt) an private Hilfsorganisationen weitergeben darf.

Obwohl das SMI im früheren Schriftwechsel meine Auffassung, dass eine Opferschutzorganisation nur informiert werden darf, wenn die Zustimmung des Opfers vorliegt, geteilt hatte, übersandte es auf meine Nachfrage zur Dokumentation der Einwilligung eine Verfahrensanleitung (Handlungsanleitung für die sächsische Polizei zum Umgang mit „Häuslicher Gewalt“) sowie ein Standard-Fax zur Benachrichtigung der zuständigen Koordinierungs- und Interventionsstelle, welches der Betroffene im Falle seines Einverständnisses mit der Datenübermittlung zu unterschreiben hat. Im Übersendungsschreiben teilte das SMI mit, dass für den Fall, dass die Zustimmung nicht erteilt wird, das Fax mit einem entsprechenden Vermerk zur Vorgangsakte zu nehmen sei. Die Handlungsanleitung selbst enthielt allerdings den Hinweis an den bearbeitenden Polizeibeamten, dass eine Datenübermittlung „nach eingehender Prüfung und entsprechender Begründung auch gegen den Willen der Betroffenen gemäß § 45 SächsPolG möglich“ sei.

Ich machte daraufhin gegenüber dem SMI deutlich, dass eine Datenübermittlung ohne oder sogar gegen den Willen des Betroffenen unter keinem rechtlichen Aspekt in Betracht kommt. § 45 Abs. 1 SächsPolG lässt zwar eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs auch ohne Einverständnis des Betroffenen zu, allerdings muss dies zur Erfüllung der dem Polizeivollzugsdienst übertragenen Aufgaben, hier z. B. die Abwehr einer gegenwärtigen Gefahr für die Haushaltsangehörigen oder für das Kindeswohl, erforderlich sein. Erst unter diesen Voraussetzungen kann gegen den Willen des Betroffenen vorgegangen werden. Als polizeiliche Gefahrenabwehrmaßnahmen kommen hier vollzugspolizeiliche Maßnahmen oder die Verständigung der zuständigen staatlichen Stellen (z. B. Jugendamt, Gesundheitsamt) in Betracht. Die Opferschutzstelle nimmt dagegen keine polizeilichen Aufgaben, auch nicht hilfsweise, wahr. Ebenso wenig ist die Verständigung dieser Stelle zur polizeilichen Aufgabenerfüllung erforderlich. Für entsprechende Gefahrenabwehrmaßnahmen sind die genannten staatlichen Stellen zuständig, eine „Beauftragung“ oder auch nur Verständigung dieser Stelle und damit einhergehende Datenübermittlung gegen den Willen des Betroffenen ist nicht von § 45 SächsPolG gedeckt und daher unzulässig.

Auf eine entsprechende Änderung der Handlungsanleitung werde ich gegenüber dem SMI weiter hinwirken.

5.9.2 Löschung personenbezogener Daten aus polizeilichen Auskunftssystemen

Wie schon in 12/5.9.1 erreichte mich auch in diesem Berichtszeitraum ein Fall, bei dem sich die Frage stellte, wie nach der Einstellung strafrechtlicher Ermittlungsverfahren gemäß § 170 Abs. 2 StPO mit den gespeicherten personenbezogenen Daten des Beschuldigten verfahren wird und vor allem wie lange sie gespeichert werden sollen.

Der betroffene Petent bat mich dafür zu sorgen, dass seine seit zwei Jahren gespeicherten Daten gelöscht werden. Gegen ihn waren aufgrund einer Anzeige Ermittlungsverfahren wegen verschiedener Delikte geführt worden, wovon alle bis auf eines nach § 170 Abs. 2 StPO eingestellt worden waren. Gleichzeitig wurde gegen den Anzeigeerstatter ein Verfahren wegen Vortäuschens einer Straftat geführt, welches gegen Ableisten von Arbeitsstunden eingestellt wurde.

Der Petent selbst hatte bei der zuständigen Polizeidienststelle die Löschung seiner Daten aus den Auskunftssystemen der Polizei verlangt. Dies hatte die Polizei jedoch abgelehnt. Sie ging von einer anfänglichen Speicherdauer von zehn Jahren aus, da alleine aufgrund der Einstellung nach § 170 Abs. 2 StPO eine polizeilich-präventive Speicherung nicht ausgeschlossen sei. Die dem Petenten vorgeworfenen Straftaten seien so schwerwiegend gewesen, dass die Speicherung über zehn Jahre angemessen erscheine.

Hierzu stellte ich fest: Zwar dürfen die erforderlichen personenbezogenen Daten eines Betroffenen, gegen den das Ermittlungsverfahren nach § 170 Abs. 2 StPO eingestellt worden ist, bei bestehendem „Restverdacht“ weiter in polizeilichen Auskunftssystemen gespeichert werden, wenn der Betroffene aufgrund tatsächlicher Anhaltspunkte verdächtig ist, künftig eine Straftat zu begehen. Bei der Speicherprüffrist von zehn Jahren handelt es sich nach § 43 Abs. 4 SächsPolG jedoch um die gesetzlich festgelegte Höchstfrist. Sie darf nur im Hinblick auf schwere Straftaten angeordnet werden. Das war hier nicht der Fall. Erst nach einem eingehenden Gespräch mit dem SMI wurde ein Kompromiss gefunden. Man einigte sich auf eine Löschung der Daten nach fünf Jahren.

Dieser Zeitraum war nun Ende 2010 vorbei, so dass ich eine Anfrage stellte, ob die Daten des Bürgers nun auch wirklich gelöscht worden seien. Dies wurde letztendlich seitens der Polizei bestätigt.

5.9.3 Auswertung von Protokolldaten

Im Berichtszeitraum hatte ich erneut mit einem Fall der Auswertung von Protokolldaten zu Zwecken der Gefahrenabwehr zu tun. Bei Protokolldaten handelt es sich um personenbezogene Daten, die ausschließlich zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Daten-

verarbeitungsanlage gespeichert werden. Diese sind grundsätzlich nach § 13 Abs. 4 SächsDSG einer zweckfremden Nutzung entzogen. Eine Ausnahme wurde in § 43 Abs. 1a SächsPolG geschaffen, wonach Protokolldaten nach Anordnung durch den Leiter des LKA oder einen von ihm beauftragten Beamten auch zum Zweck der Abwehr von Gefahren für Leben, Gesundheit oder Freiheit einer Person oder für bedeutende fremde Sach- oder Vermögenswerte sowie zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung verwendet werden dürfen. Über eine solche Anordnung bin ich unverzüglich zu unterrichten.

So erhielt ich Mitteilung von einem Fall, wonach auf Anfrage einer Polizeidienststelle eines anderen Bundeslandes die in Sachsen gespeicherten Protokolldaten über zwei vermisste Personen mitgeteilt werden sollten. Ihr Verschwinden war im Familien- und Angehörigenkreis nicht nachvollziehbar und entsprechende konventionelle Ermittlungsmethoden hatten bisher keinen Erfolg erbracht. Die Auswertung der Protokolldaten sollte nunmehr zur Feststellung des Aufenthaltsortes der Vermissten dienen. Diese zweckändernde Nutzung der Protokolldaten war angesichts des hohen Gewichts des betroffenen Rechtsgutes - Leben - auch meines Erachtens eine geeignete Maßnahme zum Auffinden der Vermissten. Ich habe daher keine Einwände gegen die Auswertung der Protokolldaten geltend gemacht. Leider führte die Auswertung jedoch nicht zu dem erhofften Erfolg - die Vermissten blieben unauffindbar.

5.9.4 Belehrungen sächsischer Polizeivollzugsbeamter über Datenschutz im Zusammenhang mit der Nutzung polizeilicher Datenbanken

Seit dem Jahr 2007 stieg die Anzahl von Ordnungswidrigkeitenverfahren gegen Polizeibeamte an. Gegenstand der Verfahren war regelmäßig der unbefugte Abruf personenbezogener Dateien (IVO, PASS, ZEVIS, SCHENGEN, INPOL) durch Polizeivollzugsbeamte.

Die Argumentation der Betroffenen zeigte, dass unter den Beamten immer noch eine gewisse Unsicherheit hinsichtlich der zulässigen Nutzung polizeilicher Datenbanken bestand. So wurde vorgetragen, dass ein Abruf nicht unbefugt sein könne, wenn er aufgrund der im Einzelfall bestehenden Zugriffsrechte technisch möglich sei. Diese Annahme trifft nicht zu. Jeder Abruf muss für die Erfüllung konkreter dienstlicher Aufgaben der abrufenden Person erforderlich sein. Für einen befugten Abruf personenbezogener Daten aus polizeilichen Dateien kommt es nicht auf den jeweiligen Zugriffsstatus, sondern auf den dienstlichen Anlass an.

Neben der Verletzung des Rechts auf informationelle Selbstbestimmung der betroffenen Personen sind Verstöße gegen datenschutzrechtliche Bestimmungen in hohem Maße ge-

eignet, das Vertrauen der Allgemeinheit in die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten durch den Polizeivollzugsdienst zu beeinträchtigen. Deshalb habe ich mich an das SMI gewandt und angeregt, in den ohnehin jährlich durchgeführten Belehrungen über den Datenschutz und die Amtsverschwiegenheit besonders auf die Nutzung polizeilicher Dateien und das in diesem Zusammenhang zentrale Erfordernis der dienstlichen Veranlassung für jede Nutzung einzugehen. Insbesondere sollte über den Abruf personenbezogener Daten aus polizeilichen Dateien belehrt werden, um gegen potentielle amtliche Verfehlungen vorzubeugen. Das Staatsministerium informierte mich darüber, dass die nachgeordneten Dienststellen über meinen Vorschlag informiert und darum gebeten wurden, zukünftig danach zu verfahren. Hierfür möchte ich mich bedanken.

5.9.5 Kostenerhebung bei Auskunftserteilungen?

Im Berichtszeitraum hatte ich mich mit der Frage zu beschäftigen, ob Polizeidienststellen Kosten für die Erteilung von Auskünften nach § 18 SächsDSG oder die Vornahme von Löschungen nach § 20 SächsDSG erheben dürfen.

Die Frage war aus folgenden Gründen zu verneinen: Die Auskunft ist ausdrücklich (§ 18 Abs. 1 SächsDSG) kostenfrei; bei den übrigen Rechten, die wie die Berichtigung, Löschung und Sperrung auch objektive Amtspflichten sind, oder wie der Schadensersatzanspruch auf Geld zielen, ergibt sich dies aus der Natur der Sache. Nichts anderes ergibt sich bei öffentlich-rechtlichen (§ 54 VwVfG) oder zivilrechtlichen (z. B. Arbeitsverträge; privatrechtliche Hilfsgeschäfte) Verträgen einer öffentlichen Stelle mit dem Betroffenen oder auch bei Dienstvereinbarungen der Dienststellenleitung mit dem Personalrat: § 5 Abs. 2 SächsDSG stellt insofern ausdrücklich klar, dass die Rechte des Betroffenen nach den §§ 18 bis 24 und 34 Abs. 3 SächsDSG nicht durch Rechtsgeschäft beschränkt oder ausgeschlossen werden dürfen.

Die entsprechende Polizeidienststelle hat auf meine Intervention hin das SMI um Entscheidung gebeten; dieses hat sich meiner Auffassung angeschlossen.

5.9.6 Zulässigkeit von Bildüberwachungen von Demonstrationen etc. durch die Polizei

Wiederholt wurde ich mit der Frage der Zulässigkeit der Anfertigung von Übersichtsaufnahmen durch die Polizei bei Versammlungen, Demonstrationen, öffentlichen Veranstaltungen etc. konfrontiert.

Grundsätzlich sind Bild- und Tonaufnahmen im Rahmen von öffentlichen Versammlungen etc. durch die Polizei nur unter den Voraussetzungen der §§ 12a, 19a

VersammlG bzw. § 38 Abs. 1 und 2 SächsPolG zulässig. Außerhalb dieser Anwendungsbereiche dürfen Aufnahmen und Aufzeichnungen mittels Videotechnik m. E. nicht erfolgen, da hierfür im Hinblick auf den Eingriffscharakter für die Versammlungsteilnehmer eine gesetzliche Grundlage nötig ist, die es in Sachsen nicht gibt. Das SMI hat auf meine Anfrage vom August 2010 hin mitgeteilt, dass es bei Großdemonstrationen auch Übersichtsaufnahmen fertigt, soweit diese für die polizeiliche Aufgabenbewältigung (z. B. zur Lageeinschätzung) erforderlich sind. Mit den eingesetzten Kameras sei es technisch möglich, einen Personenbezug herzustellen.

Die durch den Gesetzgeber im Zuge der Neuregelung des § 12a VersammlG geäußerte Auffassung, die bloße Videobeobachtung einer Versammlung - ohne eine Speicherung der Aufnahmen - sei kein Grundrechtseingriff, da der Einzelne nicht individualisierbar gemacht werden solle und könne (BT-Drs. 11/4359 vom 18. April 1989, S. 17) ist rechtlich nicht haltbar (vgl. BVerfG, Beschluss vom 17. Februar 2009 - 1 BvR 2492/08, BVerfG 122, 342, 368 f.). Wie das Bundesverfassungsgericht ausführt, ist die Anfertigung von Übersichtsaufzeichnungen nach dem heutigen Stand der Technik für den Aufgezeichneten immer ein Grundrechtseingriff, da auch in Übersichtsaufzeichnungen die Einzelpersonen in der Regel individualisierbar mit erfasst sind. Sie könnten, ohne dass technisch weitere Bearbeitungsschritte erforderlich sind, durch schlichte Fokussierung erkennbar gemacht werden. Ein prinzipieller Unterschied zwischen Übersichtsaufzeichnungen und personenbezogenen Aufzeichnungen besteht nach dem heutigen Stand der Technik nicht. Auch der Sächsische Verfassungsgerichtshof bejaht einen Eingriff in den Schutzbereich des informationellen Selbstbestimmungsrechts (Art. 33 SächsVerf) selbst dort, wo es „lediglich“ um das Anfertigen von Bild- und Tonaufnahmen geht, gleich, ob es sich bei der Bildübertragung um Nahaufnahmen handelt oder um Übersichtsaufnahmen, die jederzeit zu Detailaufnahmen vergrößert werden können (SächsVerfGH, Urt. v. 10. Juli 2003 - Vf. 43-II-00, S. 85 f.). Damit stellt auch die bloße Übertragung von Bildern, z. B. in die Einsatzleitstelle, einen Grundrechtseingriff dar, der nur unter den Voraussetzungen der §§ 12a, 19a VersammlG bzw. 38 Abs. 1 und 2 SächsPolG zulässig ist.

Ich hatte das SMI seinerzeit darauf hingewiesen, dass die bisherige Rechtsprechung erkennen lässt, den Einsatz von Videotechnik im Hinblick auf den Einschüchterungseffekt für die Versammlungsteilnehmer nur bei besonderer Rechtfertigung unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes, insbesondere des Kriteriums der Erforderlichkeit, zuzulassen.

Ferner sei die Tendenz zu erkennen, auch für das Anfertigen von Übersichtsaufnahmen zur Lenkung und Leitung des Polizeieinsatzes während der (friedlichen) Versammlung (Videobeobachtung) eine gesetzliche Grundlage zu fordern, selbst wenn keine Speiche-

rung der Aufnahmen erfolgt (vgl. VG Münster, Urt. v. 21. August 2009, 1 K 1403/08; bestätigt durch OVG NRW, Beschluss v. 23. November 2010, 5 A 2288/09; VG Berlin, Urt. v. 5. Juli 2010, 1 K 905.09; BVerfG, Beschluss v. 17. Februar 2009, 1 BvR 2492/08).

Das VG Münster hat im o. g. Urteil ausgeführt, dass auch bloße Übersichtsaufnahmen in Echtzeitübertragung (Kamera-Monitor-Übertragungen) aufgrund der möglichen Einschüchterungseffekte durch die Präsenz einer Kamera einer gesetzlichen Grundlage bedürften, auch wenn die Eingriffsqualität gegenüber der Anfertigung von Aufzeichnungen deutlich geringer sei. Dies gelte selbst dann, wenn die Versammlungsteilnehmer darüber aufgeklärt würden, dass keine Aufzeichnung erfolge, solange die Versammlung einen friedlichen Verlauf nehme. Das Gericht führte aus, dass auch im Falle der Information über den Umfang der Maßnahme die konkrete Vorgehensweise (Begleitung des Demonstrationszuges mit einem Fahrzeug, auf dem eine Kamera befestigt war, welche auf die Teilnehmer gerichtet war) in Verbindung mit den technischen Möglichkeiten einer Videokamera (Weitwinkel, Zoom, Aufnahmefunktion) eine besondere Einschüchterung zu bewirken vermochte. „Wer wisse, dass er als Versammlungsteilnehmer am Monitor überwacht werde, wer jederzeit befürchten müsse, herangezoomt und damit als Individuum registriert zu werden, wer nicht wahrnehmen könne, wann bei einer aufnahmebereiten Kamera beabsichtigt oder gar versehentlich der Aufnahmeknopf betätigt werde, werde sich gravierender beeinflusst fühlen und sich daher möglicherweise anders verhalten, als derjenige, der lediglich durch Polizeibeamte ohne Einsatz technischer Hilfsmittel wahrgenommen oder mittels Fernglas beobachtet wird.“ (VG Münster Rdnr. 18, a. a. O.). Dieser Argumentation folgt das VG Berlin (a. a. O.).

Ergänzend ist zu bemerken, dass Versammlungsteilnehmer nicht erkennen können, zu welchen Zwecken Bild- und Tonaufnahmen angefertigt werden, sodass sie auch dann von der Wahrnehmung ihres Grundrechts aus Art. 8 GG, Art. 23 SächsVerf abgeschreckt werden können, wenn die Datenerhebung von Anfang an und ausschließlich zum Zweck der Leitung des Polizeieinsatzes erfolgt (vgl. Dietel/Gintzel/Kniesel, Versammlungsgesetz, 16. Aufl. (2011), § 12a Rdnr. 13).

Das Bundesverfassungsgericht beschränkt die Zulässigkeit von Übersichtsaufnahmen zur Lenkung und Leitung des Polizeieinsatzes selbst bei Vorliegen einer entsprechenden Rechtsgrundlage auf Fälle, in denen diese wegen der Größe oder Unübersichtlichkeit der Versammlung im Einzelfall erforderlich sind (BVerfG Rdnr. 135, a. a. O.).

Übersichts*aufzeichnungen* seien hiernach - unter der Maßgabe einer vorläufigen Regelung im einstweiligen Rechtsschutzverfahren - nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von der Versammlung erhebliche Gefahren für

die öffentliche Sicherheit oder Ordnung ausgehen (BVerfG Rdnr. 134, a. a. O.). Dies entspricht der Regelung in § 12a Abs. 1 Satz 1VersammlG.

Nach alledem ist zu folgern, dass das Anfertigen von Übersichtsaufnahmen, die nicht in den Anwendungsbereich von § 12a Abs. 1 Satz 1 i. V. m § 19a VersammlG oder § 38 Abs. 1 und 2 SächsPolG fallen, ebenfalls nur bei Vorliegen einer gesetzlichen Ermächtigung zulässig wäre, die - zudem - die o. g. Vorgaben des Bundesverfassungsgerichts aufgreift (vgl. Art. 9 Abs. 1 Satz 1 des Bay. Versammlungsgesetzes, in Kraft getreten zum 1. Juni 2010). Eine solche ist im Freistaat Sachsen derzeit nicht vorhanden. Somit sind Übersichtsaufnahmen bei Versammlungen nur unter den engen Voraussetzungen des § 12a VersammlG zulässig (so auch Dietel/Gintzel/Kniesel, Versammlungsgesetz, 16. Aufl. (2011), § 12a Rdnr. 15).

Im Hinblick auf die o. g. Ausführungen der Verwaltungsgerichte Münster und Berlin zum Einschüchterungseffekt dürfte das Anfertigen von Übersichtsaufnahmen - ohne gesetzliche Grundlage - auch dann unzulässig sein, wenn die Versammlungsteilnehmer gleichzeitig darauf hingewiesen werden, dass keine Aufzeichnung erfolgt.

5.9.7 Polizeiliche Videoüberwachung im Bereich der Prager Straße in Dresden

Seit Oktober 1999 überwachte die Polizei in der Landeshauptstadt eine große Einkaufsstraße mittels Videotechnik. Bei der Einführung wurde die Maßnahme damit begründet, dass hier eine offene Rauschgiftanbieterszene vorhanden sei. Die polizeiliche Videoüberwachung darf als letztes Mittel nur dann erfolgen, wenn andere, weniger in die Grundrechte der Betroffenen eingreifende Maßnahmen nicht zum Erfolg führen. Hierbei ist auch von Bedeutung, dass ein Großteil der aufgenommenen Personen unbescholtene Passanten oder Kunden der Einkaufsgeschäfte in dieser Straße sind. Die Zulässigkeit einer solchen Maßnahme hängt davon ab, ob es sich bei dem überwachten Bereich um einen Kriminalitätsschwerpunkt i. S. v. § 38 Abs. 2 Satz 1 i. V. m. § 19 Abs. 1 Satz 1 Nr. 2 SächsPolG handelt. Dies muss von der Polizei anhand der polizeilichen Kriminalstatistik nachvollziehbar belegt werden. Ferner muss bei unbefristeten Maßnahmen die Erforderlichkeit regelmäßig überprüft werden. Bereits bei meinem Kontrollbesuch im Jahre 2007 erteilte die Polizeidirektion Dresden die Auskunft, dass die sogenannte offene Rauschgiftszene zurückgedrängt werden konnte und auch andere Straftaten kontinuierlich rückläufig seien. Mit dem Argument, dass der Anfall an Straftaten hier noch immer wesentlich höher sei als in vergleichbaren Straßen in der unmittelbaren Umgebung, wurde der Bereich von der Polizei dennoch weiterhin als Kriminalitätsschwerpunkt eingestuft und an der Videoüberwachung festgehalten. Nach meinen mehrfachen Hinweisen entschloss sich die Polizeidirektion Dresden im Juni 2010 - auch im Hinblick auf die veraltete Technik - die Videoüberwachung zunächst für einen bestimmten

Zeitraum auszusetzen und sodann nach Evaluierung und in Abstimmung mit mir über eine Wiederaufnahme zu entscheiden. Hierfür danke ich.

5.9.8 Trennung der Formblätter für DNS-Erhebungen nach § 81e StPO (Molekulargenetische Untersuchung im anhängigen Strafverfahren) und § 81g StPO (DNA-Datenbank des BKA für künftige Strafverfahren)

Ein Petent wandte sich an mich, welcher im Jahre 2008 im Rahmen eines Ermittlungsverfahrens als Beschuldigter vernommen worden war. Ihm wurde mitgeteilt, dass einem der Täter ein Büschel Haare ausgerissen worden war. Daher wurde er um seine Zustimmung zur Anfertigung von Lichtbildern, zur Abnahme von Fingerabdrücken und zur Untersuchung von DNA-Material seiner Person gebeten. Nach Abschluss des Ermittlungsverfahrens würden diese Daten wieder gelöscht. Der Petent erklärte sich daraufhin u. a. zur Entnahme von DNA-Material freiwillig bereit und füllte das dafür vorgesehene Einwilligungsformular aus. Anhand der DNA-Spuren wurde festgestellt, dass die DNA-Spuren an den ausgerissenen Haaren mit denen des Petenten nicht übereinstimmten. Daraufhin hat die Staatsanwaltschaft das Ermittlungsverfahren gegen den Petenten mit der Begründung eingestellt, dass er sicher als Täter ausgeschlossen werden könne.

Im Jahr 2010 wurde erneut ein Ermittlungsverfahren gegen den Petenten geführt. Aufgrund der im Verfahren von 2008 abgenommenen Fingerabdrücke wurde eine Übereinstimmung mit Fingerabdrücken am Tatort festgestellt. Grund hierfür war, dass der Petent am Tatort beruflich tätig war. Diese personenbezogenen Daten des Petenten waren trotz Einstellung des Ermittlungsverfahrens durch die zuständige Staatsanwaltschaft nicht gelöscht worden. Auf Nachfrage beim LKA und der zuständigen Polizeidirektion erfuhr ich, dass die Polizei die Daten sowohl im PASS als auch im IVO gespeichert hatte. Dies sei aufgrund der Tatsache erfolgt, dass gegen den Petenten ein Restverdacht wegen des Ermittlungsverfahrens von 2008 bestehe, welcher sich darauf stütze, dass einer der Geschädigten den Petenten bei einer Lichtbildvorlage als denjenigen erkannt haben wollte, dem er die Haare ausgerissen habe.

Hierzu stellte ich fest: Die Polizei darf personenbezogene Daten weiter speichern, wenn ein sogenannte Restverdacht besteht und die Speicherung der Daten des Beschuldigten künftig bei der vorbeugenden Straftatenbekämpfung von Nutzen sein kann. Ein Restverdacht ist gegeben, wenn der Tatnachweis hinsichtlich einer Straftat nicht geführt werden kann, aber sonstige konkrete Anhaltspunkte dafür sprechen, dass der Tatverdacht fortbesteht (vgl. BVerfG, Urt. v. 16. Mai 2002, BvR 2257/01). Die Einstellung eines Verfahrens oder ein gerichtlicher Freispruch für sich alleine beseitigt den polizeilichen Tatverdacht nicht automatisch. Dieser Fall war hier jedoch gerade nicht gegeben. In der Einstellungsverfügung der Staatsanwaltschaft stand ausdrücklich, dass der Petent sicher

als Täter ausscheide. Ein Restverdacht im oben beschriebenen Sinne bestand gerade nicht. Die Daten hätten daher unverzüglich gelöscht werden müssen.

Dies war unrechtmäßigerweise nicht erfolgt. Vielmehr war eine Täterschaft seitens der Staatsanwaltschaft ausgeschlossen worden. Darauf habe ich hingewiesen und um eine Löschung der Daten gebeten. Nach Mitteilung meiner Bedenken an das LKA und die zuständige Polizeidirektion teilten diese mir mit, dass die Daten des Petenten aus dem PASS gelöscht worden seien.

Des Weiteren ergab sich durch die Auskunft des LKA, dass das DNA-Identifizierungsmuster des Petenten in die DNA-Analyse-Datei des BKA aufgenommen worden war. Eine Eintragung in diese Datei erfolgt nach § 81g StPO (nur) dann, wenn eine Straftat gegen die sexuelle Selbstbestimmung, eine andere Straftat von erheblicher Bedeutung oder eine Negativprognose bezüglich des Täters vorliegt. Auf dem Einwilligungsformular, welches der Petent ausgefüllt hatte, war die Möglichkeit der Eintragung mit einem Sternchen versehen, welcher auf die Voraussetzungen am Ende des Formulars verwies. Wenn die Voraussetzungen nicht gegeben sind, sollte man diese Möglichkeit streichen. Im Falle des Petenten sollte für das laufende Ermittlungsverfahren aus dem Jahre 2008 eine DNA-Untersuchung auf der Grundlage von § 81e StPO erfolgen. Die Voraussetzungen einer Speicherung in der DNA-Analyse-Datei des BKA für künftige Strafverfahren gemäß § 81g StPO waren hingegen nicht erfüllt.

Eine Straftat im Sinne von § 81g StPO war nicht gegeben und auch eine sogenannte Negativprognose, d. h. eine Gefahr neuer einschlägiger Straftaten, bestand bei dem Petenten gerade nicht. Auf diesen Sachverhalt habe ich ebenfalls hingewiesen und weiterhin mitgeteilt, dass das Einwilligungsformular nicht mit der entsprechenden Sorgfalt verwendet wurde.

In diesem Zusammenhang habe ich die Trennung der Formularblätter der Einwilligungserklärung zu § 81e StPO und zu § 81g StPO gefordert. Hierfür sprachen jedoch nicht nur der Grundrechtsschutz, sondern auch ökonomische Gründe, namentlich die Vermeidung falscher Speicherungen in der DNA-Datei des BKA und des in diesen Fällen gegebenen erheblichen Löschungsaufwands.

Daraufhin wurde ich informiert, dass die Daten des Petenten auch in der DNA-Analyse-Datei gelöscht worden seien. Weiterhin wurden meine Anmerkungen zu dem Formular zum Anlass genommen, die Vordruckgestaltung zur Einwilligung im Rahmen einer Besprechung mit den Leitern der Kriminaldienste der Polizeireviere sowie dem LKA zu erörtern. Die Generalstaatsanwaltschaft hat sich meiner Auffassung angeschlossen.

Der Vordruck zur Einwilligung wurde aufgrund dieser Besprechung zwischenzeitlich geändert, so dass dieser Missstand bei der Erhebung und Speicherung personenbezogener Daten in der kriminalpolizeilichen Praxis behoben werden konnte. Ich gehe deshalb davon aus, dass das LKA zukünftig getrennte Formblätter verwenden wird. Der Fall ist ein Beispiel wie in Zusammenarbeit zwischen den öffentlichen Stellen und dem Datenschutzbeauftragten vorbeugender Datenschutz durch organisatorische Maßnahmen gewährleistet werden kann. Er zeigt auch, dass eine datenschutzrechtliche Prüfung in einem konkreten Fall zur Vorbeugung beitragen kann. Für die gute Zusammenarbeit möchte ich mich beim LKA und der Generalstaatsanwaltschaft bedanken.

5.10 Verfassungsschutz

In diesem Berichtszeitraum nicht belegt.

5.11 Landesnetz

5.11.1 Einsatz eines Billing- und Reportingsystems im Freistaat Sachsen

Seit Oktober 2008 betreibt der Freistaat Sachsen mit dem Sächsischen Verwaltungsnetz (SVN) eine zentrale Kommunikationsinfrastruktur für das Land und die Kommunen. Im Bereich Sprache ist der schrittweise Ausbau zu einem leistungsfähigen Voice-Over-IP-Netz geplant. Damit werden schrittweise die bislang eingesetzten analogen, lokal vorhandenen Telefonanlagen abgelöst und die Sprache über das Datennetz abgewickelt. Teil des Paketes ist ein sogenanntes Billing- und Reportingsystem, in welchem die Verbindungs- und Abrechnungsdaten des Festnetztelefonverkehrs der gesamten Landesverwaltung abgebildet werden soll. Meine Behörde wurde mit der Freigabe der Plattform befasst. Gegenüber dem SMJus als zuständiger Stelle habe ich bereits mehrfach betont, dass die zentrale Verarbeitung aller Verbindungsdaten der Behörden und Einrichtungen des Freistaates Sachsen nur innerhalb eines eindeutigen Rechtsrahmens realisierbar ist. Solange dieser nicht vorhanden ist, kann keine Freigabe des Systems erfolgen. Die derzeit geltende Verwaltungsvorschrift der Sächsischen Staatsregierung über die Errichtung, den Betrieb und die Benutzung dienstlicher Telekommunikationsanlagen für die Landesverwaltung des Freistaates Sachsen (Dienstanschlussvorschrift - DAV) sieht die zentrale Speicherung und Verarbeitung der Verbindungsdaten nicht vor, ob eine Neufassung in Form der Verwaltungsvorschrift Telekommunikation (VwV TK) zustande kommt, ist aus derzeitiger Sicht fraglich. Innerhalb von zwei Jahren ist es bis jetzt nicht gelungen, einen tragfähigen Entwurf vorzulegen. Dies ist in besonderer Weise unverständlich, da es bereits eine Regelung gibt, die lediglich an die mit dem SVN neu geschaffenen Verhältnisse anzupassen ist. Zwischenzeitlich war das SMJus sogar der Auffassung, eine derartige Regelung sei unter dem Aspekt der Deregulierung verzichtbar. Vor dem Hintergrund einer starken Zentralisierung der Datenverarbeitung

im SVN ist der Wegfall einer übergreifenden Regelung für den Freistaat Sachsen nicht hinnehmbar. Diese Auffassung wurde von nahezu allen Ressorts geteilt. Mittlerweile hat das SMJus die Arbeit an einer Verwaltungsvorschrift wieder aufgenommen.

5.11.2 Zentrale Protokollierung von Verbindungsabbrüchen im SVN

Der Freistaat Sachsen betreibt seit Inbetriebnahme des SVN eine zentrale Voice-Over-IP-Plattform für den internen und externen Sprachverkehr. In der zweiten Jahreshälfte 2010 häuften sich Verbindungsabbrüche bei externen Telefonaten. Aus diesem Grund hat mich das SMJus um Beratung gebeten, wie bei der Eingrenzung von Verbindungsabbrüchen im SVN aus datenschutzrechtlicher Sicht vorzugehen sei. Das SMJus als verantwortliche Stelle, die T-Systems als Netzbetreiber und ebenso die British Telecom als Dienstleister der Voice-Over-IP-Plattform standen vor der Frage, inwieweit Verbindungsdaten für die Analyse und Eingrenzung der Fehler genutzt werden dürfen. Dass die Verbindungsabbrüche nach Angaben des SMJus sporadisch und landesweit auftraten und als Hauptmotivation für die rasche Fehlerbeseitigung eine mögliche negative Wirkung auf die Außendarstellung des Freistaates Sachsen benannt wurde, habe ich in meiner datenschutzrechtlichen Bewertung berücksichtigt.

Eine solche Datenerhebung ist - den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit folgend - auf abgehende dienstlich veranlasste Telefonate zu beschränken. Für die Verarbeitung der privaten Telefondaten der Bediensteten oder potenzieller privater Anrufer besteht keine Erforderlichkeit. Nach § 13 Abs. 4 SächsDSG ist die Zweckgebundenheit der Datenverarbeitung zu beachten. Es ist genau festzulegen, welche Verbindungsdaten für welche Auswertung erforderlich sind.

Für eine Auswertung der dienstlich veranlassten Telefonate ist das Sächsische Datenschutzgesetz einschlägig. Sollte im Rahmen einer solchen Untersuchung festgestellt werden, dass eine Erweiterung der Untersuchung auf eingehende Telefonate erforderlich sein sollte, müssten weitere Rechtsgrundlagen herangezogen werden. Wegen des möglichen privaten Charakters eines Anrufs ist beispielsweise das Telekommunikationsgesetz anzuwenden.

Die Maßnahme wäre auf einen begrenzten Zeitraum zu beschränken, die Dauer des Zeitraums wäre zu begründen. Die Daten, die an die T-Systems oder an British Telecom weitergegeben werden sollen, sind zu anonymisieren; das angewandte Verfahren zur Anonymisierung ist zu beschreiben.

Ferner müsste begründet werden, warum eine Vollerhebung von Verbindungsdaten erforderlich ist. Nach meiner Einschätzung sind nur solche Telefonate für die Fehlersuche relevant, bei denen Verbindungsabbrüche zu verzeichnen sind. Es stellt sich daher die

Frage, inwieweit diese Telefonate isoliert werden könnten und die Speicherung aller Telefonatsdaten vermieden werden kann.

Bei der geplanten Maßnahme handelt es sich um eine Datenverarbeitung im Auftrag. Zu prüfen ist damit, ob diese Datenverarbeitung durch bestehende vertragliche Regelungen zwischen dem Freistaat Sachen und den Vertragspartnern im SVN bereits abgedeckt oder ob eine Erweiterung der Verträge erforderlich ist.

Nach Aussagen des SMJus ist es schlussendlich nicht zu einem Eingriff in Verbindungsdaten gekommen, da sich eine von T-Systems und British Telecom versuchsweise vorgenommene Konfigurationsänderung als technisch stabil und in akzeptabler Weise als fehlerresistent erwiesen hat.

5.12 Ausländerwesen

5.12.1 Nennung des Namens der Ehefrau auf einem Aufenthaltstitel

Im letzten Berichtszeitraum wandte sich ein Petent an mich, welcher sich gegen die Nennung des vollständigen Namens seiner Ehefrau in seinem Aufenthaltstitel wandte. Aus seiner Sicht sei diese Nennung nicht notwendig und datenschutzrechtlich bedenklich. Er hatte gegen diese Nennung auch bei der zuständigen Ausländerbehörde Widerspruch eingelegt.

Die Ausländerbehörde teilte mir auf Anfrage mit, dass sie die Nennung des Namens als Anmerkung zum Aufenthaltstitel ansehe und so die Zweckbindung des Titels unterstreicht.

Dieser Auffassung konnte ich mich nicht anschließen. Die Nennung des Namens der Ehefrau ist eine Verarbeitung personenbezogener Daten und insofern als Grundrechtseingriff nur gerechtfertigt, wenn sie erforderlich zur konkreten Aufgabenerfüllung ist. Dies erschien mir angesichts dessen, dass der zuständigen Ausländerbehörde, die das zweckgebundene Aufenthaltsrecht „prüft, erteilt oder versagt“, der Name der Ehefrau bekannt und in der Ausländerakte hinterlegt ist, zumindest zweifelhaft. Mir erschloss sich nicht, weshalb es zur Erfüllung der Aufgaben der Ausländerbehörde notwendig sein soll, dass auch Dritte, nämlich diejenigen, die die Nebenbestimmung der Aufenthaltserlaubnis in dieser selbst oder im Reisepass zur Kenntnis nehmen, den Namen der Ehefrau erfahren müssen.

Dieser Auffassung hat sich die Landesdirektion Dresden als Widerspruchsbehörde angeschlossen. Die Nennung des Namens der Ehefrau diene weder der Sicherstellung der Erteilungsvoraussetzungen noch wird der Zweck des Aufenthaltstitels dadurch näher

bestimmt. Vielmehr sei die Nennung des Namens vom Gesetzgeber nicht vorgesehen und stoße auf erhebliche datenschutzrechtliche Bedenken.

Daraufhin hat die Ausländerbehörde auf die Nennung des Namens der Ehefrau verzichtet und ihn in den bestehenden Aufenthaltstiteln gestrichen.

5.13 Wahlrecht

5.13.1 Datenschutz bei Bürgerbegehren nach § 25 SächsGemO

Mehrere Einwohner wandten sich an mich wegen der Weitergabe von Unterschriftslisten zu einem Bürgerbegehren gegen die Eingemeindung der Gemeinde E. in die Stadt F. Die Unterschriftslisten - so der Vorwurf - seien an die Mitglieder des damals zuständigen Gemeinderats weitergereicht worden. Verschiedene, auch namentlich benannte Gemeinderäte und andere Einwohner hätten daraufhin - so die Beschwerdeführer - die Kenntnisnahme der Unterschriftslisten genutzt, um die Unterstützer des Bürgerbegehrens aufzusuchen und diese zu veranlassen, die Unterschrift zu dem Bürgerbegehren zurückzuziehen. Dabei sei ein vorbereitetes Blanko-Widerrufsschreiben an eine der Initiatorinnen des Bürgerbegehrens vorgelegt worden. Die insgesamt 47 Widerrufserklärungen, die eine Unterschreitung des Quorums zur Folge hatten, seien bis auf ein Schreiben ohne Kenntnis der Initiatorin direkt bei der Gemeinde E. eingegangen. Das eingereichte Bürgerbegehren hätte mit 469 Unterschriften - so die Beschwerdeführer weiter - eigentlich das erforderliche Quorum erreicht. Mit Schreiben vom 5. November 2008 habe die Gemeinde E. das beantragte Bürgerbegehren aber wegen Nichterreichens des Unterschriftenquorums als unzulässig beschieden.

Nach Prüfung des Sachverhaltes stellte ich Folgendes fest: Am 21. Oktober 2008 wurden dem Bürgermeister der Gemeinde E. Unterschriftslisten mit 469 Unterschriften zu einem Bürgerbegehren gegen die von der Gemeinde beabsichtigte Eingemeindung in die Stadt F. überreicht. Mit Schreiben vom 27. Oktober 2008 erging die Einladung zur Sitzung des Gemeinderates der Gemeinde am 4. November 2008 mit den Beratungsunterlagen zur Tagesordnung, unter anderem zu TOP 2 „Beratung und Beschlussfassung zur Prüfung des eingereichten Bürgerbegehrens“. Die Beratungsunterlagen zu TOP 2 bestanden aus der Beschlussvorlage und den Unterschriftslisten. Die Anlage zum Gemeinderatsbeschluss Nr. 48/2008 „Prüfergebnis des Bürgerbegehrens“ wurde erst für die Gemeinderatssitzung gefertigt. Wie die Stadt F. mitteilte, habe die Anzahl der gültigen Unterschriften für das am 21. Oktober 2008 eingereichte Bürgerbegehren nicht das gesetzliche Quorum erfüllt. Die überwiegende Anzahl der Widerrufserklärungen von Unterzeichnern der Unterschriftenlisten seien am 28. Oktober 2008 und am 3. November 2008 in der Gemeindeverwaltung E. abgegeben worden bzw. seien per Post eingegangen. Eine Widerrufserklärung sei bereits am 27. Oktober 2008 und ungefähr drei

Widerrufserklärungen seien noch am 4. November 2008 eingereicht worden. Darüber hinaus sei die Unzulässigkeit des Bürgerbegehrens auch wegen weiterer rechtlicher Gründe festgestellt worden.

Mit dem Versand der Beratungsunterlagen (deren Bestandteil die Unterschriftslisten zum Bürgerbegehren waren) am 27. Oktober 2008 zur Sitzung des Gemeinderates am 4. November 2008 hatten die Gemeinderäte Kenntnis von Namen und Anschriften sämtlicher Unterzeichner. Die Feststellung, dass die überwiegende Anzahl der gleichlautenden Widerrufserklärungen am 28. Oktober 2008 und am 3. November 2008 in der Gemeindeverwaltung E. abgegeben wurden bzw. per Post eingingen, verstärkte den Verdacht einer unbefugten Nutzung personenbezogener Daten durch Gemeinderäte für eine Kontaktaufnahme mit Unterstützern mit dem Ziel eine Widerrufserklärung herbeizuführen, geht man davon aus, dass die Gemeindeverwaltung selbst nicht Widerrufe eingesammelt hatte.

Die Stadt F. - nach der zum 1. Januar 2009 wirksam gewordenen Eingemeindung Rechtsnachfolger der Gemeinde E. - lehnte meine Bitte zur Befragung von auch namentlich bezeichneten Gemeinderäten, die Unterzeichner des Bürgerbegehrens mit dem Ziel des „Widerrufs“ angesprochen hatten, aus „rechtlichen“ Gründen ab.

Ich beanstandete letztendlich die Stadt F. als Rechtsnachfolger der Gemeinde E. wegen eines Datenschutzverstoßes gegen § 36 Abs. 3 Satz 1 SächsGemO i. V. m. § 9 Satz 2 SächsDSG sowie § 28 Abs. 1 SächsDSG.

Unter Inanspruchnahme der Rechtsgrundlagen der §§ 25 Abs. 3, 36 Abs. 3 SächsGemO waren am 27. Oktober 2008 zur Sitzung des Gemeinderates der Gemeinde E. am 4. November 2008 zu TOP 2 „Beratung und Beschlussfassung zur Prüfung des eingereichten Bürgerbegehrens“ der Tagesordnung als Beratungsunterlagen die Beschlussvorlage und die Unterschriftslisten zum Bürgerbegehren übermittelt worden. Eine Anlage zum Gemeinderatsbeschluss Nr. 48/2008 mit dem Titel „Prüfergebnis des Bürgerbegehrens“ wurde erst für die Gemeinderatssitzung gefertigt. Eine fristgerechte Ausreichung obengenannter Anlage mit den Beratungsunterlagen ohne Unterschriftslisten wäre für eine sachgerechte Information und Auseinandersetzung der Gemeinderäte in der Gemeinderatssitzung erforderlich und ausreichend gewesen. Eine Übermittlung der Unterschriftslisten an die Gemeinderäte war hingegen nicht erforderlich und damit unzulässig. § 36 Abs. 3 Satz 1 SächsGemO bestimmt nicht, dass der Bürgermeister zur Einberufung der Sitzung des Gemeinderates und der Nennung der Verhandlungsgegenstände alle (möglichen) Unterlagen an die Gemeinderäte zu übermitteln hat. Es sind vielmehr alle für eine angemessene Vorbereitung erforderlichen Unterlagen, die dem Gemeinderat eine sachgerechte Entscheidung ermöglichen, zu übermitteln.

Es gehört auch zu den Aufgaben der Kernverwaltung, die Überprüfung der Unterzeichnungsberechtigung und Prüfung der Einhaltung des Quorums nach § 25 Abs. 1 Satz 2 SächsGemO vorzunehmen. Diese Feststellung berührt nicht die Zuständigkeit für die nach § 25 Abs. 3 Satz 1 SächsGemO durch den Gemeinderat und die zu treffende Entscheidung über die Zulässigkeit des Bürgerbegehrens. Die Überprüfung der Unterzeichnungsberechtigung und Prüfung der Einhaltung des Quorums nach § 25 Abs. 1 Satz 2 SächsGemO ist durch befugte Mitarbeiter der Verwaltung unter Nutzung des Melderegisters (§ 5 Abs. 2 Nr. 1. a) SächsMG) bei Wahrung des Meldegeheimnisses vorzunehmen. Eine Weitergabe der Daten (oder auch die Gewährung von Einsichtnahme in die Unterschriftslisten) an Dritte ist der Gemeinde verwehrt. Die Gemeinde hat bei der Auswertung der Unterschriftslisten deren Zweckbindung zu berücksichtigen, was bedeutet, dass die Listen nur in dem zur Zulässigkeitsprüfung des Bürgerbegehrens erforderlichen Umfang ausgewertet werden dürfen. Eine darüber hinausgehende Datenauswertung ist unzulässig (Rehak in Quecke u. a., SächsGemO, § 25 Rdnr. 8 m. V. a. Kunze/Bronner/Katz, GemO BW, § 21 Rdnr. 18).

Darüber hinaus hat sich die Verwaltung neutral zu verhalten und ist pflichtig, Bürgerbegehren in der Durchführung zu unterstützen. Die Entgegennahme und Aufrechnung von Widerrufen von Unterzeichnern von Bürgerentscheiden und die damit einhergehende Datenverarbeitung findet hingegen keine gesetzliche Stütze; Unterzeichnungen sind wie Stimmabgaben üblicherweise gar nicht rückgängig zu machen. Mit dem Eingang des Antrags auf ein Bürgerbegehren und den dafür eingereichten Unterschriftslisten wird der Geschäftsgang für das Bürgerbegehren eröffnet. Die Rücknahme von Erklärungen durch Unterzeichner des Begehrens ist verfahrensrechtlich nicht vorgesehen und würde die Durchsetzung von Bürgerbegehren nach Zugang bei der Gemeindeverwaltung in Frage stellen.

Gesetzlich ist mit Eingang des Antrages die (neutrale) Gemeindeverwaltung beauftragt, die Unterschriftsberechtigung zu prüfen und es obliegt dem Gemeinderat die Entscheidung über den Antrag vorzunehmen, § 25 Abs. 3 SächsGemO. Daher ist die vorgenommene Datenverarbeitung im Zusammenhang mit den Widerrufen als rechtswidrig anzusehen gewesen (vgl. VG Augsburg Au 7 K 05.304, Au 7 K 05.306). Die Datenverarbeitung ist insoweit rechtswidrig gewesen, als dass sie hier über die Annahme der Widerrufe und die Ablage in einen Vorgang hinausgegangen ist und ein Datenabgleich mit den Unterschriftslisten des Bürgerbegehrens erfolgt war.

Durch die ungeprüfte Vervielfältigung für die Übersendung von Kopien der Unterschriftslisten an die Gemeinderäte vor der Sitzung waren neben dem zuvor dargestellten Datenschutzverstoß die allgemeinen datenschutzrechtlichen Grundsätze der Datenvermeidung und der Datensparsamkeit (§ 9 Satz 2 SächsDSG) verletzt worden.

Nach Aufforderung gab die Stadt F. mehrere Stellungnahmen ab. Mit der Begründung einer fehlenden Rechtsgrundlage verweigerte die Stadt jedoch die Befragung eines genannten Gemeinderates und anderer Gemeinderäte der Altgemeinde E., die in Bezug auf eine mißbräuchliche Nutzung der Unterschriftslisten in Betracht kamen. Ungeklärt blieb damit die datenschutzrechtliche Frage, ob neben der zu beanstandenden ungesicherten Übermittlung der Unterschriftslisten an den Gemeinderat ein weiterer Datenschutzverstoß von Gemeinderäten unter Verletzung der Verschwiegenheitspflicht durch die eigenmächtige Verwendung der Unterschriftslisten stattgefunden hatte. Da sich Verstöße von Stadträten gegen die Verschwiegenheitspflicht nach § 19 Abs. 2 SächsGemO und das Datengeheimnis nach § 6 SächsDSG nach meiner behördlichen Erfahrung nur schwer nachweisen lassen, war ich auf die von mir erbetenen unterstützenden Maßnahmen der Stadt in besonderem Maße angewiesen.

Der einzelne Gemeinderat steht als Teil des Hauptverwaltungsorgans der Gemeinde in einem öffentlich-rechtlichen Amtswalterverhältnis, das einem Ehrenbeamtenverhältnis angenähert ist (Menke in Quecke u. a., SächsGemO, § 27 Rdnr. 20). Er hat sich in dieser Eigenschaft jeglicher Einflussnahme oder die Aussprache von Empfehlungen, die einmal geleistete Unterschrift zum Bürgerbegehren zurückzuziehen, zu enthalten (VG Augsburg, a. a. O.). Die Verpflichtung zur Geheimhaltung für Gemeinderäte besteht nach § 19 Abs. 3 SächsGemO auch nach Beendigung der ehrenamtlichen Tätigkeit fort. Vergleichbare fortdauernde Verschwiegenheitspflichten finden sich für allgemein ehrenamtlich Tätige in § 84 VwVfG und für Beamte in § 37 Abs. 1 BeamtStG und § 67 Abs. 1 BBG. Aus der Rechtsstellung des einzelnen Gemeinderates leitet sich wegen der fortdauernden Verpflichtung zur Verschwiegenheit ein nachwirkendes Prüf- und Sanktionsrecht durch die zuständige Stelle - hier den Gemeinderat, vertreten durch den Bürgermeister - ab, das eine Verfolgung und Ahndung möglicher Pflichtverletzungen auch im Nachgang ermöglicht.

Der Bürgermeister als Leiter der Gemeindeverwaltung und Vorsitzender des Gemeinderates hatte über das gesetzmäßige Handeln der Gemeinde zu wachen. Ihm oblag es, ggf. Maßnahmen gegen Gesetzesverstöße oder Pflichtverletzungen zu ergreifen. Die Weigerung, Hinweisen auf mögliche Pflichtverletzungen von Gemeinderäten nachzugehen, verletzt die Unterstützungspflicht nach § 28 SächsDSG meiner Behörde gegenüber. So sind mögliche Rechtsverletzungen Einzelner ggf. nur noch im Wege eines Ordnungswidrigkeitenverfahrens aufklärbar.

Zur Vermeidung vergleichbarer zukünftiger Datenschutzverstöße habe ich die Stadt F. aufgefordert, dem Stadtrat und dem Ortschaftsrat E. meine Beanstandung zuzuleiten. Darüber hinaus bat ich um Weitergabe meiner Hinweise an die Räte, um solche

Vorkommnisse und Datenschutzverstöße auszuschließen. Die Stadt F. teilte mir mit, dass sie meine Aufforderungen befolgt habe.

5.14 Sonstiges

5.14.1 Archivierung und Vernichtung von Sicherheitsakten

Das SMF fragte an, ob es die bei ihm entstandenen Unterlagen über eine Sicherheitsüberprüfung von Bediensteten (Sicherheitsakten, § 19 SächsSÜG) dem Sächsischen Staatsarchiv nach § 5 Abs. 1 SächsArchivG zur Archivierung anbieten müsse. Das Staatsarchiv habe diese Frage bejaht. Dagegen spreche, dass das Archivgesetz eine Anbietung solcher Unterlagen nur vorschreibe, „soweit Rechtsvorschriften nichts anderes bestimmen“. Eine solche andere Bestimmung aber sei im Sicherheitsüberprüfungsgesetz enthalten, wonach die „Vorschriften des Archivgesetzes … unberührt bleiben“. Deshalb stelle sich die Frage, welche Vorschrift vorgehe. Auch stelle sich die Frage, ob das SMF solche Unterlagen überhaupt an das Archiv übersenden dürfe, da das Sicherheitsüberprüfungsgesetz gerade nicht die erforderliche Befugnis zur Übermittlung solcher Daten zu Archivierungszwecken regelt.

Ich habe die Anfrage sinngemäß wie folgt beantwortet:

Sicherheits- und Sicherheitsüberprüfungsakten (§ 19 SächsSÜG) sind besonders heikle Unterlagen. Sie enthalten zumindest in der Regel Angaben zur Privatsphäre, mitunter zur Intimsphäre des Betroffenen. Sie können in die Nähe dessen kommen, was die Verfassungsgerichte von Bund und Ländern in ständiger Rechtsprechung als mit den Datenschutzgrundrechten des Einzelnen unvereinbar erkannt haben, namentlich die „Zusammenführung von Daten zu Persönlichkeitsprofilen“, vgl. § 13 Abs. 6 SächsDSG. Deshalb ist an die Verarbeitung (das Erheben, Speichern, Übermitteln etc.) personenbezogener Daten zu Sicherheitsüberprüfungszwecken, insbesondere auch an die Führung, Aufbewahrung und Anbietung von Sicherheits- und Sicherheitsüberprüfungsakten, ein strenger Maßstab der Gesetzmäßigkeit anzulegen.

Nach § 20 SächsSÜG unterliegen Sicherheitsakten der „zuständigen Stelle“, d. h. der Beschäftigungsbehörde des Sicherheitsüberprüften, einem strengen Regime. Sie sind u. a. grundsätzlich innerhalb bestimmter Fristen zu vernichten. Nach § 20 Abs. 4 SächsSÜG bleiben dabei die Vorschriften des Archivgesetzes jedoch „unberührt“. Sowohl aus dem Wortlaut als auch aus der Begründung der Vorschrift ergibt sich damit eine uneingeschränkte Verweisung auf die Anbietungspflicht nach § 5 SächsArchivG. Die Anbietungspflichten nach § 5 Abs. 1 Satz 1 bis 4 SächsArchivG setzen die Vernichtungspflichten vorübergehend aus. Die vom SMF erwogene Problematik einer Rückverweisung von § 5 Abs. 1 Satz 4 SächsArchivG auf § 20 Abs. 4 SächsSÜG be-

steht nicht. Denn eine „etwas anderes bestimmende Rechtsvorschrift“ i. S. v. § 5 Abs. 1 Satz 4 SächsArchivG müsste gerade die Anbietung von Sicherheits- und Sicherheitsüberprüfungsakten abweichend von § 20 Abs. 4 SächsSÜG regeln. Eine solche Rechtsvorschrift ist indes nicht ersichtlich. Auch der Gesetzgeber wollte offensichtlich nichts anderes. Er hat die Anbietung von Sicherheits- und Sicherheitsüberprüfungsakten in vollem Bewusstsein der archivrechtlichen Anbietungspflichten nach § 5 Abs. 1 Satz 1 bis 3 SächsArchivG geregelt. Die Begründung des Gesetzentwurfs der Staatsregierung vom 10. Oktober 2002 (LT-Drs. 3/7094) lautet insofern:
„*Es wird klargestellt, dass auch auf Unterlagen über Sicherheitsüberprüfungen die archivrechtlichen Vorschriften anzuwenden sind. D. h., die Unterlagen sind vor der Vernichtung dem zuständigen Archiv zur Übernahme anzubieten. Das Archiv hat der Geheimhaltungsbedürftigkeit der Unterlagen Rechnung zu tragen*.“ (S. 29 des Gesetzentwurfs).

Damit sind Sicherheitsakten des SMF dem Sächsischen Staatsarchiv zur Archivierung anzubieten. Verneint dieses die Archivwürdigkeit, so kann (richtig: hat) das SMF nach § 5 Abs. 5 Satz 2 SächsArchivG die Unterlagen vernichten, wenn weder Rechtsvorschriften noch schutzwürdige Belange des Betroffenen dem entgegenstehen. Bejaht es dagegen die Archivwürdigkeit, stellt sich die vom SMF problematisierte Frage der Übermittlungsbefugnis. Auch dazu hat jedoch der Gesetzgeber durch den Verweis von § 20 Abs. 4 SächsSÜG auf § 5 Abs. 1, 5 Satz 1 SächsArchivG eine ausreichende Regelung getroffen, da sowohl die Anbietung als auch die Übernahme der Sicherheitsakten notwendig mit der Übermittlung personenbezogener Daten verbunden sind. § 22 SächsSÜG steht dem nicht entgegen, da die Vorschrift lediglich Übermittlungsbeschränkungen und Zweckbindungsgebote im Rahmen der Aufgabenerfüllung (Durchführung von Sicherheitsüberprüfungen und Wiederholungsüberprüfungen nach § 1 Abs. 1 SächsSÜG) regelt. Die Anbietung und eventuelle Übernahme der Sicherheitsakten betrifft jedoch nicht mehr die Aufgabenerfüllung des SMF als zuständige Stelle nach dem Sächsischen Sicherheitsüberprüfungsgesetz, sondern ausschließlich seine Aufgabenerfüllung als speichernde Stelle nach dem Archivgesetz für den Freistaat Sachsen.

Mithin sind die Sicherheitsakten des SMF, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich und eventuelle Aufbewahrungsfristen abgelaufen sind, dem Sächsischen Staatsarchiv anzubieten.

Ich habe diesen Fall im Übrigen zum Anlass genommen, gegenüber der Staatsregierung auf eine Reduzierung der Zahl von Sicherheitsüberprüfungen zu dringen.

6 Finanzen

6.1 Bezügerechnung für Dritte

In 12/5.1.9 und 13/5.1.8 hatte ich die Bezügerechnung für Dritte thematisiert. Unter anderem hatte ich moniert, dass öffentliche Stellen ohne gesetzlich oder staatsorganisatorisch mit dieser Aufgabe betraut zu sein, die Bezügerechnung für externe, zumeist nicht-öffentliche Stellen durchführten.

Zwischenzeitlich ist die Nachfolgebehörde des Landesamtes für Finanzen, das Landesamt für Steuern und Finanzen durch die Neufassung des Sächsischen Verwaltungsorganisationsgesetzes mit der Befugnis ausgestattet worden, Bezüge- und Beihilfeabrechnungen für Dritte durchzuführen, wenn dies im öffentlichen Interesse liegt (§ 9 Abs. 2 Satz 5 SächsVerwOrgG). Da diese Stelle auch in langjähriger Praxis die Bezüge für dritte Stellen verwaltete und mir im Berichtszeitraum erneut Vorgänge auffielen, richtete ich an diese Landesbehörde die Nachfrage, wie das öffentliche Interesse begründet werden könnte und erhielt unter anderem die Antwort, dass das Landesamt über ein hohes Datenschutzniveau und gesteigerte fachliche Kompetenzen verfüge, was ein öffentliches Interesse begründe. Auch weitere Begründungsversuche konnten mich nicht überzeugen. Zudem wäre in jedem Einzelfall das öffentliche Interesse für das Tätigwerden für Stellen außerhalb der Landesverwaltung festzustellen gewesen.

7 Kultus

7.1 Erhebung von Gesundheitsdaten durch die Schule - Forderung nach Angabe von Hinderungsgründen bei Sportbefreiung oder bei Allgemeinunterricht

Immer wieder erhalte ich Anfragen, in denen sich Elternsorgeberechtigte danach erkundigen, inwieweit die Forderung der Schule nach Angabe eines Grundes bei Sportbefreiung oder bei Verhinderung der Teilnahme am Unterricht rechtmäßig ist. Ein seltsames Beispiel war das Verlangen eines Sportlehrers einer Mittelschule. Dieser beabsichtigte zur Sicherstellung der Teilnahme am Sportunterricht eine Liste zu erstellen, aus der hervorgehen sollte, wann die Schülerinnen der Klasse menstruationsbedingt dem Sportunterricht fernblieben. Aber auch andere Eltern führten in anderen Fällen aus, dass sie von der Schule ihres Kindes informiert worden seien, dass bei Krankheit zukünftig zwingend eine Bescheinigung vorzulegen wäre, aus der der Grund der Erkrankung ersichtlich werden müsste. Die datenschutzrechtliche Überprüfung dieser Anforderung der Schule ergab, dass die Forderung der Schule nach der Mitteilung des Grundes der Erkrankung (im Sinne einer Diagnose) rechtswidrig gewesen war.

Nach § 4 Abs. 1 SächsDSG darf die Schule als öffentliche Stelle personenbezogene Daten verarbeiten, wenn das Sächsische Datenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt. Das Erheben personenbezogener Daten ist dabei nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist (§ 12 SächsDSG). Zur Teilnahme am Unterricht regelt § 1 SBO, dass die Schüler an öffentlichen Schulen im Sinne von § 3 Abs. 2 SchulG zur pünktlichen und regelmäßigen Teilnahme am Unterricht und an vom Schulleiter für verbindlich erklärten Schulveranstaltungen verpflichtet sind. Ist ein Schüler durch Krankheit oder aus anderen nicht vorhersehbaren zwingenden Gründen verhindert die Schule zu besuchen, so ist dies der Schule unter Angabe des Grundes und der voraussichtlichen Dauer der Verhinderung unverzüglich mitzuteilen (§ 2 SBO). Bei einer Krankheitsdauer von mehr als fünf Tagen sowie bei Teilzeitunterricht von mehr als zwei Unterrichtstagen kann der Klassenlehrer oder der Tutor vom Entschuldigungspflichtigen die Vorlage eines ärztlichen Zeugnisses verlangen. Bei der Information „Angabe des Grundes“ im Sinne der Schulbesuchsordnung handelt es sich lediglich um allgemeine Angaben, z. B. „krankheitsbedingt“ oder aus „gesundheitlichen Gründen“. Darüber hinausgehende Daten zum gesundheitlichen Zustand eines Schülers ist die Schule nicht zu erheben befugt.

Angaben zur Gesundheit einer Person sind im Sächsischen Datenschutzgesetz als besonders schutzwürdig eingestuft: In § 4 Abs. 2 SächsDSG ist geregelt, dass die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft,

politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben, nur unter erschwerten Voraussetzungen zulässig ist, unter anderem dann, wenn eine Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt oder der Betroffene eingewilligt hat.

Die Voraussetzungen des § 4 Abs. 2 SächsDSG waren in den mir vorliegenden Fällen nicht erfüllt. Weder lag eine Rechtsvorschrift vor, die die Erhebung der Gesundheitsdaten ausdrücklich vorsah, noch hatten Betroffene eingewilligt, noch lagen andere Gründe zur Verarbeitung von Gesundheitsdaten vor. Für die Erfüllung der Aufgaben der Schule ist lediglich der Grund des Fernbleibens vom Unterricht, hier z. B. „aus gesundheitlichen Gründen“ zur Gewährleistung der Schulpflicht gemäß § 26 SchulG erforderlich. Im Ausnahmefall, z. B. bei auffällig häufigen oder langen Erkrankungen, kann der Schulleiter gemäß § 2 Abs. 3 SBO vom Entschuldigungspflichtigen die Vorlage eines amts- oder vertrauensärztlichen Zeugnisses verlangen. Die Anforderung ist durch den Schulleiter besonders zu begründen. Auffällig lang sind Erkrankungen von mehr als zehn Tagen, bei Teilzeitunterricht von mehr als vier Unterrichtstagen. Selbst in diesen Fällen darf mangels anderslautender Rechtsvorschrift das amts- oder vertrauensärztliche Zeugnis lediglich allgemeine Angaben z. B. „aus gesundheitlichen Gründen“ enthalten. Ähnlich ist die Rechtslage im Fall der Sportbefreiungen. Gemäß der Grundsätze der Verwaltungsvorschrift des SMK und des SMS zur Befreiung vom Sportunterricht vom 1. März 1996 können Schüler aus gesundheitlichen Gründen (auch teilweise) vom Sportunterricht befreit werden. Vielen Elternsorgeberechtigten ist dabei nicht bekannt, dass gemäß Nummer 2 der Grundsätze der Verwaltungsvorschrift der Sportlehrer über Art und Umfang der Befreiung vom Sportunterricht entscheidet, soweit diese vier Wochen nicht überschreitet. Für eine Befreiung von mindestens einer Woche kann der Sportlehrer ein ärztliches Zeugnis vom Schüler anfordern. Einige Schulen schlussfolgerten aus dieser Rechtsnorm, dass sie - wohl um die Entscheidung über die Rechtmäßigkeit des Fernbleibens vom Sportunterricht zu treffen - den Grund der Erkrankung (teilweise bei den Eltern, teilweise als Zusatzangabe auf dem ärztlichen Attest) einzufordern befugt seien. Auch an dieser Stelle ist die Schule über die allgemeine Angabe „aus gesundheitlichen Gründen“ hinaus zur Erhebung von Gesundheitsdaten mangels Rechtsgrundlage nicht befugt. Über eine Befreiung vom Sportunterricht, die den Zeitraum von vier Wochen überschreitet, entscheidet der Schulleiter aufgrund einer Stellungnahme des Jugendärztlichen Dienstes des Gesundheitsamtes. Der Jugendärztliche Dienst gibt seine Stellungnahme für das laufende Schuljahr auf dem Formblatt „Jugendärztliche Bescheinigung über die Teilnahme am Sportunterricht“ ab. Dieses Formblatt enthält entsprechend der Rechtslage keine Diagnose, sondern lediglich Empfehlungen aufgrund des Befundes, z. B. eine Vollbefreiung. Zur Klarstellung regelt die Verwal-

tungsvorschrift zur Befreiung vom Sportunterricht unter Nr. III. - Zusammenarbeit zwischen Jugendärztlichem Dienst und Schule - unmissverständlich: „Die Zusammenarbeit entbindet nicht von der ärztlichen Schweigepflicht."

Die Speicherung von Gesundheitsdaten im schulischen Bereich ist mit der Einwilligung der Eltern oder bei volljährigen Schülern und Auszubildenden mit deren Einwilligung jedoch möglich. Dazu regeln die jeweils geltenden Schulordnungen, dass z. B. eine durch dafür qualifizierte Lehrer oder Schulpsychologen festgestellte Teilleistungsschwäche, Art und Grad einer Behinderung oder chronischen Krankheit, soweit sie für den Schulbesuch oder die Ausbildung von Bedeutung sind, durch die Schule gespeichert werden dürfen. Zumeist werden diese Angaben bereits nach den Verordnungen der einzelnen Schulrichtungen bei der Schulaufnahme erhoben und sie werden als Informationen von den Elternsorgeberechtigten an die Schule gegeben. Als ein Beispiel, in dem die Kenntnis von solchen Daten sinnvoll ist, sei die Kenntnis des Sportlehrers von chronischen Erkrankungen genannt, die er im Rahmen des regulären Sportunterrichts beachten muss. Diese Daten kann er in dem zusätzlich zum klassischen Klassenbuch speziell für den Sportunterricht angeordneten Klassenbuch in einer Spalte für besondere Eintragungen notieren. In dieser Spalte ist Raum für Eintragungen, z. B. über chronische Erkrankungen wie Asthma oder Diabetes, aber auch für aktuelle Einschränkungen, die ihm Eltern aus eigenem Antrieb mitgeteilt haben und die der Sportlehrer im Rahmen des regulären Sportunterrichts beachten muss, wie z. B. eine schwere Chlorallergie. Der Sportlehrer ist gehalten, die Gesundheit des Schülers zu schützen und trägt dafür die Verantwortung. Dieses spezielle Notenbuch des Sportlehrers unterliegt im Übrigen den gleichen datenschutzrechtlichen Bestimmungen wie das klassische Notenbuch.

Darüber hinaus werde ich häufig gefragt, ob die Erhebung der Krankenkassendaten von Schülern allgemein und wegen der durchzuführenden Klassenfahrten zulässig sei. Die Angabe der Krankenkasse, der Krankenkassennummer und weiterer Angaben sind nur beim Eintritt eines Krankheitsfalles oder bei Unfällen erforderlich. Eine Erfassung der Daten in der Schülerakte, in Dateien oder im Notenbuch ist nicht erforderlich. Bei einem Unfall und im Krankheitsfall sind die Elternsorgeberechtigten zu benachrichtigen, die die erforderlichen Krankenkassenangaben machen können. Sofern eine Gesundheitsgefahr für den Schüler abgewendet werden muss, können medizinische Maßnahmen ohnehin bereits ohne die Elternsorgeberechtigten eingeleitet werden und es ist nach den Regeln der mutmaßlichen Einwilligung zu verfahren.

7.2 Internetpräsenzen von Schulen und erforderliche Einwilligungen

Bereits in 12/7.7 hatte ich mich mit Internetauftritten der Schulen auseinandergesetzt. Hingewiesen hatte ich auf den Umstand, dass Abbildungen von Schülern, Lehrern, Beschäftigten und anderen Personen nach § 22 KunstUrhG einwilligungsbedürftig sind. Bei anderen Daten als Bilddaten, wie z. B. bei Namensnennungen von Schülern, richtet sich eine Einwilligung nach dem Sächsischen Datenschutzgesetz, § 4 Abs. 1 Nr. 2 und den Formvorschriften des § 4 Abs. 3 bis 5 SächsDSG, bei Beschäftigten nach § 37 Abs. 2 Nr. 1 SächsDSG. Die Schriftform ist auch bei Einwilligungen nach § 37 SächsDSG einzuhalten.

Während eine Veröffentlichung von Schülerdaten nur mit Einwilligung zulässig ist, kommt es bei Beschäftigten darauf an, ob eine Veröffentlichung von Angaben wie Vorname, Nachname, dienstliche E-Mail-Adresse, Dienstanschrift etc. zur Aufgabenerfüllung der Schule erforderlich ist (§ 37 Abs. 2 Nr. 2 SächsDSG). Nach der Rechtsprechung sind Amtsträgerdaten nicht ohne Weiteres schutzwürdig (vgl. dazu BVerwG, Beschluss v. 12. März 2008 - 2 B 131/07 zur Veröffentlichung einer E-Mail-Adresse eines Beamten auf der Internetseite einer Behörde). Allerdings wird beamten- und arbeitsrechtlich Fürsorgegrundsätzen Rechnung zu tragen und z. B. dann von einer Veröffentlichung abzusehen sein, wenn der Beschäftigte durch die Veröffentlichung einer Gefährdung ausgesetzt wird.

Bei der Einwilligung der Schüler ist zu beachten, dass die Schüler zum Teil noch nicht volljährig sind. In diesen Fällen ist auch die Einwilligung der gesetzlichen Vertreter, in der Regel der Eltern, erforderlich. Darüber hinaus ist zu beachten, dass bei 14-jährigen oder älteren Schülern bereits regelmäßig eine Grundrechtsfähigkeit im Hinblick auf das informationelle Selbstbestimmungsrecht angenommen werden kann, so dass zwei Einwilligungen erforderlich werden. So kann auch bei Einwilligung der Sorgeberechtigten, aber bei Nicht-Einwilligung der Schüler - oder umgekehrt - die personenbezogene Datenverarbeitung dennoch unzulässig werden (vgl. 12/7.7).

Eine Einwilligung von Lehrern und Beschäftigten an der Schule wird primär zu Eigenpräsentationszwecken der Schule in Betracht kommen, bei der in aller Regel eine Datenverarbeitung nach § 37 Abs. 2 Nr. 2 SächsDSG aus Gründen fehlender Erforderlichkeit nicht erzwungen werden kann.

Da ich zu den vorstehenden Angelegenheiten immer wieder Nachfragen erhalte, biete ich als Hilfe unter 17.2.5 ein Einwilligungsformular als Muster an, das an die jeweiligen behördlichen Bedürfnisse angepasst werden muss.

7.3 Neuartige Unterrichtsmethoden und Möglichkeiten der Überwachung des Nutzerverhaltens der Schüler während des Lehrbetriebs in der Schule

In Schulen - insbesondere an Berufsschulen - wird zunehmend Unterrichtsstoff mit Hilfe von PCs, Terminals oder Notebooks vermittelt. In den Einrichtungen finden dabei Lernplattformen Verwendung, die die Einhaltung der Unterrichtsvorgaben durch Steuerung und Kontrolle aller Computer durch die Lehrkräfte sicherstellen sollen. Bei derartigen Schulnetzwerkprogrammen werden dem Lehr- und Aufsichtspersonal zum Teil Administrativfunktionen eingeräumt, die nicht nur die Freigabe von Hardwarezugängen und Geräten (Datenträgeranschlüssen, Druckern, Scannern etc.), Dateien und dem Internet unterstützen, sondern auch eine Bildschirm- und Anwendungskontrolle der sich in Gebrauch befindenden Computereinheiten ermöglichen. In diesem Zusammenhang haben mich Schulen mehrfach gefragt, ob derartige Programme zur Nutzerverwaltung und laufenden Kontrolle von Schülern auch eingesetzt werden dürfen, wenn die Schüler in Echtzeit und ohne Aufzeichnung bei ihrem Nutzerverhalten an den Computereinrichtungen über den Monitor des Lehrers beobachtet werden können.

Durchgreifende Bedenken habe ich gegen eine derartige Kontrolle aufgrund der bestehenden schulrechtlichen Aufsichtspflicht nicht. Auch ist eine Echtzeitüberwachung der Computerplätze - ohne Aufzeichnungen - aus meiner Sicht noch vertretbar, da ansonsten nur bliebe, dass Lehr- und Aufsichtspersonal die Schülerplätze abgeht und so einen ordnungsgemäßen Unterrichtsablauf zu gewährleisten versucht, ein bei größeren Klassen und Prüfungen nicht mehr realisierbares Unterfangen. In jedem Fall wäre aber beim Einsatz derartiger automatisierter Technik nicht außer Acht zu lassen, aus Transparenzgründen eine Information für die Elternsorgeberechtigten bzw. die Schüler anzubieten, die es den Betroffenen und den Elternsorgeberechtigten ermöglicht, die Datenverarbeitung im Hinblick auf Umfang, Tiefe und Ausmaß nachzuvollziehen (§ 9 Abs. 2 SächsDSG). Eltern- und Informationsabende, auf denen das Verfahren kommuniziert und genauer erörtert und besprochen werden kann, wären gangbare Wege.

Selbstverständlich nicht mehr wegzudenken ist die Nutzung des Internets im Schulbetrieb. Beim Einsatz der Computer fallen bei der Inanspruchnahme von Internetdiensten Daten an, die je nach Schulnetzlösung einzelnen Nutzern zugeordnet werden können, sogenannte Internetprotokolldaten. Diese Daten geben weitgehenden Aufschluss über die aufgerufenen Internetinhalte, etwa im Hinblick auf politische Auffassungen und private Vorlieben, und sind daher persönlichkeitsrechtlich relevant.

Dennoch ist die Protokollierung regelmäßig zur Sicherstellung des ordnungsgemäßen Verfahrens beim Internetbetrieb und des Schulnetzes kurzzeitig zulässig und erforder-

lich. Zusätzlich ist auch wiederum die Aufsichtspflicht der Schule zu beachten. Im Hinblick auf einen technisch-inhaltlich nicht beschränkten schulischen Internet-Zugang besteht grundsätzlich das Risiko, dass die Schule Schüler zu deren Nachteil gewähren lässt oder dass sich die Schule schadensersatzpflichtig machen könnte, indem Schüler jugendgefährdende Inhalte konsumieren, Urheberrechtsverstöße begehen oder rechtswidrige Inhalte verbreiten. Eine Haftung der Schule selbst kommt allerdings in aller Regel nur bei Verletzung der Aufsichtspflichten in Betracht. Häufig unterschätzt wird die Verantwortlichkeit der Schule in Bezug auf jugendgefährdende, pornographische, Gewalt verherrlichende oder extremistische Internet-Inhalte nach dem Strafgesetzbuch und nach dem Jugendschutzgesetz. Je nach Alter der Schüler und nach den örtlichen und technischen Gegebenheiten werden neben adäquaten Vorsorgemaßnahmen - z. B. Jugendschutzprogrammen - weitere nachträgliche Kontrollen notwendig sein, um von unerwünschten Abrufen Kenntnis zu erlangen und diese für die Zukunft zu unterbinden. Auf diese Weise ist es auch möglich, dass sich die Schule urheberrechtlich exkulpiert. (Bei rechtswidrigen Inhalten, die von Schülern abgerufen oder verbreitet werden, kann die Schule letzte Risiken zudem bei volljährigen Schülern mit Hilfe einer Haftungsfreistellung, die von diesen zu unterzeichnen ist, ausschließen.)

Eine Internet-Nutzungsordnung der Schule, in der die nicht erlaubten Tatbestände klar festgelegt und die schulordnungsrechtlichen Konsequenzen eines Missbrauchs aufgeführt sind, ist unerlässlich. Der Umfang der Datenverarbeitung der Protokolldaten und das Verfahren stichprobenartiger Kontrollen sind in der Ordnung darzustellen. Die Speicherung der Protokolldaten ist zeitlich auf das erforderliche Maß zu beschränken. Im Regelfall wird ein Monat ausreichend sein. Eine Speicherdauer von sechs Monaten, wie sie zum Beispiel nach dem Telekommunikationsgesetz - die entsprechenden Vorschriften sind vom Bundesverfassungsgericht aufgehoben worden - vorgesehen gewesen sind, ist keinesfalls notwendig.

Zur Auswertung der Protokolldaten auf Verstöße empfiehlt sich ein Gremium unter Beteiligung von Vertrauenslehrern und des Datenschutzbeauftragten der Schule einzurichten, auch um ein ordnungsgemäßes und weitgehend neutrales Verfahren bei der Kontrolle gewährleisten zu können. Im Hinblick auf die Protokollierung, die Zweckbindung der Datenverarbeitung, die Speicherdauer und mögliche Kontrollen sind die Festlegungen in der Schulordnung so präzise zu treffen, dass die Schüler Umfang, Tiefe und Ausmaß der Datenverarbeitung abzuschätzen in der Lage sind.

7.4 Datenübermittlungen von Schulen an andere öffentliche und nicht-öffentliche Stellen

Häufig erhalte ich Nachfragen zu den Möglichkeiten von Datenübermittlungen durch Berufsschulen an andere öffentliche und nicht-öffentliche Stellen. Dass Ausbildenden Abschlussergebnisse bzw. Ergebnisse von Teilprüfungen übermittelt werden dürfen, ergibt sich aus § 37 Abs. 2 Satz 1 BBiG und § 31 Abs. 2 Satz 2 HwO. Eine Mitteilung von Zwischenprüfungen - darauf zielen viele Nachfragen von Berufsschulzentren - ist gesetzlich nicht mehr vorgesehen. In 7/9.3.2 hatte ich noch auf die alte Gesetzeslage Bezug genommen, die dies zuließ. Die einschlägigen Schulordnungen nehmen auf die gesetzlichen Regelungen Bezug, so z. B. § 25 Abs. 2 BSO. Unabhängig davon können allgemeine und zusammenfassende Informationen zum Leistungsstand - soweit dies in den Schulordnungen vorgesehen ist - mitgeteilt werden (vgl. z. B. § 18 Abs. 6 Satz 2 BSO).

Eine weitere, mehrmalig auftauchende Frage war, ob Berufsschulen an die BaföG-Ämter Mitteilungen zur Schulteilnahme zu machen befugt sind. Nach § 14 Abs. 1 SächsDSG können an die BaföG-Ämter Fehlzeiten (aber nur unentschuldigtes oder vom Schüler zu vertretendes Fehlen) übermittelt werden. Die Übermittlungsbefugnis korrespondiert dabei mit einer Erhebungsbefugnis auf der Empfängerseite, da § 20 Abs. 2 BaföG bei der Rückerstattung eine Kenntnisnahme der Zuschuss gewährenden Behörde voraussetzt (vgl. u. a. VG Dresden, Urt. v. 17. August 2010 - 5 K 266/10).

Allgemeiner zu beantworten ist die Frage, inwieweit die Schule anderen Stellen Daten preiszugeben befugt ist, wenn dies zur Organisation der Lehre notwendig erscheint, wie z. B. bei der dualen Berufsausbildung, bei der die Auszubildenden nach der Ausbildungsordnung Kurse bei der Industrie- und Handelskammer, der Handwerkskammer oder der Innung zu belegen haben. So benötigen die Kammern zur Organisation z. B. Angaben zur Klassenzuordnung einzelner Lehrlinge, um Lehrgangstermine außerhalb der Unterrichtszeiten organisieren zu können. Die Schulordnungen als speziellere Datenverarbeitungsvorschriften enthalten in gewissem Umfang Übermittlungsbefugnisse, auf die als Rechtsgrundlage zurückgegriffen werden kann, z. B. das Zusammenarbeitsgebot nach § 5 Abs. 1 BSO. Enthalten bereichsspezifische Vorschriften keine Übermittlungsvorschriften, so wäre, was die öffentlich-rechtlichen Kammern betrifft, nach § 14 SächsDSG zu prüfen, ob eine Übermittlung im konkreten Einzelfall zulässig ist. Bei nicht-öffentlichen Stellen wiederum wäre nach § 16 SächsDSG zu klären, ob eine Übermittlung stattfinden darf.

Eine Einwilligung wird auch bei einem möglichen Rückgriff auf die Datenverarbeitungsbestimmungen des allgemeinen Datenschutzgesetzes für eine Datenweitergabe in

aller Regel nicht erforderlich sein. Aus Transparenzgründen empfehle ich gleichwohl eine Information an die Betroffenen, dass Angaben an bestimmte Empfänger und Ausbildungspartner weitergegeben werden sollen. In Zweifelsfällen wäre es darüber hinaus immer noch möglich, den Betroffenen, das heißt den Schüler, zu der beabsichtigten Datenübermittlung anzuhören.

7.5 Videoüberwachung und Webcams im Schulbereich

Es erreichten mich mehrere Anfragen zur Zulässigkeit von Videoüberwachungen und Videoaufzeichnungen im Schulbereich.

Der Einsatz von Videokameras und Webcams stellt rechtlich eine Beobachtung mit optisch-elektronischen Einrichtungen nach § 33 SächsDSG dar. Bei der Videoüberwachung und der Überwachung mit Webcams ist zu unterscheiden zwischen einer Überwachung öffentlich zugänglicher Räume (z. B. eines Foyers oder des Eingangsbereichs der Schule) und nicht öffentlich zugänglichen Räumen (zum Beispiel ein Computerkabinett oder bestimmte Klassenräume). Darüber hinaus ist zu differenzieren zwischen der Videoüberwachung und der Videoaufzeichnung. Die Videoaufzeichnung, bei der Videodaten für einen bestimmten Zeitraum gespeichert werden, ist „Mehr“ als ein tiefgehender Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Letztendlich ist auch entscheidend, in welcher Qualität die Videodaten anfallen. Eine Webcam zur Präsentation der Schule im Internet, bei der zu der optisch-elektronischen Beobachtung die Verbreitung über das weltweite Web hinzukommt, wird regelmäßig nicht zur Aufgabenerfüllung erforderlich sein. Sie wird regelmäßig daher auch nur dann zulässig sein, wenn gar keine personenbezogenen Daten verarbeitet werden (vgl. 5.5.7). Die Auflösung der Kamera muss so grob sein bzw. die Kamera muss so unscharf eingestellt sein, dass die Identifizierung einzelner Personen nicht mehr möglich ist. Eine Anfrage, die den Einsatz einer Webcam auf einem Schulplatz zum Gegenstand hatte, beantwortete ich in diesem Sinne.

§ 33 SächsDSG sieht eine Beobachtung öffentlich zugänglicher Räume vor. Voraussetzung hierfür ist, dass das Videografieren zur Aufgabenerfüllung, insbesondere zur Gewährleistung der öffentlichen Sicherheit und Ordnung oder zur Wahrnehmung eines Hausrechts, erforderlich ist. Darüber hinaus dürfen die schutzwürdigen Interessen der Betroffenen an einem Unterbleiben der Datenverarbeitung nicht überwiegen. Das bedeutet, dass immer eine Abwägung vorzunehmen ist. Bloße Dienlichkeit genügt nicht im Hinblick auf die Erforderlichkeit. Der beobachtete Bereich ist darüber hinaus zu kennzeichnen (§ 33 SächsDSG). Sind auch Bedienstete von den Videomaßnahmen betroffen, ist außerdem eine Dienstvereinbarung gemäß § 37 Abs. 1 SächsDSG notwendig. In einem Fall, bei dem es um den Schutz von Computeranlagen in einem nicht

öffentlich zugänglichen Internetarbeitsraum ging, hatte das VG Osnabrück entschieden, dass eine Videoüberwachung in nicht öffentlich zugänglichen Räumen zulässig ist (vgl. VG Osnabrück, Urt. v. 10. April 2006 - 3 A 107/05). Das Gericht hielt die Maßnahme, die auf die allgemeine Datenerhebungsvorschrift des Landesdatenschutzgesetzes gestützt werden sollte, aufgrund einer Abwägung der beiderseitigen berechtigten Interessen für zulässig.

Den Einsatz von Videotechnik sollte die Schulleitung, die über die Maßnahme zu entscheiden und wegen deren Bedeutung regelmäßig die Schulkonferenz, Personal-, Schüler- und Elternvertretung zu beteiligen hätte, nur dann wählen, wenn der Zweck der Videoüberwachung schriftlich festgelegt wurde und die Erforderlichkeit (insbesondere keine anderen zumutbaren Maßnahmen zur Zweckerreichung bestehen) bejaht werden konnte. Des Weiteren muss die Abwägung unter Einbeziehung aller Grundrechtspositionen ergeben, dass die optisch-elektronische Einrichtung verhältnismäßig bleibt. Darüber hinaus ist ggf. wegen der mitverarbeiteten Beschäftigtendaten eine Vorabkontrolle gemäß § 10 Abs. 4 Nr. 3 SächsDSG durchzuführen. Vielfältige Umstände sind zu berücksichtigen: Je nachdem, ob es um den nicht öffentlich oder den öffentlich zugänglichen Bereich der Schule geht, wie weit die Beobachtung ausgestaltet wird, ob zu welchen Zeiten und wie lange aufgezeichnet wird, welche Personen Zugriff auf die Daten haben, welche datenschutzorganisatorischen Maßnahmen ergriffen worden sind, wird das Ergebnis der Prüfung sehr unterschiedlich sein. Ohne datenschutzrechtliche Anleitung des behördlichen Datenschutzbeauftragten oder eines fachkundigen Juristen ist eine Entscheidung und Einführung nicht zu empfehlen. In allen mir bisher bekannt gewordenen Fällen musste ich von einer Videoüberwachung oder -aufzeichnung wegen mangelnder Erforderlichkeit oder Unverhältnismäßigkeit der Maßnahme abraten.

8 Justiz

8.1 Erteilung von Auskünften aus aufbewahrtem Schriftgut

Im Berichtszeitraum war ich mit einer Frage zur Aufbewahrung von Unterlagen über strafprozessuale Ermittlungsverfahren und Auskünften daraus an öffentliche Stellen befasst.

Ein Petent wandte sich an mich und beschwerte sich darüber, dass sieben Jahre nach Abschluss eines gegen ihn gerichteten Verfahrens eine sächsische Staatsanwaltschaft auf Ersuchen einer öffentlichen Stelle eines anderen Bundeslandes dieser Einsicht in die noch aufbewahrten Aktenbestandteile gewährt hatte, indem sie Kopien dorthin übersandt hatte. Das Verfahren war damals rechtskräftig abgeschlossen worden, der Petent hatte die im Strafbefehl - es handelte sich also um ein Vergehen, eine Straftat von eher geringer Schwere - ausgeworfene Geldstrafe beglichen und war seitdem polizeilich nicht mehr in Erscheinung getreten. Der größte Teil der Akte war nach Ablauf der vorgesehenen Aufbewahrungs- und Aussonderungsfristen vernichtet worden, allerdings werden Urteile, aber auch Strafbefehle, und die Nachweise über die Strafvollstreckung für die Dauer von 30 Jahren aufbewahrt.

Auf meine Anfrage verwies die Staatsanwaltschaft auf die Aufbewahrungsfrist von 30 Jahren sowie auf § 474 StPO i. V. m. §§ 13, 14 EGGVG als Rechtsgrundlage für die Übermittlung und bemerkte, dass auch nach der Vernichtung von Aktenteilen nach bestimmten Fristen im Rahmen der gesetzlichen Vorschriften das Recht auf Einsicht in die weiter aufbewahrten Aktenbestandteile nicht eingeschränkt werde.

Rein formal ist diese Auffassung zutreffend. Gleichwohl habe ich dem SMJus mitgeteilt, dass ich an der Verfassungsmäßigkeit einer derartigen Praxis starke Zweifel habe.

Zwar war die Aufbewahrung und Aussonderung von Unterlagen zum damaligen Zeitpunkt im Berichtszeitraum noch nicht gesetzlich geregelt. Für eine Aufbewahrungsfrist von 30 Jahren für bestimmte Aktenbestandteile von Akten, die wegen der geringen Bedeutung der Verfahren bereits nach fünf Jahren vernichtet werden, besteht meines Erachtens keinerlei Notwendigkeit. Diese Aufbewahrungsdauer war auch deshalb bedenklich, weil im gesamten Aufbewahrungszeitraum eine Akteneinsicht für andere öffentliche Stellen - also für Dritte - möglich sein soll. Der Umgang mit länger aufzubewahrenden Aktenbestandteilen muss Belange der Betroffenen, insbesondere deren Grundrecht auf informationelle Selbstbestimmung, angemessen berücksichtigen und könnte sich an den bereits gesetzlich geregelten Verfahren bei der Polizei bzw. zu staatsanwaltschaftlichen Dateien orientieren. In beiden genannten Bereichen besteht nach § 43 Abs. 4 SächsPolG sowie § 489 Abs. 4 StPO eine maximale Löschungsprüf-

bzw. Aufbewahrungsfrist von zehn Jahren. Diese Frist sollte im Hinblick auf einen effektiven Grundrechtsschutz und die Einheit der Rechtsordnung („Fristengleichlauf“) der Maßstab für die Aufbewahrung und Behandlung von Unterlagen auch bei der Staatsanwaltschaft sein. Spätestens nach Ablauf dieser Zeit sollten auch bei der Staatsanwaltschaft aufbewahrte Unterlagen bzw. Aktenbestandteile aus Akten, die bereits vernichtet wurden, zumindest einer Auskunftssperre unterliegen.

Eine undifferenzierte Aufbewahrung sämtlicher Urteile und Strafbefehle für eine Dauer von 30 Jahren mit der Möglichkeit anderer Stellen, Auskünfte aus bzw. Einsicht in diese Unterlagen zu erhalten, ist meines Erachtens unverhältnismäßig und läuft darüber hinaus dem Resozialisierungsgedanken des § 51 BZRG (Verwertungsverbot bzgl. aus dem Bundeszentralregister getilgter Eintragungen) zuwider.

Ich hatte das SMJus deshalb darum gebeten, die Staatsanwaltschaften anzuhalten, Auskunfts- und Akteneinsichtsersuchen Dritter in den Fällen, in denen die (Haupt-)Akte bereits vernichtet wurde und nur noch Aktenbestandteile aufbewahrt werden, besonders genau zu prüfen. Auskünfte aus und Einsicht in derartige Unterlagen aus Verfahren, die seit über zehn Jahren abgeschlossen sind, sollten Dritten grundsätzlich verwehrt, d. h. nur in begründeten Ausnahmefällen gewährt werden.

Der nunmehr geschaffene § 13a SächsJG sieht die Möglichkeit vor, dass das SMJus eine Rechtsverordnung über das aufzubewahrende Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden und die hierbei zu beachtenden Aufbewahrungsfristen erlässt. Das Staatsministerium hat mir in diesem Zusammenhang einen ersten Entwurf zur Kenntnis und zur Stellungnahme übersandt.

8.2 Personenbezogene Daten in der Dolmetscherliste der Justiz

Eine Übersetzerin, die sich nach ihrer erfolgreichen Prüfung vereidigen lassen wollte, wandte sich an mich, weil sie Bedenken dagegen hatte, dass nach ihrer Beeidigung ihre Daten, wie Name, Anschrift, Telefonnummer, E-Mail-Adresse und Sprachprofil in die öffentliche, jedermann im Internet zugängliche Dolmetscher- und Übersetzerliste der sächsischen Justiz aufgenommen würden. Sie wolle gern für Behörden und Gerichte tätig werden, verstehe aber nicht, warum eine Liste mit diesen Daten nicht zum Beispiel verschlüsselt oder nur in einem Intranet verfügbar sein solle.

Ich hielt die Bedenken für durchaus berechtigt; es ist nicht jedermanns Sache, im Internet mit Namen, (Wohn-)Anschrift, Telefonnummer und E-Mail-Adresse präsent zu sein. Allerdings ist in § 6 SächsDolmG gesetzlich vorgesehen, dass die im Freistaat Sachsen öffentlich bestellten und allgemein beeidigten Dolmetscher, Übersetzer und Gebärden-

sprachdolmetscher in eine in elektronischer Form geführte Liste (Dolmetscher- und Übersetzerliste) eingetragen werden und diese Liste in maschinell lesbarer Form zur öffentlichen Einsichtnahme und zum Abruf bereitgehalten wird. Die Liste und deren Veröffentlichung dienen der schnellen und aktuellen Information interessierter Stellen, die Hilfe von Übersetzern und Dolmetschern benötigen. Eine Aufnahme in die Liste kann auch im wirtschaftlichen Interesse der Übersetzer und Dolmetscher selbst liegen, da sie bei Bedarf direkt von Auftraggebern kontaktiert werden können.

Die Übersetzerin wies ich auf die gesetzlichen Vorschriften und damit auf die gesetzliche Befugnis der Justizverwaltung zur Veröffentlichung der Kontaktdaten hin. Ich teilte ihr aber auch mit, dass weder dem Gesetzeswortlaut noch der Verwaltungsvorschrift des SMJus zum Sächsischen Dolmetschergesetz (VwV Dolmetscher) vom 29. August 2008 zu entnehmen ist, welche persönlichen Daten in die Dolmetscher- und Übersetzerliste eingetragen werden. Eine Pflicht zur Veröffentlichung bestimmter Daten besteht nicht. Meines Erachtens ist es - um der Informationsfunktion der Dolmetscher- und Übersetzerliste Rechnung zu tragen - ausreichend, den Namen, die Sprache(n) und ein Kontaktdatum (Telefonnummer und/oder E-Mail-Adresse) anzugeben und in die im Internet einzusehende Liste aufzunehmen. Dies würde beispielsweise Übersetzern und Dolmetschern entgegenkommen, deren Wohnadresse zugleich Büro- bzw. Arbeitsanschrift ist und die eine Veröffentlichung dieser Adresse im Internet nicht wünschen. Ich riet der Übersetzerin, sich zur Klärung dieser Frage an den für die Führung der Dometscher- und Übersetzerliste zuständigen Präsidenten des Oberlandesgerichts Dresden zu wenden.

Wie die Übersetzerin mir kurz darauf telefonisch mitteilte, sei ihr Wunsch nach Eintragung nur bestimmter Daten in die Dolmetscher- und Übersetzerliste akzeptiert worden.

8.3 Datenerhebung bei Gefangenen für die GEZ

Ein Gefangener einer sächsischen JVA wandte sich mit folgendem Vortrag an mich: In der JVA sei Voraussetzung für die Genehmigung zur Nutzung eines Fernsehgerätes, dass durch den Gefangenen ein Vordruck der GEZ ausgefüllt werde. Dieser Vordruck enthalte einen Textbaustein, durch den offenbart werde, dass der Unterzeichner in der JVA inhaftiert ist. Darüber hinaus seien Angaben zur früheren Anschrift und zu Dritten (Familienangehörige, Partner) zu machen. Ohne diesen Vordruck ausgefüllt zu haben, habe ein Antrag auf ein Fernsehgerät keine Aussicht auf Genehmigung.

Die JVA teilte mir aufgrund meiner Bitte um Erläuterung mit, dass der Sachverhalt zutreffend geschildert sei und übersandte die entsprechenden Unterlagen, die von den

Inhaftierten auszufüllen seien. Weiterhin stellte sie dar, dass die Gefangenen regelmäßig eine Einverständniserklärung zur Weitergabe persönlicher Daten an den MDR unterzeichnen. Neben Namen, Geburtsdatum und der letzten Wohnanschrift müssen die Inhaftierten dort auch den Beginn und das voraussichtliche Ende der Haft angeben. Darauf aufbauend füllen die Gefangenen zur Nutzung eines Fernsehgerätes in der JVA ein Formular der GEZ zum Rundfunkteilnehmerverhältnis aus. In diesem muss angegeben werden, ob unter der früheren Privatanschrift weiterhin Rundfunkgeräte vorhanden sind und zum Empfang bereitgehalten werden. Sofern dies der Fall ist, muss der Name des Familienangehörigen bzw. Partners mitgeteilt werden, der dieses Rundfunkgerät derzeit nutzt. Zur organisatorischen Vereinfachung wurde durch die GEZ eingerichtet, dass dort die Justizvollzugsanstalten über ein Sammelkonto verfügen. Von Gefangenen erhebt die GEZ keine Rundfunkgebühren. Falls der Gefangene ein Konto bei der GEZ unter seinem Namen und der früheren Anschrift führt, muss die Änderung im Rundfunkteilnehmerverhältnis mit Hilfe des Formulars angezeigt werden.

Nach rechtlicher Prüfung und Sichtung der von der JVA übersandten Vordrucke für Inhaftierte teilte ich der JVA meine datenschutzrechtlichen Bedenken zu diesem Vorgang mit und bat um Änderung der Formulare. Der Gefangene hatte in der damaligen Situation keine Möglichkeit ein Fernsehgerät zu nutzen, ohne dass der GEZ mitgeteilt wurde, dass er in der JVA inhaftiert war. Außerdem musste er, sofern er bereits bei der GEZ angemeldet war, personenbezogene Angaben über Dritte machen. Problematisch daran war, dass die GEZ weder zum Kreis der Empfänger von Übermittlungsdaten nach § 180 StVollzG, der die Nutzung und Verarbeitung personenbezogener Daten im Strafvollzugsdienst regelt, gehört, noch befugt ist, bei Rundfunkteilnehmern personenbezogene Daten über Dritte zu erheben.

Sicher ist bei Gefangenen, die von der Rundfunkgebührenpflicht befreit werden möchten, die Übermittlung des Umstandes, dass sie inhaftiert sind, notwendig. Dann ist gegen diese Angabe auch nichts einzuwenden. Aber selbst in diesen Fällen, in denen der Gefangene den Umstand seiner Inhaftierung der GEZ zu offenbaren bereit ist, ist die Erhebung der voraussichtlichen Haftdauer und bei bisherigen Teilnehmerkontoinhabern die Erhebung des Namens von Ehegatten/Partnern des Gefangenen durch die GEZ unzulässig. Die Genehmigung eines Fernsehgerätes durch die JVA darf jedenfalls nicht davon abhängig gemacht werden, dass der Gefangene sein Einverständnis in die Übermittlung des voraussichtlichen Endes der Haft an den MDR erklärt bzw. in der Erklärung den Namen des Ehegatten/Partners angibt.

Welche Angaben für die Klärung zum Rundfunkteilnehmerverhältnis notwendig sind, lässt sich den üblicherweise gebräuchlichen GEZ-Formularen für An-, Um- und Abmeldungen entnehmen. Namen dritter Personen werden in keinem der Fälle verlangt.

Diese Daten sind für die Aufgabenerfüllung der GEZ nicht erforderlich (kein Rundfunkteilnehmer hat gegenüber der GEZ anzugeben, wie lange er unter einer angegebenen Adresse zu wohnen gedenkt; die üblichen Formulare enthalten auch keine entsprechenden Felder). Es obliegt auch nicht der JVA, der GEZ zu mehr personenbezogenen Informationen zu verhelfen als die GEZ bei „üblichen“ An-, Um- oder Abmeldungen erheben darf und erhebt.

Für Gefangene, die der GEZ nicht offenbaren möchten, dass sie inhaftiert sind, und die bereit sind, deshalb Rundfunkgebühren zu zahlen bzw. - soweit sie bereits über ein Teilnehmerkonto bei der GEZ verfügen - weiterzuzahlen, sollte ein alternatives Verfahren gefunden werden, das beispielsweise so ausgestaltet sein könnte, dass diese Gefangenen das Fernsehgerät einzeln normal (mittels der üblichen GEZ-Formulare) anmelden und bei der GEZ ein individuelles Teilnehmerkonto erhalten bzw. ihr bestehendes Teilnehmerkonto behalten und der GEZ ihre Adressänderung mitteilen.

Die JVA hat mir daraufhin mitgeteilt, dass künftig im Rahmen der Antragstellung hinsichtlich der Rundfunkgebührenbefreiung die voraussichtliche Haftdauer und Namen von Ehegatten/Partnern der Gefangenen nicht mehr übermittelt werden sollen. Die Einverständniserklärung würde entsprechend geändert werden. Um Gefangenen, die nicht bereit sind, gegenüber der GEZ den Umstand der Inhaftierung zu offenbaren, die Möglichkeit der Anmeldung eines Fernsehgerätes zu eröffnen, werde die JVA diese Gefangenen künftig das allgemein übliche Anmeldeformular der GEZ verwenden lassen. Als Anschrift könne der Gefangene dann die Adresse, also Straße, Hausnummer, Ort und Postleitzahl angeben, ohne auf den Status einer JVA hinweisen zu müssen. Für diese Lösung danke ich; ich halte sie für bedeutend besser als den vorherigen Zustand.

8.4 Löschung von Lichtbildern nach unrechtmäßiger Wohnungsdurchsuchung

Eine Petentin wandte sich mit der Frage, ob eine Staatsanwaltschaft Informationen über sie zu Recht gespeichert habe, an mich. Dieser Frage ging voraus, dass ihre Wohnung aufgrund eines Ermittlungsverfahrens gegen ihren Lebensgefährten durchsucht worden war. Diese Durchsuchung hatte sich als rechtswidrig herausgestellt, wie das LG Dresden in einem Beschluss festgestellt hatte. Im Rahmen dieser Wohnungsdurchsuchung wurden u. a. Lichtbilder der sich in der Wohnung befindlichen Fotografien der Petentin und ihres minderjährigen Sohnes sowie weiterer Personen angefertigt.

Der Lebensgefährte hatte bei der Staatsanwaltschaft bereits die Herausgabe der beschlagnahmten Gegenstände und die Löschung der Informationen und Bilder beantragt, jedoch keine Antwort erhalten.

Daraufhin wandte ich mich an die Staatsanwaltschaft und bat um Stellungnahme. Von dieser erhielt ich die Mitteilung, dass die Lichtbilder und Skizzen der Wohnung Bestandteil der Ermittlungsakte geworden sind und daher erst nach Ablauf der Aufbewahrungsfrist zusammen mit der gesamten Akte vernichtet werden könnten. Auch seien auf den Fotos keine Personen detailliert zu erkennen, sondern nur schemenhaft, so dass die Persönlichkeitsrechte nicht verletzt sein könnten.

Eine Mitteilung an den Lebensgefährten sei versehentlich unterblieben, da das Hauptaugenmerk auf die Herausgabe der Gegenstände gerichtet worden sei und der Antrag auf Löschung der Daten bzw. auf Mitteilung übersehen worden sei.

Die Einschätzung der Staatsanwaltschaft konnte ich so nicht teilen. Die Erkennbarkeit der Personen auf den Lichtbildern ist nicht entscheidend. Allein die fotografische Fixierung des persönlichen Lebensbereiches eines Menschen stellt einen schwerwiegenden Eingriff in dessen Persönlichkeitsrecht dar (vgl. LG Hamburg, StV 2004, 368 m. w. N.). Hier lag nicht nur ein Eingriff in die Persönlichkeitsrechte des Beschuldigten, sondern auch in diejenigen der Petentin und ihres Sohnes vor.

Da eine Löschung der Lichtbilder nach § 20 Abs. 2 SächsDSG nur möglich ist, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist, habe ich die Staatsanwaltschaft aufgefordert, die unzulässig erlangten Daten zumindest nach § 21 SächsDSG zu sperren. Damit wird der Schutz Betroffener insofern gewährleistet, als die Sperrung zur Folge hat, dass diese Daten gesondert aufzubewahren sind und ohne Einwilligung des Betroffenen nicht mehr genutzt werden dürfen.

Auch habe ich die Staatsanwaltschaft gebeten, dem Lebensgefährten der Petentin dies mitzuteilen.

Die Staatsanwaltschaft ist dem nachgekommen und hat die Lichtbildmappe der Sachakte entnommen und gesondert verwahrt. Darüber hat sie den Lebensgefährten unterrichtet.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Controllingsystem Bundesfernstraßenbau

Erforderliche Modernisierungen der öffentlichen Verwaltung werden zunehmend durch E-Government-Lösungen angestrebt. Nicht selten werden dabei Software-Entwicklungen vorangetrieben, bevor für die mit dem Vorhaben verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht erforderlichen Rechtsgrundlagen geschaffen wurden. Ein Beispiel ist der nachstehend dargestellte Vorgang.

Das durch das BMVBS geplante Vorhaben Controllingsystem Bundesfernstraßenbau (CSBF) sollte personenbezogene Daten der Auftragnehmer und Mitarbeiter der Straßenbauverwaltung der Länder nach einheitlichen Vorgaben automatisiert und zentral verarbeiten, um mit diesen Informationen ein Frühwarnsystem für eine wirksame Korruptionsbekämpfung zu unterstützen. Die nach Art. 85 Abs. 4 GG geregelte Aufsicht über die Bundesauftragsverwaltung durch die Länder gestattete zwar die Vorlage von Akten. Es mangelt jedoch an einer normenklaren und dem Bestimmtheitsgrundsatz genügenden bereichsspezifischen Regelung für die Übermittlung personenbezogener Daten beispielsweise im Bundesfernstraßengesetz.

Aufgrund der Beratung und Einwirkung der Datenschutzbeauftragten des Bundes und der Länder auf die Software-Entwicklung wurde auf die beabsichtigte Erfassung und Übermittlung personenbezogener Daten teilweise verzichtet oder man beschränkte sich. Vermieden wurde beispielsweise die vorratsweise Erfassung und Übermittlung von Mitarbeiterdaten der Behörden. Ich habe das SMWA darauf hingewiesen, dass eine eigene Erfassung und Verarbeitung personenbezogener Daten für den beabsichtigten Zweck durch das BMVBS möglich ist, die ohnehin durch Verordnung zu melden oder zu veröffentlichen sind. Rechtsgrundlage wäre in diesem Fall §§ 12, 13 SächsDSG gewesen.

Nach meiner Empfehlung entschied sich das SMWA zwar für eine Teilnahme an dem Datenbank-Verfahren, lehnte aber die geforderte Übermittlung der Namen von beteiligten Ingenieurbüros aus datenschutzrechtlichen Gründen ab. Die Staatsregierung hatte mich auch im Übrigen in meinem datenschutzrechtlichen Anliegen weitgehend unterstützt.

9.2 Gewerberecht

9.2.1 Namensschild im Taxi

Bedenken wegen einer möglichen Verletzung der Persönlichkeitsrechte von Taxifahrern erreichten mich, weil eine Änderung der Taxiordnung eines Landkreises verlangte, im Innern des Fahrzeugs für den Fahrgast gut sichtbar ein Schild mit der Unternehmeranschrift sowie dem Vor- und Familiennamen des Fahrpersonals anzubringen. Es sei zum Schutz des Persönlichkeitsrechts der Taxifahrer auf die Angabe des Vor- und Familiennamens des Fahrpersonals zu verzichten.

Gemäß § 1 Abs. 1, 2 SächsPBefZuVO sind die Landkreise und kreisfreien Städte für den Vollzug des Personenbeförderungsgesetzes zuständig und zum Erlass von Rechtsverordnungen ermächtigt. Beim Erlass von Taxiordnungen durch die Landkreise und kreisfreien Städte sind die Vorgaben des Bundes in der Verordnung über den Betrieb von Kraftfahrunternehmen im Personenverkehr maßgeblich und zu beachten. § 27 BOKraft fordert in Taxen das Anbringen der nach außen und innen wirkenden Ordnungsnummer der Genehmigungsbehörde an der rechten unteren Ecke der Heckscheibe und im Wageninnern an einer für den Fahrgast gut sichtbaren Stelle ein Schild mit Namen und Betriebssitz des Unternehmers.

Insofern ist eine zusätzliche Forderung zum Anbringen der Vor- und Familiennamen des Fahrpersonals in einer Taxiordnung durch die Rechtsnorm des Bundes nicht vorgegeben. Es ist aber auch nicht abschließend geregelt und dem Verordnungsgeber in den Ländern bleibt ein Spielraum, um bestehende Gesetze zu ergänzen. Tatsächlich werden durch die Regelung das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung des Fahrpersonals beeinträchtigt, dem die Entscheidungsfreiheit genommen wird, fremden Fahrgästen seinen Vor- und Zunamen zu offenbaren.

Allerdings können Eingriffe in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung dann gerechtfertigt sein, wenn sie im überwiegenden Allgemeininteresse erfolgen. So hat u. a. das Hamburgische OVG (Urteil vom 6. August 2004, Az. 1 Bf 83/03) in einem vergleichbaren Fall entschieden, dass eine Beeinträchtigung zum Schutz überwiegender Interessen der Allgemeinheit gerechtfertigt sei. Dem Urteil lag die Regelung der Hamburgischen Taxiordnung zugrunde, nach der im Wageninnern an einer für den Fahrgast gut sichtbaren Stelle ein Schild mit Lichtbild sowie Ruf- und Familiennamen des Taxifahrers anzubringen ist.

Zumindest erscheint es vertretbar, in einem Bereich der wegen seiner Grundversorgungswirkung öffentlich-rechtlich zu regulieren ist, die Anonymität des Fahrpersonals im Hinblick auf deren Namen aufzuheben, wird dadurch doch auch ein anderer Umgang

im Miteinander zwischen Fahrpersonal und Fahrgästen bewirkt werden können, u. a. auch deshalb, weil die Fahrer von ihren Gästen mit Namen angesprochen werden können und eventuellem Fehlverhalten des Fahrpersonals besser nachgegangen werden kann. Demgegenüber erscheint die Preisgabe des Vor- und Zunamens auch im Hinblick auf mögliche (theoretische) Gefährdungen des Fahrpersonals regelmäßig als ein nicht so gravierender Eingriff.

Dennoch handelt es sich nicht um eine von mir gewollte und empfohlene Rechtssetzung, ist doch die erhobene Forderung, Vor- und Zunamen nicht nennen zu müssen, auch aus Persönlichkeitsrechtsgründen seitens der Taxibediensteten nachzuvollziehen. Ich werde, soweit sich ein sächsischer Verordnungsgeber für eine derartige Regelung entscheidet, diese nicht aktiv unterstützen.

9.3 Industrie- und Handelskammern; Handwerkskammern

9.3.1 Datenerhebungs-, Datenweitergabebefugnis und -pflicht der Kammern

Bereits in 6/9.3 hatte ich mich zu der zulässigen Übermittlung von Besteuerungsgrundlagen durch die Finanzämter an die Industrie- und Handelskammern und Handwerkskammern und zur Festsetzung der Kammerbeiträge auf der Grundlage von § 113 Abs. 2 HwO, § 9 Abs. 2 IHKG i. V. m. § 31 Abs. 1 AO geäußert. Da immer wieder Nachfragen zu solchen Datenübermittlungen bei mir eingehen, verweise ich erneut auf meinen Beitrag.

In Bezug auf die von den Kammern geführten Registerdaten bestehen immer wieder Befürchtungen im Hinblick auf einen Adresshandel. Betroffene klagen über die Weitergabe ihrer (personenbezogenen) Daten an Versicherungs- und Adresshandelsunternehmen und mutmaßen Weitergaben durch die Industrie- und Handelskammern bzw. die Handwerkskammern. Die gesetzlichen Grundlagen sind den Anfragenden dabei in der Regel nicht gegenwärtig. Vorauszusetzen ist, dass Daten juristischer Personen, soweit auch ein mittelbarer Personenbezug auszuschließen ist, keinen datenschutzrechtlichen Einschränkungen unterliegen. Lediglich personenbezogene Daten unterliegen dem Datenschutz (§ 3 Abs. 1 SächsDSG).

Nach § 9 Abs. 4 IHKG sind die Industrie- und Handelskammern befugt, Name, Firma, Anschrift und Wirtschaftszweig der Kammerzugehörigen zur Förderung von Geschäftsabschlüssen und zu anderen wirtschaftlichen Zwecken an nicht-öffentliche Stellen zu übermitteln. Den Betroffenen wird ein Widerspruchsrecht lediglich in Bezug auf die übrigen in Absatz 1 genannten - aus den Gewerbeanzeigen stammenden - Daten eingeräumt (§ 9 Abs. 4 Satz 2 IHKG). Im Hinblick auf die Übermittlung anderer Daten als denen nach § 9 Abs. 1 IHKG gilt das Sächsische Datenschutzgesetz. Als Übermittlung

gilt auch - dies nebenbei - die in der Praxis immer mehr Bedeutung erlangende Internetveröffentlichung von Firmendaten in Branchendatenbanken. Im Hinblick auf Datenübermittlungen unterliegen die Industrie- und Handelskammern einer Zweckbindung, d. h., dass sie bei der Übermittlung zu prüfen haben, ob die Datenweitergabe gesetzlich durch den Zweck, den der Datenempfänger vorgibt, gedeckt ist.

Gemäß § 6 Abs. 2 HwO ist eine Einzelauskunft aus der Handwerksrolle jedermann zu erteilen, der ein berechtigtes Interesse glaubhaft darlegt. Die personenbezogenen Daten der Handwerksrolle sind in Anlage D der Handwerksordnung aufgeführt. Neben der Bezeichnung der Firma und des Handwerks enthält die Handwerksrolle, Namen, Vornamen und Anschriften. Ausdrücklich lässt der Gesetzgeber auch eine listenmäßige Übermittlung von Daten an nicht-öffentliche Stellen zu, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat (vgl. § 6 Abs. 2 Satz 2 HwO). Dies wird generell im Hinblick auf die Übermittlung lediglich des Vor- und Familiennamens des Betriebsinhabers oder des gesetzlichen Vertreters oder des Betriebsleiters oder des für die technische Leitung des Betriebs Verantwortlichen persönlich haftenden Gesellschafters, die Firma, das ausgeübte Handwerk oder die nach Anschrift der gewerblichen Niederlassung angenommen (§ 6 Abs. 2 Satz 3 HwO). Der Gewerbetreibende hat nach § 6 Abs. 2 Satz 4 HwO die Möglichkeit, Einzel- und Listenauskünften zu widersprechen. Darüber hinaus wird man bei der Beantragung eines listenweisen Datenbezugs eine erhöhte Prüfungspflicht der Kammer fordern müssen, insbesondere was die Übermittlung an einzelne, von den Betroffenen benannte erkennbare Empfängergruppen wie z. B. Versicherungen angeht. Im Hinblick auf Einzelauskünfte besteht seitens der Kammer nach dem Gesetz eine Auskunftspflicht, bei den Listenauskünften eine Auskunftsbefugnis und nur ein Anspruch des Auskunftsersuchenden auf eine ermessensfehlerfreie Bescheidung.

Den verkammerten Betroffenen ist zu raten, die Widerspruchsmöglichkeiten nach ihren Bedürfnissen genau zu prüfen. Die Handwerksordnung sieht für den Widerspruch keine besondere Form vor, so dass auch mündlich oder fernmündlich widersprochen werden kann. Gegenüber öffentlichen Stellen besteht kraft Gesetzes keine Möglichkeit, per Widerspruch Auskünfte zu verhindern.

Den Kammern ist zu empfehlen, die Datenübermittlungsbefugnisse behutsam auszuüben und sich ggf. durch die Einholung von Einwilligungen abzusichern.

Die Datenübermittlungen an öffentliche Stellen richten sich gemäß § 9 Abs. 6 IHKG nach dem Sächsischen Datenschutzgesetz, also § 14 SächsDSG, bei der Handwerksordnung nach § 6 Abs. 3. Die Empfänger haben die Daten zweckgebunden zu verwenden (vgl. § 6 Abs. 4 HwO).

10 Gesundheit und Soziales

10.1 Gesundheitswesen

10.1.1 Verhinderung der Akteneinsicht bei einem Beauftragten einer berufsständischen Kammer

Das Recht auf Auskunft - und im speziellen der datenschutzrechtliche Akteneinsichtnahmeanspruch gemäß § 18 SächsDSG - gewährt Betroffenen ein subjektiv-öffentliches Recht sich Kenntnis zu verschaffen, welche Daten durch welche öffentliche Stelle zu welchem Zweck und auf welcher Rechtsgrundlage zu seiner Person gespeichert sind. Nach § 18 Abs. 1 SächsDSG ist Betroffenen durch die Daten verarbeitende Stelle auf Antrag kostenfrei und ohne unzumutbare Verzögerung Auskunft zu erteilen über die zur Person gespeicherten Daten. Sind die personenbezogenen Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, hat ihm die Daten verarbeitende Stelle auf Verlangen Einsicht in die Akten zu gewähren (§ 18 Abs. 3 SächsDSG). Grundsätzlich besteht dieser Auskunftsanspruch des Betroffenen voraussetzungslos. Vor dem Hintergrund, dass das Auskunftsrecht als Betroffenenrecht eine wesentliche Vorkehrung zum Schutz des Rechts auf informationelle Selbstbestimmung ist, sind Fälle der Missachtung dieses Betroffenenrechts besonders kritisch zu bewerten. Von einem Beispiel, bei dem eine wirksame Akteneinsichtnahme des Betroffenen gar unterbunden wurde, sei hier beispielhaft berichtet.

Ein Betroffener wandte sich an mich, um ihn bei der Wahrnehmung seiner Auskunftsrechte gegenüber einer berufsständischen Kammer zu unterstützen. Der Betroffene hatte zuvor bereits schriftlich die Einsichtnahme in die zu seiner Person bei der Kammer geführten Akten beantragt. Zu den Vorgängen gehörten auch Akten, die der Menschenrechtsbeauftragte der Körperschaft zur Person des Betroffenen im Zusammenhang mit dessen Beschwerden geführt hatte. So war Schriftverkehr des Beauftragten mit ehemals behandelnden Ärzten des Betroffenen entstanden. Der Menschenrechtsbeauftragte teilte dem Betroffenen auf einem Briefbogen, der diesen als Menschenrechtsbeauftragten der Kammer auswies, mit, dass er die beantragte Akteneinsicht im Hinblick auf seinen Datenbestand nicht gewähren werde.

Meine Kontrollrechte gemäß § 27 SächsDSG wahrnehmend bat ich daraufhin die Kammer um Stellungnahme und wies auf die Bedeutung des Auskunftsrechts hin, auf dessen Grundlage die Geltendmachung weitergehender Rechte der Betroffenen, zum Beispiel auf Berichtigung oder Löschung der personenbezogenen Daten, erst ermöglicht wird. Als Reaktion auf mein Schreiben wurde mir mitgeteilt, dass der Betroffene in die sonstigen bei der Kammer vorliegenden Vorgänge Einblick nehmen dürfe. Die Einsichtnahme in die beim Menschenrechtsbeauftragten geführten Akten wurde aber weiterhin

verweigert. Zur Begründung stellte die Kammer dar, dass der Menschenrechtsbeauftragte nicht als Amtsträger der Kammer, sondern als Privatperson gehandelt habe, und die Rechte Dritter, nämlich der an der Korrespondenz beteiligten Ärzte, zu schützen seien. Auch wurde § 13 Abs. 2 der Hauptsatzung der Kammer hervorgehoben. Danach hätten ehrenamtlich Tätige über die ihnen bei ihrem Ehrenamt bekannt gewordenen Tatsachen Verschwiegenheit zu wahren.

Daraufhin teilte ich der öffentlichen Stelle mit, dass meines Erachtens der Menschenrechtsbeauftragte Amtsträger sei, da dieser von der Kammer als Beauftragter bestellt gewesen sei und auf Briefbogen der Kammer Schriftverkehr führte, so dass sich das Recht auf Einsichtnahme in die zur Person geführten Akten im Sinne von § 18 Abs. 3 SächsDSG auch auf die Akten und Vorgänge erstrecke, die der Beauftragte in dieser Funktion zu dem Betroffenen angelegt habe. Ich forderte die Kammer auf, die Unterlagen, Akten und Dateien, die personenbezogene Daten zu dem Betroffenen enthielten und sich bis dahin im persönlichen Gewahrsam des Menschenrechtsbeauftragten befunden haben sollen, in den Diensträumen der Kammer zu verwahren und dem Betroffenen eine Einsichtnahme in die zu seiner Person geführten Akten zu gewähren.

Daraufhin übersandte mir die Kammer eine Mehrfertigung eines Schreibens an den Betroffenen. In diesem teilte sie ihm mit, dass der Menschenrechtsbeauftragte in der Annahme, dass dies aus Gründen der ärztlichen Schweigepflicht notwendig gewesen sei, ärztliche Berichte und Stellungnahmen an die jeweiligen Verfasser zurückgesandt habe. Nachdem ich der Kammer eine datenschutzrechtliche Beanstandung in Aussicht stellte, teilte sie mir zu dem Sachverhalt weiter mit, dass es von dem Rücksendevorgang im Einzelnen keine Unterlagen mehr gebe und man nicht in der Lage sei, die Adressaten bzw. die zurückgesendeten Akten zu rekonstruieren. Zudem betonte die Kammer erneut, dass das Zurücksenden der Arztunterlagen und der Korrespondenz nach den Angaben des Menschenrechtsbeauftragten erfolgt sei, um die schutzwürdigen Interessen der behandelnden Ärzte zu bewahren.

Das Auskunftsrecht wurde damit nach meiner Überzeugung durch die Kammer schwerwiegend verletzt. Die zu dem Betroffenen geführten Akten und Unterlagen enthielten Einzelangaben über persönliche Verhältnisse des Betroffenen. Zwar war davon auszugehen, dass auch personenbezogene Daten von Ärzten verarbeitet worden waren, doch immer in Bezug auf den Betroffenen und dessen Beschwerden.

Handlungen der Amtsträger öffentlicher Stellen sind der nach dem Sächsischen Datenschutzgesetz pflichtigen Stelle zuzurechnen, seien es Bedienstete oder andere für öffentliche Stellen tätigen Personen, die personenbezogene Daten verarbeiten (§ 6 Abs. 1 SächsDSG). Nach den Angaben der Kammer konnte der bestellte Beauftragte Kraft sei-

ner Funktion selbständig Schriftverkehr mit den von dem Betroffenen benannten Ärzten führen und erhob in diesem Zusammenhang nach seinen eigenen Einschätzungen „äußerst vertrauliche Daten“. Die durch den Beauftragten veranlasste und vorgenommene Datenverarbeitung erfolgte auch mit Kenntnis der Kammer. Die Rechtsabteilung der Kammer war ausweislich des Schriftverkehrs frühzeitig mit dem Beauftragten in Kontakt zu der Angelegenheit getreten bzw. stimmte sich mit ihm ab. Durch eine rechtzeitige Sicherung des Aktenbestandes in den Diensträumen der Kammer hätte ein Vorenthalten der Schriftstücke vermieden werden können. Die Rücksendung der Aktenstücke und die Verkürzung der Akteneinsichtnahmemöglichkeit des Betroffenen war auch nicht nach § 18 Abs. 5 Nr. 3 SächsDSG gerechtfertigt gewesen. Nach dieser Vorschrift muss eine Auskunftserteilung unterbleiben, wenn berechtigte Interessen eines Dritten überwiegen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Nach dem Gesetz ist eine Abwägung vorzunehmen. Aus § 18 Abs. 6 SächsDSG ergibt sich, dass die ablehnende Entscheidung, also Akteneinsicht nicht oder nicht vollständig zu gewähren, zu begründen ist; Entscheidungen über Akteneinsichtnahmegesuche sind Verwaltungsakte. Die wiederholt vorgebrachten zu schützenden Interessen der Ärzte wurden aber nicht weiter begründet. Auch wurden besondere Umstände, die ausnahmsweise ein Vorenthalten ärztlicher Aufzeichnungen im Arzt-Patientenverhältnis gegenüber dem Patienten rechtfertigen, nicht dargetan. Soweit schützenswerte Daten in dem Vorgang enthalten gewesen waren, wären diese bei der Einsichtnahme des Betroffenen zu schwärzen gewesen (vgl. § 18 Abs. 5 Nr. 3 SächsDSG). Eine generelle Verweigerung der Einsichtnahme gegenüber dem Betroffenen, da personenbezogene Daten Dritter in dem Vorgang enthalten sind, war jedoch nicht zulässig, da keine überwiegenden berechtigten Interessen Dritter begründet werden können. Demnach wurde dem Betroffenen rechtsgrundlos Akteneinsicht verwehrt.

Zu dem Verstoß gegen die Vorschrift des § 18 Abs. 3 Satz 1 SächsDSG kam hinzu, dass auch die Rechtspflicht zur Unterstützung bei meiner Kontrolle nach § 28 SächsDSG nur unzureichend erfüllt werden konnte. Aufgrund der nicht revisionsfähigen Rücksendung der Originalunterlagen wurden diese meiner Kontrolle entzogen, obwohl zum Zeitpunkt dieser rechtswidrigen Handlung mein kontrollbehördliches Tätigwerden schon lange bekannt war. Von einer Beanstandung gemäß § 29 SächsDSG konnte ich nach alledem nicht absehen.

Die Kammer teilte mir abschließend mit, dass der bisher als Menschenrechtsbeauftragter fungierende Mediziner zwischenzeitlich aus dem Kammervorstand ausgetreten sei und nunmehr ein anderes Vorstandsmitglied die Funktion des Menschenrechtsbeauftragten wahrnehme würde. Mir wurde versichert, dass künftig auch die Vorgänge unter Beteiligung des Menschenrechtsbeauftragten ausschließlich bei der Hauptgeschäftsstelle

der Kammer unter Beachtung sämtlicher verwaltungsverfahrens- und datenschutzrechtlicher Vorschriften geführt würden.

10.1.2 Auskünfte aus Todesbescheinigungen der Gesundheitsämter bei Anfragen zu Verstorbenen

Gesundheitsämter registrieren nach dem Bestattungsgesetz Todesbescheinigungen und bewahren diese 30 Jahre lang auf. Mehrfach wandten sich Behörden und Hinterbliebene an mich, insbesondere wenn es um Angaben zu Todesart und -ursachen ging, weil seitens der Gesundheitsbehörden Unsicherheit bestand, ob Informationen aus der Todesbescheinigung beauskunftet werden durften. Genaugenommen handelt es sich bei den Angaben in den Dokumenten der Gesundheitsämter nicht um personenbezogene Daten, da diese nur die lebenden Personen betreffen (vgl. § 3 Abs.1 SächsDSG). Dennoch beantworte ich - wegen des engen Sachzusammenhangs zu einem evtl. noch zu Lebzeiten geäußerten Willens des Verstorbenen - auch Anfragen, die den postmortalen Persönlichkeitsschutz betreffen.

Gemäß § 14 Abs. 7 Nr. 1 SächsBestG dürfen Antragstellern durch das Gesundheitsamt bei berechtigtem Interesse an der Kenntnis der Todesumstände der verstorbenen Person Auskünfte aus der Todesbescheinigung erteilt werden. Die Vorschrift zur Auskunft unterscheidet dabei nicht zwischen dem vertraulichen und dem nichtvertraulichen Teil der Todesbescheinigung (vgl. § 14 Abs. 2 SächsBestG). Dennoch ist in der Praxis im Hinblick auf die Auskunftsanforderungen zu differenzieren, ob z. B. Auskünfte zur Todesart, d. h., ob es sich um einen natürlichen, nichtnatürlichen oder unaufgeklärten Tod gehandelt hat (vgl. § 14 Abs. 2 Nr. 6 SächsBestG), oder zur Krankheitsgeschichte (Nr. 7) oder zu unmittelbaren, mittelbaren Todesursachen und wesentlichen Krankheiten erfragt werden (Nr. 8). Auf Seiten des Antragstellers wird im Übrigen lediglich ein berechtigtes Interesse, d. h. ein von der Rechtsordnung anerkanntes Interesse verlangt. Für die Abwägung und Entscheidung sind der ausdrücklich geäußerte oder mutmaßliche Wille des Verstorbenen und die Interessen der Hinterbliebenen heranzuziehen.

Häufig sind auch Ersuchen von Berufsgenossenschaften wegen zu bearbeitender Versicherungsfälle, von gesetzlichen Krankenkassen wegen Schadensersatzfragen oder anderen Sozialversicherungsträgern nach dem Sozialgesetzbuch. Auch dann kann eine Übermittlung auf § 14 Abs. 7 Satz 3 Nr. 1 SächsBestG gestützt werden, da die Kenntnis der konkreten Todesumstände und der Todesursachen im Hinblick auf Zahlungen an Hinterbliebene oder von Schadensersatzansprüchen durch die Krankenkasse zur gesetzlichen Aufgabe der Sozialversicherungsträger gehören und insofern ein berechtigtes Interesse bejaht werden kann. Dabei können Auskünfte grundsätzlich auch durch Übersendung von Kopien der Todesbescheinigung oder Teilen der Todesbescheinigung er-

teilt werden. Zu beachten ist aber, dass auf der Empfängerseite, d. h. beim Leistungsträger, die Datenerhebung auf die Daten und Umstände beschränkt ist, die für die gesetzliche Aufgabenerfüllung und Prüfung des Zusammenhangs erforderlich sind (§ 100 Abs. 1 Nr. 1 SGB X). Soweit z. B. nur bestimmte Angaben aus den Todesbescheinigungen benötigt werden, sind aus Gründen der Datensparsamkeit Teilschwärzungen durch das Gesundheitsamt auf den zu übermittelnden Ablichtungen der Todesbescheinigungen vorzunehmen. Die Aktenführung und Datenverarbeitung unterliegen nach der Übermittlung an einen Sozialversicherungsträger dem Sozialgeheimnis.

10.1.3 Elektronische Gesundheitskarte - Der Basis-Rollout der mit Fotos versehenen Versichertenkarten in Sachsen

Bisher hatte ich mehrfach über den Stand des Projekts der elektronischen Gesundheitskarte und des Testgebiets im sächsischen Landkreis Löbau-Zittau berichtet (vgl. 14/ 10.1.1, 13/10.1.1, 12/10.1.2). Bis zum Ende des Berichtszeitraums hatten sich erneut Veränderungen ergeben. U. a. wurde das elektronische Rezept zwischenzeitlich zurückgestellt. Zu viele Probleme hatten sich bei den technischen Prozessen der teilnehmenden Apotheken ergeben.

Die Anzahl der Arztpraxen, in denen bisher testweise elektronische Gesundheitskarten zum Einsatz gekommen waren, blieb bis zum Ende des Berichtszeitraums mit über 60 Praxen überschaubar. Die Anwendungsfälle bewegten sich bis dahin insgesamt in einem niedrigen vierstelligen Bereich.

In einem sogenannten „Basis-Rollout“ beginnt zum Ende des Berichtszeitraums die sukzessive und flächendeckende Ausstattung der Leistungserbringer mit Kartenterminals und angepassten Primärsystemen. Damit soll eine Voraussetzung für die Ausgabe elektronischer Gesundheitskarten in der ostsächsischen Region Löbau-Zittau, in der etwa 600.000 Menschen leben, durch die beteiligten Krankenkassen - insbesondere die AOK - geschaffen werden. Damit sollen in Sachsen über zehn Prozent der Versicherten in absehbarer Zeit eine elektronische Gesundheitskarte erhalten. Unter Beteiligung von ca. 950 Ärzten und 15 Krankenhäusern der Region sollen die Voraussetzungen für spätere flächendeckende Onlinetests geschaffen werden.

Eine Online-Kommunikation der Leistungserbringer und Versicherten soll nach neuesten Berichten bis 2015 in ganz Deutschland verfügbar sein. Zu Umfang und Ausgestaltung werden in den Medien widersprüchliche Forderungen und Einschätzungen referiert. Ursprünglich sollte bereits zu Beginn des Jahres 2006 die elektronische Gesundheitskarte die alten Versichertenkarten abgelöst haben. Über den Fortgang des Dauer-Projekts werde ich weiter berichten.

Im Berichtszeitraum erreichten mich verschiedentlich Anfragen von Betroffenen, die sich darüber beklagten, dass ihre Versicherung von ihnen ein Foto für die elektronische Gesundheitskarte verlange, das als Datei gespeichert werden und auf der neu ausgegebenen Versichertenkarte aufgebracht werden soll. Die gesetzliche Grundlage dafür ergibt sich aus § 291 Abs. 2 Satz 1 SGB V. Das Einwilligungsverfahren für eine länger dauernde Speicherung hatte ich mit der AOK in Sachsen abgestimmt (vgl. 13/10.1.1 - Einwilligung, Lichtbild). Wegen der Datenverarbeitung habe ich auch keine datenschutzrechtlichen Bedenken erhoben. Das Foto - der ab 15-jährigen Versicherten - auf der Karte soll letztendlich die Missbrauchsmöglichkeiten mit Krankenkassenkarten vermindern helfen. Soweit sich Betroffene weigern, der Krankenversicherung ein Lichtbild zur Verfügung zu stellen, wird es vorübergehend noch ein Ersatzverfahren geben, bei dem die Daten der Versicherten ohne entsprechende Karte manuell in einem Ersatzverfahren in der Arztpraxis oder im Krankenhaus erhoben werden. Letztendlich wird man aber die Beibringung der Fotos als eine nicht vermeidbare versicherungsvertragliche Nebenpflicht der Versicherten zu betrachten haben. Ausnahmen, was die Beschaffung der Fotos betrifft, gelten schließlich nur für die Versicherten, denen es objektiv nicht möglich ist, selbst ein Foto zu besorgen, z. B. Schwerstbehinderte.

10.2 Sozialwesen

10.2.1 ELENA (Elektronischer Einkommensnachweis): Jähes Ende nach langem Anlauf

Meine Akte zu ELENA beginnt mit einem Schreiben des BfDI vom Sommer 2003. Zu diesem Zeitpunkt war dieser schon längere Zeit an der Erarbeitung des Vorhabens beteiligt gewesen, das damals noch den Namen „Job-Card“ führte. Im Herbst jenes Jahres hat sich erstmals die DSK in Leipzig mit der Angelegenheit befasst.

Über ein „technisches Grobkonzept“ im Jahre 2004, die Einrichtung einer Arbeitsgruppe „Datenschutz“ im Projektsteuerungs-Gremium, die Einrichtung einer Unterarbeitungsgruppe innerhalb des Arbeitskreises „Gesundheit und Soziales“ der DSK (2004), die intensive Beschäftigung mit Verschlüsselungsfragen und anderen Belangen des technischen Datenschutzes, die erste Vorlage eines Roh-Entwurfes für ein „JobCard-Gesetz“ (Frühjahr 2005) und einen Beschluss der DSK im Herbst desselben Jahres, der sich skeptisch zur verfassungsrechtlichen Zulässigkeit geäußert hat, hat sich das vom (damaligen) Bundesministerium für Wirtschaft und Arbeit vorangetriebene Vorhaben zunächst weiterentwickelt, dem der BfDI recht wohlwollend, einzelne meiner Kollegen in den anderen Bundesländern bereits zu diesem Zeitpunkt sehr kritisch gegenüberstanden.

Worum ist es, und zwar bis zuletzt, gegangen? Die Arbeitgeber sollten von der Ausstellung papierener Entgeltbescheinigungen (Entgelthöhe, Daten zu Beschäftigungszeiten) entlastet werden, die als Nachweis bei der Beantragung von Sozialleistungen den Leistungsträgern vorgelegt werden müssen - etwa bei der Beantragung von Arbeitslosengeld, Wohngeld, Kindergeld oder BAföG. Zu diesem Zwecke[5] sollten alle privaten und auch öffentlichen Arbeitgeber monatlich sämtliche insoweit möglicherweise relevanten Einkommensdaten, insbesondere auch die Abzüge für Sozialversicherungsbeiträge, elektronisch an eine zentrale Speicherstelle übermitteln, aus deren Beständen sie dann von Sozialleistungsträgern im Wege eines automatisierten (mit Prüfroutinen versehenen, vgl. § 101 SGB IV) Abrufverfahrens sollten erhoben werden können. Dabei sollten die Bediensteten der betreffenden Sozialleistungsträger die Daten allerdings nur abrufen können, wenn ein Antrag vorlag und wenn der antragstellende Beschäftigte (oder ehemalige Beschäftigte) die Daten durch Verwendung einer „qualifizierten“ elektronischen Signatur, konkret mittels einer dem Signaturgesetz entsprechenden Chip-Karte (Signatur-Karte) - daher der Name „JobCard“ - an einem in der Behörde sich befindenden Gerät freigeben würde (vgl. § 98 Abs. 1 und 2, § 103 Abs. 1 und 2 SGB IV). Der Zweck war also im Wesentlichen eine Kostenersparnis bei den Arbeitgebern und auch für die Verwaltungsabläufe innerhalb der Sozialbehörden. Klar war auch: Ein großer, ja womöglich ganz weit überwiegender Teil der Daten würde niemals genutzt werden, da von der betroffenen Person während der Speicherfrist kein Leistungsantrag gestellt werden würde.

Ende 2005 hat dann das federführende Bundesministerium (nunmehr BMWi) einen Referentenentwurf zur Einführung des Verfahrens vorgelegt, mit dem dieses in ELENA-Verfahren umbenannt wurde. Erklärtes Ziel des - vor allem aus in das SGB IV (§§ 95 bis 103) eingefügten Änderungsregelungen bestehenden - Gesetzes sollte nunmehr neben der finanziellen Entlastung der Arbeitgeber und der Verwaltung von den Kosten des Medienbruches auch ein Datenschutzvorteil sein, der in der Tat insoweit zu verzeichnen sein würde, als der Arbeitgeber nicht mehr konkret erfahren würde, für welchen Sozialleistungszweck der Beschäftigte eine Bescheinigung benötigte.

Im Laufe des Jahres 2007 lag dann eine überarbeitete Fassung des Gesetzentwurfes vor, die Presse begann, sich für das Thema zu interessieren, und die Auffassungen unter den Datenschutzbeauftragten zur Verfassungsmäßigkeit des Vorhabens - unter dem Stichwort „Vorrats-Datenverarbeitung“ - entwickelten sich stärker auseinander: Zwar war ich nicht, wie zwei meiner Kollegen, vollständig überzeugt, dass die ganz überwiegende Anlasslosigkeit der Datenverarbeitung das Vorhaben sicher verfassungswidrig gemacht hat, jedoch war ich insoweit äußerst skeptisch und habe daher mit diesen beiden Kol-

[5] In der ersten ‚Ausbaustufe’ zunächst auf Arbeitslosengeld, Wohngeld und Bundeselterngeld (§ 95 Abs. 1 SGB IV) beschränkt.

legen entschieden darauf gedrungen, dass jedenfalls in der Gesetzesbegründung insoweit ein Nachbesserungsversuch unternommen werden müsste - ich habe also eine *Verfahrens*-Forderung gestellt - und man sich datenschutzseitig nicht auf Forderungen zum technischen Datenschutz beschränken dürfe.

Im Zuge des dann eingeleiteten Gesetzgebungsverfahrens[6] hat dann bemerkenswerterweise der *Bundesrat* (vgl. BR-Drs. 561/08) erhebliche Zweifel an der (verfassungsrechtlich betrachteten) Erforderlichkeit des ELENA-Verfahrens geltend gemacht und ebenfalls verlangt, dass die dazu in der Begründung des Gesetzentwurfes enthaltenen Ausführungen nachgebessert werden müssten.

Genau diese Verfahrens-Forderung nach genauerer Darlegung der Verhältnismäßigkeit, insbesondere Erforderlichkeit, der Einrichtung des Verfahrens mit seiner zentralen Erhebungsstelle habe ich dann auch im Kreise der Datenschutzbeauftragten gegenüber denjenigen entschieden vertreten, die sich nur auf die Äußerung verfassungsrechtlicher *Bedenken* beschränken wollten. (Wohlgemerkt: Es ist gut, wenn Datenschutzbehörden nicht immer derselben Rechtsauffassung sind; dies ist ein Zeichen lebendigen Rechts und im Rechtswesen bekanntlich der Normalfall.)

Nachdem insoweit im November 2008 die 76. DSK zu einer Kompromissformel-Entschließung gefunden hatte (nämlich „substantiierte Begründung“ verlangt, „erhebliche Zweifel an der Verfassungsmäßigkeit“ geäußert hat), hat der Bundesgesetzgeber dann das Gesetz verabschiedet[7]; Ende 2009 kam dann der Entwurf der dazugehörenden Datensatzverordnung („ELENA-DV“)[8] hinzu, und nun ging auch, nach Kritik aus dem Gewerkschaftsbereich an Teilen des - sehr umfangreichen - Datensatzes, der zu übermitteln sein sollte, der BfDI etwas stärker auf Distanz zu dem Vorhaben.

Auftrieb hat diese Kritik am ELENA-Verfahren unter dem Gesichtspunkt der Verhältnismäßigkeit und insbesondere der Erforderlichkeit dann durch das Urteil des Bundesverfassungsgerichts zur (schlagwortartig) sogenannte Vorratsdatenspeicherung, genauer gesagt zur Speicherung von Verbindungsdaten in der Telekommunikation (auch Telekommunikationsverkehrsdaten genannt, Urt. v. 2. März 2010 - 1 BvR 256/08, 236/08, 508/08 und 586/08, E 125, 260 = JZ 2010, 611 = NJW 2010, 833), erhalten. (Diese Entscheidung hat, vgl. dort Rdnr. 213, terminologisch unter den *vorsorglich anlasslosen* [Oberbegriff] die (a), per se, ausnahmslos verfassungswidrigen *zu unbestimmten und auch noch nicht bestimmbaren Zwecken* stattfindenden Datenverarbeitungen, als „*auf*

[6] Gesetzentwurf der Bundesregierung vom 7. Oktober 2008, BT-Drs. 16/10492.
[7] Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) vom 28. März 2009 (BGBl. I S. 634).
[8] Verordnung zur Übermittlung der Daten im Verfahren zur Erstellung und Verarbeitung des elektronischen Entgeltnachweises (ELENA-Datensatzverordnung - ELENA-DV) vom 22. Februar 2010 (BGBl. I S. 131).

Vorrat“, von den (b) möglicherweise, eben unter bestimmten Voraussetzungen, verfassungsgemäßen unterschieden, die *mit* vom Gesetz *festgelegtem Zweckbezug* stattfinden.)

Als dann ab dem 1. Januar 2010 die Arbeitgeber nunmehr verpflichtet waren, für jeden ihrer Beschäftigten - Arbeiter, Angestellte, Beamte, Richter und Soldaten - einmal pro Monat einen Datensatz zu übermitteln, kam es zu einer Massen-Verfassungsbeschwerde (1 BvR 902/10), organisiert von einer Datenschutz-Vereinigung - und zu der Äußerung einer Bundesministerin, ELENA habe sich zu etwas verwandelt, was kein Mensch mehr wolle - von solch einer Verwandlung hat allerdings keine Rede sein können! Einwände kamen jetzt auch von kleineren Arbeitgebern wegen der Umstellungskosten. Zwar ist im September 2010 ein in einem anderen Beschwerdeverfahren gestellter Antrag auf Erlass einer einstweiligen Anordnung vom Bundesverfassungsgericht abgewiesen worden.[9] Gleichwohl hat das Bundesverfassungsgericht dann im November 2010 zwei Verfassungsbeschwerden unter anderem den Datenschutzbeauftragten des Bundes und der Länder mit der Gelegenheit zur Stellungnahme nach § 27a BVerfGG übersandt, mit der Bitte, dabei unter anderem auch zu ganz bestimmten vom Gericht formulierten rechtlichen Fragen Stellung zu nehmen. Kurz darauf hat die Bundesregierung angekündigt, den (in § 119 Abs. 1 SGB IV) für den 1. Januar 2012 bestimmten Zeitpunkt, von dem ab die Nachweise für die betreffenden Sozialleistungs-Verfahren aus dem zentralen ELENA-Datenbestand zu führen sein sollten, um zwei Jahre zu verschieben.

Zu der dann von den meisten Landesdatenschutzbeauftragten unterstützten, vom Berliner (vor allem mit Darlegungen zu Mängeln beim technischen Datenschutz) und dem Bayerischen Datenschutzbeauftragten erarbeiteten Stellungnahme gegenüber dem Bundesverfassungsgericht habe ich in zwei Punkten eine abweichende Auffassung vertreten:

Zu der Frage des Gerichtes, inwieweit § 97 Abs. 1 SGB IV, also die Vorschrift, welche die Meldepflicht des Arbeitgebers ausgesprochen hat, den verfassungsrechtlichen Anforderungen des Gebotes des Normenbestimmtheit und Normenklarheit entspreche, habe ich abweichend von der Mehrheit der von den Länderdatenschutzbeauftragten geteilten Auffassung Bayerns, die Vorschrift sei bis auf dessen Satz 4 noch gerade eben hinreichend genug bestimmt, nachzuweisen versucht, dass das Gegenteil der Fall, also die Vorschrift *nicht hinreichend bestimmt* ist.

[9] Als wegen mangelnder Darlegungen zu einem die Eilbedürftigkeit begründenden Grad an Gefahr unberechtigter Datenzugriffe unzulässig abgewiesen durch Beschluss des BVerfG vom 14. September 2010 - 1 BvR 872/10, NJW 2010, 3565.

Zu der Frage des Gerichtes betreffend die Verhältnismäßigkeit der Datenübermittlung durch den Arbeitgeber und die Speicherung durch die zentrale Speicherstelle habe ich dem Gericht die - zum Ergebnis der *Verneinung* der Verhältnismäßigkeit kommende - Ländermehrheits-Stellungnahme *ergänzende* Überlegungen unterbreitet, in denen ich angeregt habe, die verfassungsrechtliche Angemessenheit (Verhältnismäßigkeit im engeren Sinne) der im ELENA-Verfahrensgesetz vorgesehenen *vorsorglich [einzel-]anlasslosen* Verarbeitung personenbezogener Daten im Rahmen eines Systems abgestufter Anforderungen an den Daten-Nutzungsgrad (er ist für ELENA grob auf 10 v. H. geschätzt worden) innerhalb eines Vergleiches verschiedener Zweck-Bereiche, in denen derartige vorsorglich anlasslose Verarbeitungen jeweils vorgesehen sind, zu bestimmen.

Im Einzelnen finden sich meine Überlegungen *unten in Abschnitt* 17.2.2 wiedergegeben. Sie betreffen Fragen[10], die auch in anderen den Datenschutz berührenden Teilen der Rechtsordnung von Bedeutung sind - und erst recht im Falle einer Neuauflage eines ELENA-ähnlichen Systems wieder zu beantworten sein werden.

Die wesentlich zurückhaltender ausgestaltete Stellungnahme (bei geringfügigen technischen Verbesserungen zugunsten des Datenschutzes „insgesamt noch verfassungsgemäß“), die der BfDI gegenüber dem Gericht abgegeben hat, hat bei den Datenschutzbeauftragten der anderen Bundesländer nur wenig Gefolgschaft gefunden.

Zum Nachteil für die Fortentwicklung des Datenschutzrechtes gerade im Hinblick auf die Bestimmtheitsanforderungen an Gesetze, aber vor allem im Hinblick auf die Anforderungen an die Angemessenheit, namentlich den notwendigen Nutzungsgrad, *vorsorglich anlassloser* Datensammlungen oder Datenabgleiche hat das Bundesverfassungsgericht dann leider doch die aufgeworfenen Rechtsfragen nicht klären müssen. Denn gemäß einer ohne viel Aufhebens gemachten, überraschenden Ankündigung des Bundeswirtschafts- und des Bundesarbeitsministeriums von Ende Juli 2011 hat die Bundesregierung die Aufhebung des ELENA-Verfahrensgesetzes durch Gesetz veranlasst, durch dessen Verabschiedung[11] die Verfassungsbeschwerden gegenstandslos werden.

Darüber, was die Bundesregierung veranlasst hat, das seit drei Legislaturperioden regierungsseitig mit jeweiliger breiter Mehrheitsgrundlage verfolgte Unternehmen aufzugeben, kann man spekulieren. Es ist bisher nicht erkennbar, dass es datenschutzrechtliche, also verfassungsrechtliche, Gründe (vorsorglicher Rückzug?) gewesen sind.

[10] Diese Rechtsfragen begegnen uns in der verschiedensten Gestalt, etwa auch unter dem Schlagwort „Generalverdacht“ bei anlasslosen Zuverlässigkeitsüberprüfungen (vgl. BVerfG Beschluss v. 4. Mai 2010 - 2 BvL 8/07, NVwZ 2010, 1146, 1151).

[11] Art. 3 des Gesetzes zur Änderung des Beherbergungsstatistikgesetzes und des Handelsstatistikgesetzes sowie zur Aufhebung von Vorschriften zum Verfahren des elektronischen Entgeltnachweises, vgl. BT-Drsen. 17/6851 und 17/7200, beschlossen vom Bundestag am 29. September 2011, am 4. November 2011 auch vom Bundesrat (vgl. BR-Drs. 608/11) beschlossen.

Möglicherweise hat eine erwartete geringe Akzeptanz (Kosten?) des Erwerbes und Einsatzes von elektronischer Signatur eine Rolle gespielt. So erfreulich die Abwicklung des riesigen Datenverarbeitungssystems ELENA unter Datenschutzgesichtspunkten ist, so bedauerlich ist, dass die Gelegenheit einer verfassungsrechtlichen Klärung grundlegender Fragen zur vorsorglichen (einzel-)anlasslosen Verarbeitung nicht hat genutzt werden können.

(Erst) Mit Inkrafttreten des Gesetzes sind die Meldungen der Arbeitgeber und Dienstherren einzustellen. Die Daten sind sinnlos verarbeitet (übermittelt und gespeichert) worden, die Arbeitgeber haben hohe unnütze Ausgaben gehabt, der Bund ohnehin. Und es ist zu erwarten, dass ein Nachfolge-Vorhaben für diese Investitionsruine nicht ausbleiben wird, womöglich (zwecks Vermeidung des Erfordernisses des Einsatzes qualifizierter elektronischer Signaturen) mit geringeren Datenschutzvorkehrungen. Dann kämen die grundlegenden verfassungsrechtlichen Fragen, die ein derartiges System aufwirft, wieder auf die Tagesordnung.

10.2.2 Zuständigkeit für Ordnungswidrigkeitenverfahren wegen Datenschutzverstößen nach SGB X

Von einer Staatsanwaltschaft ist mir eine Anzeigen-Akte übermittelt worden. Dabei ging es um die Anzeige eines angeblichen Datenschutzverstoßes, begangen durch einen Bediensteten eines Sozialleistungsträgers in Ausübung seiner Amtstätigkeit, hier als Beschäftigter einer SGB II-ARGE. Nach Prüfung meiner Zuständigkeit habe ich die Akte an die nach § 2 OWiZuVO zuständige Stelle übermittelt.

Zur Rechtslage:

Bei der Anzeige handelte es sich - entgegen der Annahme des die Anzeige seinerzeit aufnehmenden Polizeibeamten - nicht um eine angebliche Ordnungswidrigkeit nach dem Bundesdatenschutzgesetz, sondern um die Anzeige einer Ordnungswidrigkeit nach dem Sozialgesetzbuch Zehntes Buch, konkret nach § 85 SGB X, also um eine Ordnungswidrigkeit, die durch Verstoß gegen den Sozialdatenschutz (§§ 67 ff. SGB X sowie Spezialvorschriften in einzelnen Büchern des Sozialgesetzbuches) begangen wird. Die betreffende Verarbeitungshandlung sollte, so der Vorwurf, im Rahmen der amtlichen Tätigkeit eines Mitarbeiters einer an das Sozialgesetzbuch Zehntes Buch gebundenen Behörde stattgefunden haben. Dass der Polizei bei Aufnahme der Anzeige nur das Bundesdatenschutzgesetz eingefallen ist, ändert daran natürlich nichts.

Dabei ist noch auf Folgendes hinzuweisen:

Die Strafbarkeits- und Ordnungswidrigkeits-Tatbestände des Datenschutzrechtes stellen darauf ab, welchem Anwendungsbereich der handelnde Daten-Verwender zuzuordnen ist. Das ist derjenige Normenbereich, der für das Verarbeitungshandeln der Behörde gilt, in welcher der Bedienstete tätig geworden ist, auch wenn er die ihm als Bediensteten offenstehenden Datenverarbeitungsmöglichkeiten zu gänzlich außerdienstlichen Zwecken - also gewissermaßen zu seinem „Privatvergnügen“ - genutzt hat. Dies ist die Auffassung der Rechtsprechung, der ich folge (vgl. BGH Urt. vom 22. Juni 2000 - 5 StR 268/99, RDV 2001, 99; OLG Koblenz, Beschluss v. 3. Juni 2008 - 1 Ss 13/08, NJW 2008, 2794, 2795 rSp. unten; der abweichenden Auffassung von Ehmann in Simitis, Rdnr. 13 bis 15 zu § 43 BDSG ist nicht zu folgen). Kommt es demnach auf den Normenkomplex an, der für die Behörde gilt, innerhalb deren Rahmen deren Bediensteter die Verarbeitungshandlung zu einem außerdienstlichen Zweck vornimmt, so muss das speziellere Recht insoweit dem allgemeinen Recht vorgehen, hier also das Ordnungswidrigkeitenrecht nach dem Sozialgesetzbuch Zehntes Buch statt desjenigen nach dem Sächsischen Datenschutzgesetz maßgeblich sein.

Nach § 13 OWiZuVO ist der Sächsische Datenschutzbeauftragte (nur) zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG. Die Vorschrift erfasst jedoch nicht die Zuständigkeit des Sächsischen Datenschutzbeauftragten für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 85 SGB X.

Insoweit verbleibt es bei der Auffangzuständigkeit nach § 2 OWiZuVO, wonach für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach Bundesrecht die Landkreise und kreisfreien Städte zuständig sind, soweit in der Ordnungswidrigkeiten-Zuständigkeitsverordnung oder einer Verordnung nach § 15 OWiZuVO (der die Übertragung der Ermächtigung zum Erlass von Rechtsverordnungen betrifft) nichts anderes bestimmt ist.

Aufgrund dieser Rechtslage habe ich gegenüber dem SMI im Rahmen einer Bedarfsanfrage Anfang 2010 Änderungsbedarf im Bereich der Ordnungswidrigkeiten wegen Verstößen gegen datenschutzrechtliche Vorschriften im Hinblick auf die Bußgeldvorschriften des § 85 SGB X angemeldet. Denn die bislang zuständigen Landkreise und kreisfreien Städte sind selbst vielfach Sozialleistungsträger (z. B. Sozialhilfebehörde, SGB II-Behörde soweit nicht die Bundesagentur, Jugendamt, Wohngeldbehörde, Unterhaltsvorschussbehörde) und damit - neben ihren insoweit tätigen Bediensteten - auch selbst Adressat der betreffenden Bußgeldvorschriften (vgl. Karlsruher Kommentar - Rogall, Rdnrn. 32 bis 34 zu § 30 OWiG).

Überdies sind die Kommunen mit Fragen des dem Sozialdatenschutz zugrundeliegenden Sozialrechts aus dem Bereich anderer Sozialleistungsträger, etwa der Rentenversicherung und der Krankenversicherung (Krankenkasse, Kassenärztliche Vereinigung -

gemäß § 35 Abs. 1 Satz 4 sozialdatenschutzrechtlich gleichgestellt) überhaupt nicht vertraut und - wie ich leider habe feststellen müssen - auch überfordert. So hat mir das Ordnungsamt einer kreisfreien Stadt als Verwaltungsbehörde nach dem Ordnungswidrigkeitengesetz Originalunterlagen zu einer Sammelanzeige gegen zwei Bedienstete des Sozialamts der betreffenden Stadt übersandt, wonach die beiden Bediensteten außerhalb der Erfüllung von Aufgaben nach dem Sozialgesetzbuch, also gewissermaßen zu ihrem „Privatvergnügen", personenbezogene Daten unter Ausnutzung der ihrer Behörde zu Gebote stehenden Datenzugriffsmöglichkeiten - rechtswidrig - erhoben hatten. Die Übersendung der Anzeige an mich ist mit der Begründung erfolgt, der Vorgang falle nicht unter die Ordnungswidrigkeitentatbestände des Sozialgesetzbuches Zehntes Buch, sondern des Sächsischen Datenschutzgesetzes, weil die Daten nicht „im Rahmen der Antragstellung und -bearbeitung durch das Sozialamt erhoben" worden seien. Bedauerlicherweise hat sich das Sozialamt dabei jedoch überhaupt nicht mit meinem der Stadt zuvor von einem der Anzeigeerstatter zur Verfügung gestellten Schreiben an diesen auseinandergesetzt, in dem ich unter Bezugnahme auf die vorhandene Rechtsprechung (vgl. BGH Urt. v. 22. Juni 2000 - 5 StR 268/99, RDV 2001, 99; OLG Koblenz, Beschluss v. 3. Juni 2008 - 1 Ss 13/08, NJW 2008, 2794, 2795 rSp. unten) begründet habe, dass bei einem „Bedienstetenexzess", also dann, wenn der Bedienstete die ihm als Bediensteten offenstehenden Datenverarbeitungsmöglichkeiten zu gänzlich außerdienstlichen Zwecken genutzt hat, der Normbereich maßgeblich ist, der für das Verarbeitungshandeln der Behörde gilt, in welcher der Bedienstete tätig geworden ist. Vielmehr hat sich die Ordnungswidrigkeitenbehörde nur pauschal auf Eintragungen aus dem Internet berufen, die sie zum Teil missverstanden hat oder die zum Teil missverständlich (und damit falsch) sind.

Ich habe daher gegenüber dem SMI angeregt, die Zuständigkeit insoweit auf den Sächsischen Datenschutzbeauftragten zu übertragen, der bereits gemäß § 38 Abs. 3 Satz 1 SächsDSG für die im Bereich des Sozialdatenschutzes kraft Spezialitätsvorranges verdrängten Ordnungswidrigkeiten wegen Verstoßes gegen das Sächsische Datenschutzgesetz zuständig ist, und hierfür einen ausgearbeiteten Formulierungsvorschlag unterbreitet, nämlich dahingehend, dass § 13 OWiZuVO so umformuliert wird, dass am Ende hinter dem Ausdruck „(BGBl. I S. 1970)" eingefügt wird

> *sowie nach § 85 SGB X in der Fassung der Bekanntmachung vom 18. Januar 2001, zuletzt geändert durch Art. 4 Abs. 15 Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung vom 29. Juli 2009 (BGBl. I S. 2258)* [dies ist möglicherweise nicht der letzte Stand].

In diesem Umfang habe ich gegenüber dem SMI auch bereits meine Zustimmung zu der Zuweisung gemäß § 38 Abs. 3 Satz 3 SächsDSG erklärt.

Nachdem mir noch Mitte des Jahres mitgeteilt worden war, dass zeitnah mit einer Veröffentlichung der Änderungsverordnung zu rechnen sei, und ich noch einmal darauf hingewiesen habe, dass bei mir etliche Abgaben von Staatsanwaltschaften in Ordnungswidrigkeitenverfahren vorlägen, die ich in Erwartung der bereits seit langem angekündigt gewesenen Zuständigkeitsübertragung für Ordnungswidrigkeiten nach § 85 SGB X nicht weitergegeben hätte, ist mir schließlich im Herbst 2010 mitgeteilt worden, dass noch verschiedene erwartete Novellierungen des Bundesrechtes berücksichtigt werden sollten, sodass ein konkreter Termin für das Inkrafttreten einer Änderung der Ordnungswidrigkeiten-Zuständigkeitsverordnung noch nicht absehbar sei.

Angesichts dessen habe ich mich gehalten gesehen, sämtliche diesbezügliche Vorgänge an die zuständigen kommunalen Gebietskörperschaften abzugeben und die verspätete Abgabe mit der für mich unerwarteten Verzögerung der betreffenden Novellierung der Ordnungswidrigkeiten-Zuständigkeitsverordnung zu begründen.

Ich möchte nicht verschweigen, dass ich diesen Rechtszustand, dessen konkreten Auswirkungen ich immer wieder begegne, für unbefriedigend halte. Bisher hat jedoch das SMI die von mir gewünschte Erweiterung meiner Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten gemäß § 13 OWiZuVO nicht vorgenommen. Die Novellierung der Ordnungswidrigkeiten-Zuständigkeitsverordnung lässt vielmehr auch weiterhin auf sich warten.

10.2.3 Kontrollbefugnisse des Sächsischen Datenschutzbeauftragten nach dem SGB X

Eine Arbeitsgemeinschaft Grundsicherung für Arbeitssuchende (kurz ARGE) habe ich im Berichtszeitraum im Rahmen der Bearbeitung einer Eingabe betreffend Kosten der Unterkunft und Heizung nach § 22 SGB II zunächst grundsätzlich über meine Kontrollbefugnisse belehren müssen. So ist mir von der ARGE in einer Stellungnahme mitgeteilt worden, ohne Vorlage einer Vollmacht des Petenten könne mir keine Auskunft erteilt werden, und zwar aus datenschutzrechtlichen Gründen. Meine Aufforderung zur Vorlage prüfungsrelevanter Unterlagen ist seitens des Amts mit dem Hinweis abgetan worden, ich solle mich dazu an den Petenten wenden.

Mit dem Versuch, mich auf beim Petenten vorliegende Unterlagen zu verweisen und die Auskunftserteilung von der Vorlage einer Vollmacht abhängig zu machen, hat die ARGE die Rechtslage ebenso grundlegend wie bemerkenswert verkannt. Ich habe dem Amt aufgegeben, die einschlägigen Rechtsvorschriften (§ 81 Abs. 1 und § 81 Abs. 2 Satz 3 SGB X sowie § 24 und vor allem § 27 Abs. 1 und § 28 Abs. 1 SächsDSG) zu lesen.

Meine Belehrung hat Wirkung gezeigt: Der Aufforderung zur Beantwortung meiner Fragen unter Hinweis auf § 29 SächsDSG ist die ARGE danach umgehend nachgekommen.

10.2.4 Übermittlung des Belegungsplans und darin enthaltener personenbezogener Daten der Bewohner eines Ausländer- und Asylbewerberheims an die Staatsanwaltschaft

Der Datenschutzbeauftragte einer sächsischen Großstadt hat mich kurzfristig um Rückmeldung gebeten, nachdem die Staatsanwaltschaft von der Stadtverwaltung zwecks staatsanwaltschaftlicher Ermittlungen die Übersendung des aktuellen Belegungsplanes eines Ausländer- und Asylbewerberheims verlangt hatte.

Ich habe aufgrund der äußerst kurz bemessenen Stellungnahmefrist wie folgt geantwortet:

1. Soweit ausweislich des streitgegenständlichen Belegungsplans personenbezogene Daten von Leistungsempfängern nach dem Asylbewerberleistungsgesetz übermittelt werden sollen, finden die entsprechenden Übermittlungsregelungen des Sozialgesetzbuches Zehntes Buch keine Anwendung. Weder handelt es sich bei den Leistungen nach dem Asylbewerberleistungsgesetz um eine in § 18 ff. SGB I abschließend aufgeführte Sozialleistung, noch gilt das Asylbewerberleistungsgesetz als besonderer Teil des Sozialgesetzbuch Erstes Buch, denn das Asylbewerberleistungsgesetz ist in dem abschließenden Katalog des § 68 SGB I nicht aufgeführt. Bei den nach §§ 2 ff. AsylbLG zu gewährenden Leistungen handelt der Leistungsträger mithin nicht im Rahmen einer Aufgabenerfüllung nach dem Sozialgesetzbuch (Seidel in LPK-SGB-X-Kommentar, § 72 Rdnr. 31).

   Die Regelung des § 71 Abs. 2a SGB X betrifft diejenigen Fälle, in denen die betreffende Person vielmehr Leistungen nach § 18 ff. SGB I bzw. solche nach § 68 SGB I bezieht und diese Sozialdaten sodann für die Durchführung des Asylbewerberleistungsgesetz übermittelt werden sollen. Soweit das Asylbewerberleistungsgesetz keine besonderen Übermittlungsregelungen enthält, gilt § 14 SächsDSG.

2. Soweit im Rahmen der Vorlage des streitgegenständlichen Belegungsplans personenbezogene Daten sogenannter Kontingentflüchtlinge übermittelt werden sollen, handelt es sich bei den zu übermittelnden Daten insoweit um Sozialdaten nach dem Sozialgesetzbuch. Soweit mir bekannt ist, bezieht dieser Personenkreis Leistungen nach dem Sozialgesetzbuch Zwölftes Buch, wobei zu klären gewesen wäre, ob die Unterbringung in einem entsprechenden Heim eine Sozialleistung im Sinne des Sozial-

gesetzbuchs Zwölftes Buch darstellt. Sollte dies der Fall sein, gilt für die Frage der Zulässigkeit einer Übermittlung von Sozialdaten dieses Personenkreises Folgendes:

a) Die Datenübermittlung kann nicht auf § 68 SGB X gestützt werden. Zwar handelt es sich in diesem Fall nur um die Übermittlung „weniger empfindlicher“ Sozialdaten, nämlich wohl nur um die Übermittlung von Name und Vorname von derzeit in dem betreffenden Heim untergebrachten Ausländern. Das Ersuchen nach § 68 SGB X kann sich indes immer nur auf die Übermittlung bestimmter Sozialdaten eines einzelnen Betroffenen erstrecken, wobei das listenmäßige Zusammenstellen mehrerer Abfragen zu Einzelfällen insoweit keinen rechtlichen Bedenken begegnet.

   Das hier anscheinend erfolgte Ersuchen anhand eines abstrakten Kriteriums, also ein Übermittlungsersuchen von Sozialdaten einer ganzen Personengruppe, nämlich z. B. aller Personen, die im oben genannten Heim in der Zeit von … bis … oder aktuell dort untergebracht waren oder sind, wäre lediglich unter den Voraussetzungen des § 68 Abs. 3 SGB X zulässig. Die Rechtsvorschrift des § 68 Abs. 3 SGB X stellt insoweit eine Lockerung des Sozialdatenschutzes zugunsten rechtmäßiger landespolizeirechtlicher (§ 47 SächsPolG) oder strafprozessualer (§ 98a StPO) Rasterfahndungsmaßnahmen dar. Maßgeblicher Anknüpfungspunkt für die Datenübermittlung ist danach allein die Rechtmäßigkeit einer solchen Rasterfahndung, d. h. des Abgleichs personenbezogener Daten mit anderen Daten nach bestimmten Prüfungsmerkmalen (Rastern) unter Einsatz der Datenverarbeitung.

   Jedoch wäre hier auch der in § 68 Abs. 1 Satz 2 SGB X normierte Grundsatz der Subsidiarität zu beachten. Diese Verschärfung soll gerade vermeiden, dass Sozialleistungsträger als Ersatzmeldebehörde eingeschaltet werden und vielmehr sicherstellen, dass die Übermittlung von Sozialdaten nur auf die unabdingbar erforderlichen Fälle beschränkt bleibt. Insoweit ist vorliegend derzeit auch nicht erkennbar, warum die Staatsanwaltschaft die Daten nicht auch von der Meldebehörde erhalten könnte, wobei weder Schweregrad hinsichtlich der Erlangung der Daten noch Kostenhöhe Umstände sein können, um eine Übermittlung durch die Sozialbehörde zu rechtfertigen (Scholz in Kasseler Kommentar, Band 2, § 68 Rdnr. 32; Roos in v. Wulffen, Kommentar, 4. Auflage, § 68 Rdnr. 9).

b) Ob die Übermittlungsbefugnis des § 69 Abs. 1 Nr. 2 SGB X einschlägig gewesen sein könnte, war mangels näherer Angaben seitens der Staatsanwaltschaft, um welche Ermittlungen es sich konkret gehandelt hat (Leistungsmissbrauch oder aber zum Beispiel Ermittlungen wegen Drogenhandels?), nicht abschließend zu beantworten.

Die Datenübermittlung auf der Grundlage des § 69 Abs. 1 Nr. 2 SGB X ist danach zulässig, soweit sie für die Durchführung eines mit der Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch zusammenhängenden gerichtlichen Verfahrens, einschließlich eines Strafverfahrens, erforderlich ist, wobei unter Letzteres auch schon ein staatsanwaltschaftliches Ermittlungsverfahren fällt.

Hinsichtlich des nach § 69 Abs. 1 Nr. 2 SGB X geforderten Zusammenhangs des gerichtlichen Verfahrens mit einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch reicht dabei jede Aufgabe aus, die im Sinne von § 30 Abs. 1 SGB IV gesetzlich vorgeschrieben oder zugelassen ist, die sich also aus dem Sozialgesetzbuch ergibt (v. Wulffen/Bieresborn Rdnr. 13 zu § 69 SGB X). Zu den gesetzlichen Aufgaben eines Sozialhilfeträgers zählt namentlich zu überprüfen, ob die Voraussetzungen für die Leistungsgewährung vorliegen oder ob Zahlungen zu Unrecht erfolgt sind und deshalb zurückgefordert werden müssen (v. Wulffen/Bieresborn a. a. O.).

Die Bekämpfung des Missbrauchs von Sozialleistungen durch Gerichte und Staatsanwaltschaften weist daher diesen Zusammenhang mit den sozialrechtlich begründeten Aufgaben des Sozialleistungsträgers auf, nicht hingegen entsprechende staatsanwaltschaftliche Ermittlungen wegen Drogenhandels.

c) Soweit es sich *nicht* um eine Straftat zu Lasten des Sozialhilfeträgers handelt, sondern um die Verfolgung von Straftaten, die zum Nachteil Dritter verübt werden, wäre § 73 SGB X die maßgebliche Vorschrift, der gemäß Absatz 3 jedoch eine Befugnis zur Datenübermittlung nur aufgrund der (vorherigen) Entscheidung des zuständigen Ermittlungsrichters zulässt. Die Übermittlungsbefugnis des § 73 SGB X dient dabei dem notwendigen Interessenausgleich zwischen dem staatlichen Strafanspruch und dem Interesse des Einzelnen am Schutz seiner Sozialdaten. Der Regelungsgehalt des § 73 SGB X zeigt dabei, dass das Interesse der Allgemeinheit an der Sachaufklärung und Wahrheitsfindung dem Interesse des Betroffenen auf Schutz seiner Intimsphäre gerade nicht uneingeschränkt vorgeht: So wird für die Staatsanwaltschaft die Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens generell dadurch erschwert, dass die Übermittlung der richterlichen Anordnung bedarf. Dies und auch die Tatsache, dass der Gesetzgeber die Auskunftspflicht des § 161 StPO nicht in den Katalog der gesetzlichen Mitwirkungspflichten des § 71 SGB X aufgenommen hat, zeigt, dass eine unbegrenzt enge Zusammenarbeit der Leistungsträger mit der Staatsanwaltschaft gerade nicht gewollt ist. Die Vorschrift des § 73 SGB X ist insoweit daher lex specialis zu der strafprozessualen Auskunftsvorschrift des § 161 StPO (OLG Celle, Beschluss vom 30. Juli 1997, NJW 1997, 2965 f. m. w. N.).

Auf meine Frage, wie die Stadtverwaltung im Ergebnis auf das staatsanwaltschaftliche Auskunftsverlangen reagiert habe, ist mir mitgeteilt worden, dass durch die zuständige Geschäftsbereichsleitung entschieden worden sei, der Staatsanwaltschaft den Belegungsplan zu übergeben.

10.2.5 Umgang mit Sozialdaten in Bürgerämtern

Von einem Landratsamt bin ich um Rat gefragt worden, welche sozialdatenschutzrechtlichen Vorgaben zu beachten sind, wenn die Bürgerämter als zentrale Anlaufstelle bei ihrem Serviceangebot für die Bürger Sozialdaten verarbeiten.

Konkret ist es um Leistungen aus dem Bereich des Schwerbehindertenrechts (§ 29 SGB I) und des Elterngeldes (§ 25 SGB I) gegangen, wobei geplant worden war, den Mitarbeitern der Bürgerbüros Leserechte für Auskünfte zum Bearbeitungsstand in den entsprechenden Fachprogrammen einzurichten (Variante 1). Alternativ ist vorgesehen worden, den Bürgerämtern zusätzlich die Möglichkeit einzuräumen, bei ihnen eingereichte Anträge bereits in den entsprechenden Fachprogrammen anzulegen, um dem betroffenen Bürger ein weiteres persönliches Erscheinen im Fachamt zu ersparen (Variante 2).

Ich habe wie folgt Stellung genommen:

Da es sich bei den im Rahmen der Sachbearbeitung bei den Leistungsträgern anfallenden personenbezogenen Daten um Sozialdaten gemäß § 67 Abs. 1 SGB X handelt, begegnet dies unter Beachtung der Anforderungen des § 80 SGB X (insbesondere Absatz 2 Satz 2, Absatz 3 Satz 1 und 2) keinen datenschutzrechtlichen Bedenken:

Bei einer Beteiligung der Bürgerämter, und zwar sowohl im Hinblick auf die dargestellte Variante 1 wie auch Variante 2, verbleibt die datenschutzrechtliche Verantwortung für die Erhebung und weitere Verarbeitung der Sozialdaten vollumfänglich beim Auftraggeber, hier bei den jeweiligen Fachämtern des betreffenden Landratsamts. Die Bürgerämter sollen lediglich gewisse Hilfsleistungen erbringen, indem sie Sozialleistungsanträge entgegennehmen und Auskünfte zum Bearbeitungsstand erteilen. Den Bürgerämtern wird daher lediglich eine begrenzte Hilfsfunktion für die weiterhin inhaltlich für die eigentliche Sachentscheidung *allein* verantwortlichen zuständigen Fachämter in organisatorischer Hinsicht übertragen. Insoweit handelt es sich um eine nach § 80 SGB X zulässige Auftragsdatenverarbeitung der Bürgerämter (als Auftragnehmer) und nicht um eine von § 80 SGB X nicht mehr umfasste sog. Funktionsübertragung. Dies hat zur Folge, dass den Bürgerämtern insbesondere kein elektronischer Zugriff auf die gesamten Inhalte der elektronischen Akten (auf den gesamten elektronischen Datensatz des Bearbeitungsvorgangs) eingeräumt werden darf; ein solcher Zugriff steht weiterhin

nur den für die (eigentliche) Sachbearbeitung allein verantwortlichen zuständigen Fachämtern zu.

Das führt datentechnisch dazu, dass die Bürgerämter nur entsprechend eingeschränkte Leserechte bekommen dürfen.

Ich habe den Datenschutzbeauftragten des Landratsamts gebeten, dafür zu sorgen, dass diese Vorgaben in datenschutztechnischer Hinsicht eingehalten werden. Er hat mir dies schriftlich zugesagt.

10.2.6 Wegfall der Kontrollzuständigkeit für die IKK Sachsen

Aufgrund einer Satzungsänderung der IKK Sachsen, welche zum 1. August 2009 in Kraft getreten ist, hat sich der Zuständigkeitsbereich der Krankenkasse über das Gebiet des Freistaates Sachsen hinaus zudem über das Gebiet der Länder Brandenburg, Sachsen-Anhalt und Thüringen, mithin über das Gebiet von insgesamt vier Bundesländern erweitert. Bis dato waren nur drei Bundesländer betroffen, nämlich Sachsen, Sachsen-Anhalt und Thüringen, wobei Sachsen als Sitzland gemäß Artikel 1 des Staatsvertrags über die Bestimmung aufsichtsführender Länder nach Artikel 87 Abs. 2 Satz 2 des Grundgesetzes für die Bundesrepublik Deutschland (Bekanntmachung vom 9. Juni 1997, GVBl. S. 448) aufsichtsführendes Land war.

Aufgrund dieser Satzungsänderung unterliegt die Krankenkasse (sie trägt nun den Namen „IKK classic“) seit diesem Zeitpunkt nicht mehr der Kontrolle des Sächsischen Datenschutzbeauftragten, da es sich bei ihr gemäß Art. 87 Abs. 2 Satz 1 GG nunmehr um eine öffentliche Stelle des Bundes im Sinne von § 81 Abs. 1 Nr. 1 SGB X handelt, so dass nach dieser Vorschrift der BfDI zuständig ist.

Zu entscheiden war, was mit den noch beim Sächsischen Datenschutzbeauftragten in Bezug auf die IKK Sachsen anhängigen Kontrollvorgängen zu geschehen hatte. Ich bin dabei zu dem Ergebnis gekommen, dass diese umgehend an den BfDI abzugeben waren, da es für eine weitere Sachbearbeitung durch mich an der nötigen Rechtsgrundlage gefehlt hat.

Dies ergibt sich aus Folgendem:

Anders als in gerichtlichen Verfahrensordnungen, die bestimmen, dass ein einmal örtlich oder sachlich zuständiges Gericht zuständig bleibt, auch wenn sich später die zuständigkeitsbegründenden Tatsachen so ändern, dass jetzt ein anderes Gericht zuständig wäre, wobei maßgeblicher Zeitpunkt die Rechtshängigkeit der Streitsache darstellt (vgl. § 17 GVG, § 261 ZPO - Ausnahmen sind in §§ 265 Abs. 2, 264 Nr. 3 ZPO geregelt -,

§ 90 VwGO), enthält das Sozialgesetzbuch Zehntes Buch, welches auf Krankenkassen Anwendung findet, in seinem § 2 Abs. 2 zwar entsprechende Übergangsregeln für den Fall eines Zuständigkeitswechsels vor Abschluss des (Verwaltungs-)Verfahrens, die jedoch *lediglich* die hier nicht betroffene Weitergeltung der bloßen *örtlichen* Zuständigkeit betreffen und die „Verschiebung" (bereits) der örtlichen Zuständigkeit einer Behörde auch nur unter den dort genannten Voraussetzungen für zulässig erklären. Dabei liegt die Entscheidung über die Fortführung des Verfahrens im Ermessen der bisher örtlich zuständigen Behörde, wobei gegen deren Willen ihre Zuständigkeit nicht fortdauern kann, selbst bei Zustimmung der nunmehr zuständigen Behörde (Engelmann in v. Wulffen, SGB X-Kommentar 2005, § 2 Rdnr. 11 unter Hinweis auf BVerwGE 74, 206, 215).

Aufgrund der im Übrigen geltenden strikten Abgrenzung der Zuständigkeiten sind mithin (auch zeitliche) Verschiebungen nur zulässig, soweit dies ausdrücklich gesetzlich vorgesehen ist (so zum Beispiel in Art. 108 Abs. 4 Satz 1, 2. Fall GG, der unter den dort genannten Voraussetzungen dazu ermächtigt, durch Bundesgesetz eine Übertragung der nach Art. 108 Abs. 1 GG dem Bund zustehenden Zuständigkeiten auf die Länder vorzunehmen).

Derartige intertemporale Regelungen, die gegebenenfalls eine Fortsetzung bislang noch nicht abgeschlossener Kontrollvorgänge seitens des bislang zuständigen Landesdatenschutzbeauftragten anstelle des nunmehr zuständigen BfDI begründen könnten, gibt es nicht, sie ergeben sich insbesondere nicht aus § 81 SGB X, der die Aufteilung der Zuständigkeiten zwischen den Datenschutzbeauftragten des Bundes und der Länder regelt; auch dort finden sich keine entsprechenden Übergangsregelungen für den Fall einer Änderung der funktionalen Zuständigkeit für dabei noch nicht abgeschlossene Kontrollvorgänge.

Die Änderung der funktionalen Zuständigkeit hat damit ab dem genannten Zeitraum gegolten, das heißt ab dem 1. August 2009. Wegen der daraus folgenden Zuständigkeitsüberschreitung und damit zwangsläufig verbundener unzulässiger Verarbeitung personenbezogener Daten (so ausdrücklich BVerwG, Urt. v. 9. März 2005, abgedruckt in DuD 2005, 674 ff., wonach der Eingriff in das informationelle Selbstbestimmungsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG grundsätzlich auch dann nicht gerechtfertigt ist, wenn die Behörde zwar unter den materiell-rechtlichen Voraussetzungen, aber unter Verstoß gegen die gesetzliche Regel über die sachliche Zuständigkeit handelt) waren die noch anhängigen Kontrollvorgänge betreffend die IKK Sachsen an den BfDI abzugeben.

10.2.7 Anforderung von Behandlungsunterlagen zur Geltendmachung von Schadensersatzansprüchen durch gesetzliche Krankenversicherungen

Zu einer Anfrage betreffend das an ein Klinikum gerichtete Verlangen einer meiner Kontrollzuständigkeit unterliegenden gesetzlichen Krankenkasse nach Vorlage von Behandlungsunterlagen zur Prüfung und Geltendmachung von Schadensersatzansprüchen habe ich wie folgt Stellung genommen:

Es sind folgende Datenverarbeitungsschritte zu unterscheiden:

1. Übermittlungsbefugnis des Krankenhauses:

Nach dem Urteil des LSG Niedersachsen-Bremen vom 11. November 2009, Az.: L 1 KR 152/08 (gefunden in juris, dort Rdnr. 104) regelt § 294a SGB V ein aktives Tätigwerden der Regelungsadressaten, also der Vertragsärzte, ärztlich geleiteten Einrichtungen und der Krankenhäuser nach § 108 SGB V: Sie werden durch diese Norm verpflichtet, bereits von sich aus, d. h. auch ohne Aufforderung seitens der Krankenkasse, Daten zu übermitteln, wenn sie konkrete Anhaltspunkte für eine Leistungsunzuständigkeit der gesetzlichen Krankenkasse bzw. eine etwaige Schadensersatzpflicht Dritter haben (so auch Michels in: Becker/Kingreen, SGB V Kommentar 2008, § 294a Rdnr. 1; ob auch ein lediglich reaktives Übermitteln seitens der in § 294a SGB V genannten Leistungserbringer vom Tatbestand der Vorschrift gedeckt ist, hat das Gericht in seiner Entscheidung offen gelassen, a. a. O. Rdnr. 106).

Mit der Einfügung des § 294a SGB V haben die Krankenkassen also bessere Möglichkeiten erhalten sollen, eben aufgrund entsprechender Informationen der Leistungserbringer frühzeitig Verdachtsfällen nachzugehen, um ggf. Erstattungs- bzw. Ersatzforderungen gegen andere Sozialleistungsträger (§§ 102 ff. SGB X) oder Schadensverursacher (nach § 116 SGB X) sowie nunmehr (seit 1. Januar 2008) auch gegenüber Selbstverursachern (bei selbstverschuldeten und selbst zu verantwortenden Krankheiten nach § 52 Abs. 2 SGB V) geltend machen zu können.

Diese Übermittlungspflicht nach § 294a Satz 1 SGB V enthält für die Vertragsärzte, die ärztlich geleiteten Einrichtungen und für die Krankenhäuser nach § 108 SGB V zugleich die Übermittlungsbefugnis: Sie erlaubt ihnen, Daten insoweit an die Krankenkassen zu übermitteln, als dies für die Mitteilung von Anhaltspunkten für die in § 294a Satz 1 SGB V genannten Schadensfälle und damit über die ggf. bestehende Zuständigkeit eines anderen Kostenträgers erforderlich ist (siehe Begründung zu Nummer 166, § 294a SGB V, im Gesetzentwurf zur Modernisierung der gesetzlichen Krankenversicherung vom 8. September 2003, BT-Drs.: 15/1525, Seite 146). Des Weiteren enthält die Vorschrift eine entsprechende Übermittlungsbefugnis betreffend Angaben (Daten) zu

Schadensursache und möglichen Schädigern sowie seit Einfügung des § 294a Abs. 2 SGB V auch für die Erstattungsfälle nach § 52 SGB V (Selbstverschulden des Versicherten).

Diese Übermittlungsbefugnis stellt auch eine Offenbarungsbefugnis im Hinblick auf das Arztgeheimnis dar. Und sie gilt erst recht (vgl. den Rechtsgedanken des § 14 Abs. 2 SächsDSG) für eine Übermittlung auf Ersuchen (anstelle einer Spontanübermittlung).

2. Die für den Vorgang zusätzlich erforderliche Datenerhebungsbefugnis der Krankenkasse findet sich in § 284 Abs. 1 Nr. 11 SGB V.

Insoweit hat die Krankenkasse die Aufgabe, im Falle der Schädigung ihrer Versicherten durch Dritte die dadurch bedingten Leistungsaufwendungen beim Dritten oder dessen Versicherung einzufordern. Dazu müssen jedoch der Krankenkasse selbstverständlich die erforderlichen Daten zur Verfügung stehen (so ausdrücklich die Begründung zu Nummer 159 betreffend § 284 SGB V im Gesetzentwurf vom 8. September 2003, BT-Drs. 15/1525, Seite 142). Dies hat allerdings nicht nur für Schadensersatzansprüche nach § 116 SGB X zu gelten, sondern auch für die explizit in § 284 Abs. 1 Satz 1 Nr. 11 SGB V ebenfalls genannte Durchführung von Erstattungsansprüchen.

Dabei ist zu beachten, dass in den Fällen des § 116 SGB X der (Schadensersatz-)Anspruch auf die Krankenkasse als Versicherungsträger übergegangen ist. Denn die Vorschrift regelt (cessio legis) den Übergang zivilrechtlicher Schadensersatzansprüche eines Geschädigten auf einen Sozialversicherungsträger, der diesem wegen der Schädigung Sozialleistungen gewährt. Der Forderungsübergang vollzieht sich dabei bereits zum Zeitpunkt des Schadensereignisses. Die Krankenkasse macht somit in diesen Fällen keinen Anspruch eines Dritten, hier einen Anspruch ihres Versicherten, geltend, sondern ihren von vornherein *eigenen* Anspruch (mit der Folge, dass die Krankenkasse daher bei der Durchführung dieses Anspruchs auf dem Zivilrechtsweg aktivlegitimiert ist). Insoweit handelt es sich dabei bei den für die Geltendmachung eines solchen Schadensersatzanspruchs nach § 116 SGB X herangezogenen (erhobenen) Daten bei mit zu berücksichtigender zivilrechtlicher Betrachtungsweise nicht mehr nur um Daten des Versicherten (und möglicherweise des Schädigers), sondern auch um solche der Krankenkasse (Daten mit Mehrfachbezug).

Die in § 284 Abs. 1 Nr. 11 SGB V genannte „Durchführung“ der genannten Ansprüche umfasst dabei nicht erst deren tatsächliche Geltendmachung gegenüber Dritten (ggf. auf dem Rechtsweg), sondern selbstverständlich auch bereits im Vorfeld die Prüfung, ob entsprechende Erstattungs- oder Schadensersatzansprüche für die Krankenkasse entstanden sein könnten.

Um diese Prüfung durchführen zu können, ist gemäß den genannten Vorschriften die Krankenkasse berechtigt, Einsicht in entsprechende Behandlungsunterlagen zum Zweck der Durchsetzung von Ansprüchen gegen Schadensersatzpflichtige bzw. Erstattungspflichtige zu nehmen, dies insbesondere deswegen, weil die Krankenkasse im äußerst naheliegenden Bestreitensfall darlegungs- und beweispflichtig ist, dass es sich um einen entsprechenden Erstattungs- bzw. Schadensersatzfall handelt (zu den Anforderungen an eine Lockerung der Darlegungs- und Beweislast für den Versicherungsträger in den Fällen des § 116 SGB X siehe Urteil des OLG Dresden vom 21. Juli 1999, Az.: 6 U 882/99, gefunden in juris).

Dabei wird offensichtlich ausweislich des mir vorgelegten Schreibens der AOK Sachsen-Thüringen die Erhebung der Daten seitens der Krankenkasse zur Geltendmachung von Schadensersatzfällen nach § 116 SGB X (zunächst) auf das Abfordern der sogenannte Epikrise, also des Krankenhausentlassungsberichtes, beschränkt.

Zudem hat die Krankenkasse die in § 284 Abs. 3 SGB V normierte enge Zweckbindung zu beachten, die erhobenen Daten (Epikrise) dürfen mithin lediglich zur Durchführung entsprechender Erstattungsansprüche verarbeitet werden.

Dabei kann meiner Auffassung nach nicht zwingend davon ausgegangen werden, dass es für die Klärung des erforderlichen Kausalzusammenhangs zwischen der Krankheit und dem eingetretenen Schadensereignis einer Einschaltung des MDK bedarf. Nach der derzeitigen Rechtslage ist zumindest keine zwingende Beteiligung des MDK nach § 275 SGB V im Fall der Durchführung von Erstattungsansprüchen nach § 284 Abs. 1 Nr. 11 SGB V vorgeschrieben. Eine derartige - zwingende - Einschaltung des MDK habe ich immer insoweit für geboten gehalten, als eine ärztlich verordnete Leistung auf ihre medizinische Begründung hin von der Krankenkasse überprüft werden soll (siehe hierzu ausführlich 12/10.2.3, Seite 219 f.), was hier jedoch nicht der Fall ist: Prüfungsgegenstand seitens der Krankenkasse ist hier nicht die Überprüfung einer ärztlichen Leistung im engeren Sinne, sondern die Frage des Kausalzusammenhangs zwischen Krankheit und Schadensereignis.

In der Annahme ihres Interesses habe ich die Krankenhausgesellschaften Sachsen und Thüringen über meine Rechtsauffassung in Kenntnis gesetzt. Rückfragen oder gar Einwände wurden nicht erhoben.

10.2.8 Weitergabe (auf CD-ROM gespeicherter) patientenbezogener eigener Behandlungs- und Verordnungsdaten an Vertragsärzte durch eine Prüfungsstelle nach § 106 SGB V im Rahmen der Auffälligkeitsprüfung (Richtgrößenprüfung) nach § 106 Abs. 2 Satz 1 Nr. 1 SGB V zu dem Zweck, Gelegenheit zur Stellungnahme zu geben

Im Jahr 2009 ist ein datenschutzrechtliches Problem im Rahmen der Richtgrößenprüfung Arzneimittel und Heilmittel bei Ärzten an mich herangetragen worden:

Aufgrund der Neuregelung des § 106 SGB V sollen bei Ärzten Richtgrößenprüfungen bei Überschreitung der Richtgrößenvolumina durchgeführt werden, in der Regel für nicht mehr als fünf Prozent der Ärzte einer Fachgruppe. Richtgrößen sind im Vorhinein bekannt gegebene Durchschnittswerte, sogenannte Orientierungswerte. Die Richtgrößen werden bei Arzneimitteln und Verbandsstoffen auf der Basis des auf der Landesebene vereinbarten Ausgabenvolumens gebildet. Dabei wird das vereinbarte Volumen um Zuzahlungen und Rabatte ergänzt. Diese Summe teilt man in der Regel abhängig vom Verordnungsvolumen der Vergangenheit anteilig auf die einzelnen Fachgruppen und innerhalb dieser auf die einzelnen Fälle auf, getrennt nach Allgemeinversicherten (AV, Mitglieder und Familienmitglieder) und Rentenversicherten (RV). Der Prüfungszeitraum für die Richtgrößenprüfung ist in der Regel das Kalenderjahr. Die Richtgrößenprüfung kann aber auch für den Zeitraum eines Quartals durchgeführt werden.

Werden die Richtgrößen um einen festgelegten Prozentsatz überschritten, muss die Prüfungsstelle untersuchen, inwieweit die Überschreitung durch definierte Praxisbesonderheiten bedingt ist. Praxisbesonderheiten werden auf Landesebene definiert und stellen in der Regel spezielle, teure Arzneimitteltherapien dar. Die vereinbarten Praxisbesonderheiten und die Höhe des Prozentsatzes, mit dem diese berücksichtigt werden, können von KV-Bereich zu KV-Bereich variieren. Darüber hinaus können Vertragärzte individuelle Praxisbesonderheiten geltend machen, die die Prüfungsstelle entsprechend bewertet.

Für den Fall, dass ein Vertragsarzt in eine Richtgrößenprüfung kommt, ist es wichtig, dass dieser detailliert Stellung zu seinen Verordnungskosten bezieht. Reichen weder die Stellungnahme des Arztes noch die hinzugezogenen Unterlagen zur Begründung der Überschreitung aus, fällt die Prüfungsstelle in der Regel folgende Entscheidungen: Liegt die Überschreitung nach dem Prüfverfahren bei 15 bis 25 Prozent wird der Arzt bezüglich seines Verordnungsverhaltens beraten. Überschreitet das Verordnungsvolumen nach Abzug aller Praxisbesonderheiten das vorgegebene Richtgrößenvolumen um mehr als 25 Prozent, wird in der Regel ein Regress festgesetzt. Gegen den Bescheid der Prüfungsstelle kann der Vertragsarzt Widerspruch beim Beschwerdeausschuss einlegen.

Dieses Widerspruchsrecht haben aber auch die Krankenkassen und die KV. Wird vom Beschwerdeausschuss wiederum ein Regress verhängt, steht dem Vertragsarzt wie auch den Krankenkassen und der KV eine Klage vor den Sozialgerichtsbarkeiten offen. (Allesamt gefunden unter: http://www.kbv.de/ais/12918.html).

Bei der Anfrage an mich ist es datenschutzrechtlich um die Frage gegangen, ob die Prüfungsstelle im Rahmen der ihr obliegenden Wirtschaftlichkeitsprüfung nach § 106 Abs. 5 SGB V dem jeweils betroffenen Arzt diejenigen Daten (auf CD-ROM) zur Verfügung stellen darf, die die Prüfungsstelle zunächst gemäß § 106 Abs. 2c SGB V zu seiner Person auf der Grundlage des § 296 SGB V ihrerseits von der Kassenärztlichen Vereinigung und den Krankenkassen erhalten, sodann gemäß § 106 Abs. 4a Satz 6 SGB V entsprechend aufbereitet hat und die sie bis auf weiteres ihrer Sachverhaltsbeurteilung betreffend die dem Arzt vorgehaltene Richtgrößenüberschreitung zugrunde legt und zu welchen und anhand deren der betroffene Arzt auch Stellung nehmen können soll.

Meine Prüfung hat Folgendes ergeben:

a) Es ist schon recht zweifelhaft, ob es sich bei dem Vorgang des „Zur-Verfügung-Stellens“ der (auf der CD-ROM gespeicherten) Daten, die der Prüfungsstelle bzw. dem Bewertungsausschuss letztlich die maßgebliche Beurteilung in puncto Richtgrößenüberschreitung ermöglichen und (gegebenenfalls) die Grundlage für die Begründung rechtfertigender Praxisbesonderheiten bzw. die Gesamtwirtschaftlichkeit der Praxisführung liefern soll, verbunden mit der Möglichkeit für den Arzt, anhand dieses Datenbestands eine entsprechende Stellungnahme zu der ihm vorgeworfenen Richtgrößenvolumenüberschreitung vorzulegen, um eine *Übermittlung* im datenschutzrechtlichen Sinne handelt. Denn an den Arzt weitergegeben werden nur diesen selbst (mitsamt den von ihm versorgten Patienten - Daten mit Doppelbezug) betreffende Daten. Somit werden keine Daten an den Arzt weitergegeben, auf deren Erhalt er nicht im Wege des Auskunftsanspruchs einen Anspruch hätte (keine entgegenstehenden schutzwürdigen Interessen der Patienten und keine Zweckänderung), so dass es an einer Weitergabe an einen *Dritten* (§ 67 Abs. 6 Satz 2 Nr. 3 SGB X) fehlt.

Abgesehen davon: Zur Durchführung eines rechtsstaatlichen Verwaltungsverfahrens gegenüber dem Arzt ist die Prüfungsstelle verpflichtet und daher auch (vgl. § 69 Abs. 1 Nr. 1, 1. und 2. Fall SGB X) berechtigt, dem Arzt diejenigen (von ihm selbst stammenden) Daten zum Zwecke, ihm Gelegenheit zur Stellungnahme zu geben, zur Verfügung zu stellen. Dies notwendig unter Beifügung des Inhalts der bis dahin seitens der Prüfungsstelle vorgenommenen Sachverhaltsfeststellungen, eben mit dem Inhalt der (auf der CD-ROM gespeicherten) aufbereiteten Behandlungs- bzw. Verordnungsdaten. (Daran schließt sich in datenschutzrechtlicher Hinsicht im Falle einer Reaktion des Arztes

eine entsprechende *Datenerhebung* der Prüfungsstelle an, zu der diese ebenfalls verpflichtet und berechtigt ist.)

Man kann dieses Ergebnis - ebenfalls ohne darauf abzustellen, dass es sich um Daten *auch des Empfängers* (Arztes) selbst handelt - auch so begründen: Die Befugnis der Prüfungsstelle, dem jeweils betroffenen Arzt zwecks Abwendung eines drohenden Regresses Gelegenheit zur Stellungnahme zu geben, also beim Arzt die von diesem in seiner Stellungnahme gegebenenfalls gemachten Angaben als zur Durchführung der Wirtschaftlichkeitsprüfung erforderliche zusätzliche Daten zu *erheben*, umfasst implizit auch die Befugnis der Prüfungsstelle, gegenüber dem betroffenen Arzt zu diesem Zweck die Patienten-Daten offenzulegen, also weiterzugeben, die dieser für die ihm zu ermöglichende Stellungnahme im Rahmen der Wirtschaftlichkeitsprüfung benötigt: Also all diejenigen Angaben, die die Prüfungsstelle bei der Durchführung ihrer Wirtschaftlichkeitsprüfung zugrunde legt und anhand deren der Arzt seiner Mitwirkungsobliegenheit nachzukommen hat, hier also selbstverständlich die gesamten Behandlungs- wie Verordnungsdaten des Arztes, eben auch in der „aufbereiteten Form".

b) Die Weitergabe der (auf der CD-ROM befindlichen) Praxis- und Behandlungsdaten an den jeweils betroffenen Arzt ist daher zur Durchführung der nach § 106 SGB V der Prüfungsstelle obliegenden Wirtschaftlichkeitsprüfung zulässig, insbesondere ist eine diesbezügliche Weitergabe der Behandlungs- und Verordnungsdaten an den insoweit die Beweislast tragenden Arzt auch *erforderlich*: Der aus Sicht der Prüfungsstelle zugrunde zu legende Datensatz - der ja gerade die Regressabsicht der Prüfstelle begründen soll! - muss auch dem betroffenen Vertragsarzt die Sicherheit geben, dass die Prüfung auf einer vollständigen und auch sonst richtigen, die Besonderheiten seiner Praxisführung berücksichtigenden Datengrundlage erfolgt, anhand deren der Arzt seiner ihm nunmehr obliegenden Mitwirkungs- bzw. Begründungspflicht nachzukommen hat, um einem drohenden Rückgriff der Prüfungsstelle zu entgehen. Dies gilt umso mehr, als ich derzeit davon ausgehe, dass, soweit die Prüfungsstelle anhand der von ihr aufbereiteten Daten zu dem Ergebnis kommt, der Behandlungs- bzw. Verordnungsaufwand des Arztes in einem offensichtlichen Missverhältnis zu den Durchschnittswerten seiner Fachgruppe stehen, der betroffene Arzt die *alleinige* Darlegungs- und Beweislast dafür trägt, dass der Mehraufwand ggf. durch Praxisbesonderheiten gerechtfertigt ist oder durch Minderaufwand in anderen Leistungsbereichen ausgeglichen werden kann, was anhand der ihm zu überlassenden Daten belegt werden kann. Gerade auch vor diesem Hintergrund sind dem Arzt die betreffenden Daten in allen Einzelheiten zur Verfügung zu stellen.

c) Fraglich ist letztlich nur, ob sich die hierfür erforderliche gesetzliche Datenverarbeitungsbefugnis (Erheben, Nutzen, Übermitteln) der Prüfungsstelle gegenüber dem Arzt

aus den Vorschriften des Sozialgesetzbuches (V oder X) oder aber aus den allgemeinen datenschutzrechtlichen Regelungen ergibt. Dies wiederum richtet sich danach, ob es sich bei den Daten, die die Prüfungsstelle beim jeweiligen Arzt zur Durchführung der Wirtschaftlichkeitsprüfung erhebt, um *Sozialdaten* im Sinne des § 67 SGB X handelt. Nach § 67 Abs. 1 SGB X sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), *die von einer in § 35 des Ersten Buches genannten Stelle* im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.

Die in § 106 Abs. 4 SGB V normierte Prüfungsstelle, die die betreffende Wirtschaftlichkeitsprüfung nach § 106 SGB V und mithin eine Aufgabe im Sinne des § 67 SGB X eigenverantwortlich durchzuführen hat, ist meiner Meinung nach zumindest keine in § 35 SGB I explizit genannte Stelle. Dafür, dass es sich bei der Prüfungsstelle nicht um eine Stelle nach § 35 SGB I handelt, spricht auch, dass § 106 Abs. 4a Satz 4 SGB V wohl eigens die Vorschrift des § 78a SGB X in Bezug auf die Prüfungsstelle für anwendbar erklärt. Insoweit gehe ich bis auf Weiteres davon aus, dass in Bezug auf die Datenerhebung im Verhältnis zwischen Prüfungsstelle und Arzt nicht die (strengen) Regelungen des Sozialgesetzbuchs Anwendung finden, sondern vielmehr das Sächsische Datenschutzgesetz, hier § 12 Abs. 1 SächsDSG. Im Falle der Anwendbarkeit des Sozialgesetzbuchs ergibt sich die erforderliche Rechtsgrundlage aus § 67a Abs. 1 Satz 1, § 69 Abs. 1 Nr. 1, 1. und 2. Fall SGB X.

d) Im Ergebnis war daher festzuhalten, dass die Prüfungsstelle in datenschutzrechtlicher Hinsicht berechtigt ist, die betreffenden Daten (auf CD-ROM) dem jeweils betroffenen Arzt für seine Stellungnahme zu übersenden.

Ob die Prüfungsstelle nicht nur berechtigt, sondern auch verpflichtet ist, die erbetenen Angaben zu übermitteln, habe ich allerdings nicht zu entscheiden, denn datenschutzrechtlich stellt sich nur die Frage, ob die Weitergabe zulässig ist.

10.2.9 Weitreichende Beanstandungen datenschutzrechtlicher Verstöße im Zusammenhang mit der Gewährung von Leistungen nach dem SGB II durch eine optierende Kommune

Die Eingabe eines Petenten, der Leistungen nach dem Sozialgesetzbuch Zweites Buch bezog, hat mich über einen Zeitraum von 24 Monaten beschäftigt.

Eine optierende Kommune (kurz: Amt) hat im Rahmen der Ermittlung des leistungserheblichen Sachverhalts des Petenten bei den damit verbundenen Datenerhebungen und -übermittlungen gleich mehrfach gegen datenschutzrechtliche Bestimmungen verstoßen. Insbesondere der Grundsatz der vorrangigen Erhebung beim Betroffenen (§ 67a

Abs. 2 Satz 1 SGB X) ist seitens des Amts strikt ausgeblendet worden. Im Ergebnis meiner Kontrolle habe ich zuletzt eine Beanstandung nach § 29 Abs. 1 Satz 1 Nr. 2, Abs. 2 SächsDSG (i. V. m. § 81 Abs. 2 Satz 3 SGB X) wegen unzulässigen Erhebens und Verarbeitens von Sozialdaten aussprechen müssen, da das Amt trotz meiner umfangreichen Hinweise an seinen - meiner Auffassung nach rechtswidrigen - Rechtsstandpunkten festhielt und sich der Einsicht in seine Verstöße gegen Datenschutzrecht beständig verschlossen hat.

Im Einzelnen:

Bei der Entscheidung über die Erbringung von Leistungen nach dem Sozialgesetzbuch Zweites Buch an den Petenten war zu berücksichtigen, dass er Miteigentümer zweier Grundstücke war und auch Mieteinnahmen erzielt hat. Insbesondere aufgrund dieses Umstands hat sich das Amt wohl stets zu einer „intensiven Nachprüfung“ der Angaben des Petenten veranlasst gesehen und hierzu umfangreiche Sachverhaltsermittlungen angestellt:

So findet sich in der Leistungsakte des Petenten eine Gesprächsnotiz, aus der ersichtlich ist, dass das Amt bei zwei Firmen angerufen und um Auskunft darüber gebeten hat, ob die vom Petenten als Nachweis eingereichten Angebote für Arbeiten zur Instandsetzung seines vermieteten Hauses zu tatsächlich erbrachten Werkleistungen geführt haben (Fall 1).

Datenschutzrechtlich hat es sich dabei - wie auch in den nachfolgend beschriebenen Handlungen - zum einen um die *Übermittlung* von Sozialdaten gehandelt, nämlich der Angabe, dass der Petent Leistungen nach dem Sozialgesetzbuch Zweites Buch bezog oder zumindest beantragt hatte und nunmehr Tatsachen zum Vorliegen der Leistungsvoraussetzungen ermittelt würden. Zum anderen sind Sozialdaten *erhoben* worden, indem um Auskunft über die Ausführung der Firmenleistungen ersucht worden ist.

Das Amt hat dazu mir gegenüber geltend gemacht, dass es aufgrund des Untersuchungsgrundsatzes des § 20 SGB X direkt bei den beiden Firmen nachgefragt habe, ob es zu Arbeiten entsprechend den vom Petenten eingereichten Angeboten gekommen sei. Es habe Zweifel daran, ob es dabei überhaupt *Sozialdaten* übermittelt habe, zumindest seien die Sozialdaten den Firmen ohnehin bekannt gewesen. Zusätzlich hat es zur Rechtfertigung ausgeführt, der Petent erschwere die Bearbeitung seines Antrages durch „ständige Akteneinsichtnahme, wechselnde Rechtsbeistände und sehr zeitintensive fehler- und konfliktbehaftete Vorsprachen“, auch wirke er an einer Sachverhaltsaufklärung bzw. dem Fortgang des Verfahrens nicht bzw. nur widerstrebend mit, zudem mache er falsche Angaben.

Konkretisiert hat das Amt diese Behauptung gerade bezüglich der Datenerhebung (und damit, wie gezeigt, verbundenen Datenübermittlung) bei den beiden Firmen nicht. Insbesondere hat die Behörde nicht nachweisen können, dass sie zunächst, also vor ihren Erkundigungen bei den Firmen, eine Datenerhebung beim Petenten versucht hat.

Das Amt hat sich auch an eine Lebensversicherung mit der Bitte gewandt, zu bestätigen, dass die dort bestehende Lebensversicherung des Petenten erst mit Renteneintrittsalter verwertet werden kann. Diese Daten sind sodann von der Lebensversicherung übermittelt worden (Fall 2).

Das Amt hat nicht darlegen können, dass es den Petenten aufgefordert hat, darüber unter Vorlage von Nachweisen Auskunft zu geben, ob die Lebensversicherung erst nach Eintritt ins Rentenalter verwertet werden kann oder bereits eher. Es hat schon gar nicht darlegen können, dass der Petent einer solchen Aufforderung nicht nachgekommen wäre.

Mit einem Schreiben (welches sich nicht in der Akte befindet!) hat die Behörde des Weiteren eine Gemeindeverwaltung aufgefordert, ihr mitzuteilen, an welchem Ort die Schwester des Petenten ihren Hauptwohnsitz hat. Auch diese Auskunft wurde erteilt (Fall 3).

Die Behörde hat nicht erklären können, wo sich der Entwurf des Anforderungsschreibens an die Gemeinde befindet; sie hielt auch die Übermittlung der Daten des Petenten, nämlich der Angabe gegenüber der Gemeinde, dass dieser Leistungen nach dem Sozialgesetzbuch Zweites Buch bezieht, und die Erhebung der die Schwester des Petenten betreffenden Daten für rechtmäßig.

Das Grundbuchamt eines sächsischen Amtsgerichts ist seitens des Amts schriftlich aufgefordert worden, einen vollständigen Auszug des Grundbuchs der (zwei) sich dort im Eigentum bzw. Miteigentum des Petenten befindenden Grundstücke zu übersenden. In dem Schreiben wurde dem Amtsgericht mitgeteilt, dass der betreffende (Mit)Eigentümer Leistungen nach dem Sozialgesetzbuch Zweites Buch beantragt habe (Fall 4). In der Behördenakte müssen sich nach meinen Feststellungen zu diesem Zeitpunkt allerdings bereits einschlägige Grundbuchauszüge befunden haben (aufgrund handschriftlicher Bemerkungen auf einem Schreiben des Amtes an den Petenten).

Hierzu ist mir gegenüber vorgebracht worden, dass die Grundbuchauszüge nicht in der Akte vorhanden gewesen seien und der Petent deren Beibringung verweigert habe. Der Petent behauptet demgegenüber, dass sämtliche ihn betreffenden Unterlagen des Arbeitsamts, bei denen sich auch die betreffenden Grundbuchauszüge befunden hätten, bei der Erstbeantragung von Leistungen nach dem Sozialgesetzbuch Zweites Buch dem Amt vorgelegen hätten und von diesem kopiert und zu seinen Akten genommen worden

seien. Das Amt hat zu diesen Sachverhaltsangaben des Petenten nicht Stellung genommen, also weder bestritten, die betreffenden Teile der Arbeitsamtsakte kopiert zu haben, noch behauptet, dass ihm später die Grundbuchauszüge abhanden gekommen seien.

Per E-Mail hat das Amt eine Notarin, die im Jahre 1988 einen Erbvertrag zwischen dem Petenten und seinem Vater beglaubigt hat, aufgefordert, sich zur Auslegung eines in diesem Vertrag vereinbarten Vorkaufsrechts der Schwester des Petenten für eines der im Miteigentum des Petenten stehenden Hauses zu äußern. Laut einer E-Mail hat das Amt das betreffende Notariat zusätzlich telefonisch kontaktiert; dabei wurde der Sachverhalt aber nicht mit der Notarin, sondern mit einem Dritten rechtlich erörtert (Fall 5).

Das Amt hat nicht dargelegt, für die Erfüllung welcher Aufgaben die von ihm vorgenommene Datenerhebung und -übermittlung erforderlich gewesen sein soll (abgesehen davon, dass es nicht um die Ermittlung eines Sachverhalts, sondern um die rechtliche Bewertung eines bereits bekannten Sachverhalts gegangen ist).

Nach Aktenlage hat sich das Amt mehrfach mit einer ARGE in Verbindung gesetzt, um Auskünfte über die Mieter des Petenten einzuholen. Das Amt begründete diese Anfrage damit, dass der Petent seiner Mitwirkungspflicht nicht nachgekommen sei, weil er nicht mitgeteilt habe, dass die Mieter entgegen ihrer Ankündigung nicht am 31. Juli 2008, sondern erst am 31. August 2008 ausgezogen seien, und damit, dass eine weitere Mieterfamilie einen Teil ihrer Miete unmittelbar an den Petenten zahle. Zudem wirke der Petent auch bei der Beibringung der angeforderten Kontoauszüge grundsätzlich nicht mit, weil er diese nicht in Kopie übersende, sondern sie nur zur Einsichtnahme vorlege (Fall 6).

Mit zwei Schreiben hat das Amt der Schwester des Petenten mitgeteilt, dass ihr Bruder Sozialleistungen beziehe, sowie angefragt, inwieweit sie bereit sei, ihren Miteigentumsanteil an dem im Miteigentum des Petenten stehenden Grundstücks zu verkaufen oder den Anteil ihres Bruders zu erwerben. Dabei hat das Amt u. a. angeboten, die Schwester des Petenten dabei zu unterstützen, und zwar mit der Formulierung: „Hinsichtlich der Abwicklung des Kaufvertrages wären wir, soweit gewünscht, selbstverständlich gerne bereit, Sie mit unserem Fachwissen zu unterstützen.“ (Fall 7).

Das Amt hat nicht dargelegt, für die Erfüllung welcher seiner Aufgaben die von ihm vorgenommene Datenerhebung und -übermittlung erforderlich gewesen sein könnte.

Ausweislich eines Vermerks in der Akte hat sich das Amt an die Hausverwaltung gewandt, um Auskünfte zu den Mieteinnahmen des Petenten einzuholen. Einen Nachweis, dass es diesbezüglich zuvor eine Datenerhebung beim Petenten versucht hätte, hat das Amt nicht erbracht (Fall 8).

Das Amt hat weiterhin eine Mieterfamilie des Petenten aufgefordert, ihm Fragen zur Abwicklung des Mietverhältnisses, aber auch zur Bewilligung von Wohngeld zu beantworten. Ausweislich eines Vermerks über ein Telefonat sind die Fragen dem Amt auch beantwortet worden. Einen Nachweis, dass der Petent diesbezüglich vorher an der Sachverhaltsfeststellung nach Aufforderung nicht mitgewirkt hätte, hat das Amt nicht erbracht (Fall 9).

Per Bescheid hat das Amt schließlich die Gewährung von Leistungen nach dem Sozialgesetzbuch Zweites Buch davon abhängig gemacht, dass der Petent einer Auskunftserteilung durch einen Notar über von diesem beurkundete Erklärungen zum Stand der Veräußerung bzw. Belastung betreffend den Grundbesitz des Petenten zustimmt. Das Amt hat dabei gefordert, dass der Petent den betreffenden Notar von seiner Schweigepflicht zu allen seit einem bestimmten Zeitpunkt laufenden diesbezüglichen Vorgängen entbindet. Der Petent müsse auch alle sonstigen Personen (einschließlich von ihm beauftragte Rechtsanwälte), die damit befasst oder daran beteiligt waren oder sind, von ihrer Schweigepflicht entbinden bzw. eine Auskunftserteilung durch diese zustimmen. Die Leistung ist ferner davon abhängig gemacht worden, dass der Petent Auskunft über alle Personen, einschließlich deren Anschriften, erteile, die „im Zusammenhang mit seinen wirtschaftlichen Interessen tätig geworden sind“ oder Erkenntnisse über ihn und eine weitere namentlich genannte Person haben (Fall 10).

Das Amt verteidigte sich in den Fällen 1 bis 9 im Wesentlichen damit, dass eine Datenerhebung bei einem Dritten zur Aufgabenerfüllung der Behörde generell erforderlich sei und es sich bei § 67a Abs. 2 Satz 2 SGB X um eine Regelung handele, die gleichrangig neben dem in § 67a Abs. 2 Satz 1 SGB X normierten Grundsatz der (vorrangigen) Datenerhebung beim Betroffenen stehe, so dass der Leistungsträger also die Wahl zwischen Datenerhebung beim Betroffenen oder bei einem Dritten habe. Hinsichtlich des Auskunftsbegehrens gegenüber dem Notar und den Rechtsanwälten und des Verlangens nach Nennung weiterer Auskunftspersonen des Petenten meinte sich das Amt auf die Verpflichtung aus § 60 SGB I stützen zu können. Es machte zudem geltend, dass der Petent mutmaßlich falsche Angaben zum Sachverhalt gemacht habe, ohne dies jedoch weiter zu belegen.

Rechtliche Würdigung:

1. Rechtswidrigkeit der Datenerhebung

a) Gemäß § 67a Abs. 1 SGB X ist das *Erheben* von Sozialdaten durch in § 35 SGB I genannte Stellen zulässig, wenn ihre Kenntnis zur Erfüllung einer sich aus dem Sozialgesetzbuch Zweites Buch ergebenden Aufgabe der erhebenden Stelle erforderlich ist.

Für den Bereich des Sozialgesetzbuchs Zweites Buch trifft § 51b dazu spezielle Regelungen. Gemäß § 67a Abs. 2 Satz 1 SGB X sind die Sozialdaten dem Grundsatz nach (anders ausgedrückt: mit Vorrang) *beim Betroffenen* zu erheben. Ohne dessen Mitwirkung dürfen sie demgegenüber nur unter den Voraussetzungen des § 67a Abs. 2 Satz 2 SGB X erhoben werden. Das bedeutet, dass personenbezogene Daten nur ausnahmsweise bei anderen Behörden nach § 35 SGB I oder anderen Dritten erhoben werden dürfen.

Entgegen der mir gegenüber in diesem Fall vom Amt vertretenen Auffassung handelt es sich bei § 67a Abs. 2 Satz 2 SGB X auch nicht um eine Regelung, die gleichrangig neben dem in § 67a Abs. 2 Satz 1 SGB X normierten Grundsatz der (vorrangigen) Datenerhebung beim Betroffenen stünde, so dass der Leistungsträger quasi die Wahl zwischen Datenerhebung beim Betroffenen oder bei einem Dritten hätte:

Im Wortlaut der Norm - „Ohne seine Mitwirkung dürfen sie nur erhoben werden […]“ - wird unzweifelhaft deutlich, dass Sozialdaten beim Betroffenen zu erheben sind und nur ausnahmsweise - eben unter den Voraussetzungen des Satzes 2 Nummern 1 und 2 - bei Dritten erhoben werden dürfen.

Die Erlaubnis einer Datenerhebung bei Dritten enthält zusätzlich die Einschränkung, dass keine Anhaltspunkte dafür bestehen dürfen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden, siehe § 67a Abs. 2 Satz 2 Nr. 1 lit. c) und Nr. 2 lit. b) SGB X (allein die Datenerhebung aufgrund einer Rechtsvorschrift im Sinne des § 67a Abs. 2 Satz 2 Nr. 2 lit. a) SGB X ist nicht an diese Voraussetzung geknüpft).

Eine solche Beeinträchtigung überwiegender schützwürdiger Belange des Betroffenen ist aber bei einer Datenerhebung bei einem Dritten gegeben, wenn nicht zuvor eine Datenerhebung beim Betroffenen erfolgt bzw. versucht worden ist oder dieser ausdrücklich in die Datenerhebung bei dem Dritten eingewilligt hat. Dabei ist auch zu berücksichtigen, dass eine solche Erhebung notwendig eine Übermittlung von Sozialdaten des Betroffenen mit sich bringt. So erfährt etwa der Handwerker, der von der Sozialbehörde um Angaben zu einer von ihm erbrachten Werkleistung befragt wird, dass sein Auftraggeber Sozialleistungen bezieht.

Auch der Aufbau des § 67a Abs. 2 SGB X bestätigt diese Auslegung: Der Grundsatz der vorrangigen Erhebung beim Betroffenen, der nach dem Volkszählungsurteil des Bundesverfassungsgerichts einer der tragenden Grundsätze des Datenschutzrechts ist, wird als allgemeine Regel den Ausnahme-Regelungen des Satzes 2 vorangestellt.

Diese Auslegung wird übrigens auch durch § 66 SGB I bestätigt: Danach darf der Leistungsträger ohne weitere Ermittlungen die Leistungen bis zur Nachholung der Mitwirkung ganz oder teilweise versagen oder entziehen, soweit die Voraussetzungen der Leistung nicht nachgewiesen sind. Dies gilt auch dann, wenn der Antragsteller in anderer Weise die Aufklärung des Sachverhalts ersichtlich erschwert. Voraussetzung ist jedoch, dass der Antragsteller auf die Folgen fehlender Mitwirkung schriftlich hingewiesen worden ist und er seiner Mitwirkungspflicht nicht innerhalb einer ihm gesetzten angemessenen Frist nachgekommen ist.

Vom Grundsatz der vorrangigen Datenerhebung beim Betroffenen, auch „Ersterhebungsprinzip“ genannt, gehen auch Literatur (siehe Rombach in: Hauck/Noftz, § 67a Rdnr. 62 ff.; Seidel in: LPK-SGB X, § 67a Rdnr. 6; Bieresborn in: von Wulffen, § 67a Rdnr. 6 f.; Scholz in: Kasseler Kommentar, § 67a SGB X Rdnr. 20 f.) und Rechtsprechung (Bayr. LSG, Urt. v. 25. Januar 2008, Az.: L 7 AS 72/07; VGH Baden-Württemberg, Urt. v. 1. April 1992, Az.: 6 S 2203/90; SG Düsseldorf, Beschluss v. 23. November 2005, Az.: S 35 AS 34/05 ER) aus. Er folgt aus dem Grundrecht auf informationelle Selbstbestimmung und findet sich in allen Datenschutzgesetzen (vgl. etwa § 12 Abs. 2 bis 4 SächsDSG, § 4 Abs. 2 BDSG).

Ausnahmsweise darf die Datenerhebung bei Dritten, die keine öffentlichen Stellen im Sinne des § 67a Abs. 2 Satz 2 Nr. 2a SGB X sind, und ohne Mitwirkung des Betroffenen erfolgen, wenn eine Rechtsvorschrift die Erhebung bei ihnen zulässt (siehe etwa § 60 SGB II oder § 117 SGB XII) oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt (siehe etwa § 118 Abs. 4 SGB XII). Dies betrifft in der Regel Stellen, die über bestimmte Tatsachen besser Auskunft geben können als der Betroffene selbst.

Eine Datenerhebung bei einem Dritten darf ferner ausnahmsweise dann erfolgen, wenn dies wegen der Art der Aufgaben der Sozialverwaltung erforderlich ist, § 67a Abs. 2 Satz 2 Nr. 2 lit. b) Doppelbuchstabe aa) SGB X. Hierunter fällt die Erteilung von Aufträgen für Befundberichte, aber auch die Überprüfung von Angaben, deren effektive Erledigung gefährdet wäre, wenn der Betroffene davon Kenntnis erlangen sollte (Scholz in: Kasseler Kommentar, § 67a Rdnr. 40). Allerdings steht diese Erhebung immer unter dem Erfordernis der Abwägung mit den schutzwürdigen Interessen des Betroffenen, namentlich dessen Recht auf informationelle Selbstbestimmung. Der schonendste Eingriff in dieses Recht ist daher zunächst die Datenerhebung beim Betroffenen selbst (Scholz in: Kasseler Kommentar, § 67a Rdnr. 30).

Nicht zuletzt können Sozialdaten bei einem Dritten dann erhoben werden, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erforderte, § 67a

Abs. 2 Satz 2 Nr. 2 lit. a) Doppelbuchstabe bb) SGB X. Diese Voraussetzung ist dann erfüllt, wenn der Betroffene die Sozialdaten unvollständig oder unkorrekt zur Verfügung gestellt hat. Allerdings ist auch hier eine Interessenabwägung zu treffen.

Die Auffassung *Kunkels* (ZfSH/SGB 1995, 225, 230) - auf die sich das Amt mir gegenüber ausdrücklich beruft -, wonach die Erhebung bei einem Dritten erfolgen darf, wenn der Betroffene die Daten bereits in einem anderen Zusammenhang einer anderen Behörde mitgeteilt hat und es deshalb als unverständliche Belästigung empfinden würde, wenn diese Daten erneut bei ihm abgefragt würden, bezieht sich ausdrücklich auf die Datenerhebung nach § 67a Abs. 2 Satz 2 Nr. 2 lit. a SGB X, also den Fall, dass eine Rechtsvorschrift die Datenerhebung bei einem Dritten oder die Übermittlung an die erhebende Stelle erlaubt. Soweit ersichtlich, beruft sich das Amt jedoch bei keiner der beanstandeten Datenübermittlungen und -erhebungen auf diesen Erlaubnistatbestand. Es ist auch nicht ersichtlich, dass es möglich wäre, die vom Amt vorgenommenen Erhebungen auf eine diesbezügliche Vorschrift zu stützen.

Unabhängig davon kann der Auffassung *Kunkels* nicht gefolgt werden, weil sie nicht dem Wortlaut des Gesetzes entspricht, der in § 67a Abs. 2 Satz 2 Nr. 2 lit. a SGB X auf eine Übermittlungsvorschrift, nicht aber auf eine Interessenabwägung abstellt.

b) Die Voraussetzungen für die Erhebung von Sozialdaten bei einem Dritten sind in den genannten Fällen 1 bis 9 nicht erfüllt bzw. nicht erfüllt gewesen. Der Grundsatz der vorrangigen Erhebung beim Betroffenen (§ 67a Abs. 2 Satz 1 SGB X) ist verletzt worden. Die Datenerhebungen waren daher unzulässig.

Insbesondere kann die - nach Auffassung des Amts belegte - fehlende Mitwirkung des Petenten bei der Ermittlung des Verkehrswertes seines Grundbesitzes nicht dazu dienen, ihn betreffend jegliche Datenerhebung bei einem Dritten (etwa bei den Handwerksfirmen) zu rechtfertigen. Vielmehr hätte das Amt als erhebende Stelle die Voraussetzungen einer rechtmäßigen Datenerhebung nach § 67a SGB X in jedem einzelnen Fall prüfen müssen.

Dies gälte auch in dem Fall, dass der Antragsteller falsche Angaben gemacht hat (wobei die Behauptung des Amts, der Petent habe falsche Angaben gemacht, nicht belegt worden und dergleichen auch nicht aus den Akten ersichtlich ist). Folgte man in diesem Fall der Auffassung des Amts, bräuchte die Behörde bei einem Leistungsempfänger, der einmal falsche Angaben gemacht hat, gar keine ihn betreffenden Daten mehr zu erheben, sondern dürfte diese alle sogleich bei Dritten erheben. Das ginge weit über die Erforderlichkeit, auf die das Gesetz abstellt, hinaus. Richtigerweise sind auch hier die Voraussetzungen der Datenerhebung in jedem einzelnen Fall

(Erhebungsvorgang) zu prüfen: Nur so verstanden entspricht das Gesetz dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz.

Soweit das Amt zu dem Schluss gelangt, bereits eine „widerstrebende Mitwirkung" des Betroffenen berechtige zu einer quasi „begleitenden" Datenerhebung bei Dritten, so stellt sich die Frage, wie diese Mitwirkung - das wäre sie zweifelsohne ja noch - von einer „ordentlichen" oder „bereitwilligen" Mitwirkung abgegrenzt werden sollte. Wirkt der Betroffene, der nach dem Grund der Datenerhebung fragt, deswegen bereits nur noch unzulänglich mit? Eine lediglich „widerstrebende" statt bereitwillige Mitwirkung ist keine gesetzlich vorgesehene Grundlage einer Erlaubnis der Datenerhebung bei Dritten.

Wenn das Amt in diesem Zusammenhang ferner vorbringt, der Petent wirke an der Beibringung der angeforderten Kontoauszüge grundsätzlich nicht mit, weil er diese nicht übersende, sie gar nicht oder nur sehr kurz zur Einsichtnahme vorlege, so dass sich der Bearbeiter nur einzelne Daten abschreiben, die betreffenden Unterlagen aber nicht fotokopieren könne, so rechtfertigt dies für sich genommen ebenfalls nicht die Datenerhebung bei Dritten: Es liegt allein an der SGB II-Behörde, ihre Einsichtnahme in die Antragsteller-Unterlagen so zu organisieren, dass sie in alle relevanten Kontobewegungen Einblick nehmen kann, dass sie sich Notizen machen und, soweit erforderlich, Passagen ablichten und zu ihren Akten nehmen kann. Wenn das Amt diese datenschutzgerechte Verfahrensweise (siehe 13/10.2.5) gegenüber seinen Antragstellern nicht durchsetzen kann, ist dies allein ein behördliches Versagen. Der Petent hat jedoch insofern recht, als er dem Amt das *pauschale* Ablichten *sämtlicher* Kontoauszüge verwehrt.

2. Rechtswidrigkeit der Datenübermittlung

a) Gemäß § 67d Abs. 1 SGB X ist eine *Übermittlung* von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im Sozialgesetzbuch besteht. Häufig einschlägige Übermittlungsvorschrift ist § 69 Abs. 1 Nr. 1 SGB X, wonach die Übermittlung von Sozialdaten zulässig ist, soweit sie erforderlich ist für die Erfüllung der Zwecke, für die sie erhoben worden sind, oder für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch oder einer solchen Aufgabe des Dritten, an den die Daten übermittelt werden, wenn er eine in § 35 SGB I genannte Stelle ist. Diese Voraussetzungen sind nicht erfüllt, soweit die Übermittlung einer Erhebung von Daten bei Dritten dient, die nicht zulässig ist.

§ 20 SGB X normiert - entgegen der Auffassung des Amts - keine Rechtsgrundlage für die Übermittlung von Sozialdaten. Das folgt aus § 35 Abs. 2 und § 37 Satz 3 SGB I.

b) Die Datenübermittlungen in den o. g. Fällen 1 bis 9 waren - ebenso wie die Datenerhebung - unzulässig.

Insbesondere waren sie nicht für die Erfüllung gesetzlicher Aufgaben der Behörde erforderlich, da eine vorherige Befragung des Petenten - die möglicherweise die erforderlichen Informationen gebracht hätte - nicht erfolgt ist.

So gehört es nicht zur Aufgabe einer SGB II-Behörde, das Vermögen der Leistungsempfänger zu verwerten - ein anderes Aufgabenverständnis des Amts liegt demgegenüber dem Handeln des Amtes im Fall 7 zugrunde. Eine SGB II-Behörde muss lediglich eine Prognose darüber treffen, ob Vermögen verwertbar ist. Sie hat den Leistungsempfänger bei nicht zu eigenen Zwecken genutzten Grundstücken aufzufordern, den Wert des Vermögens nachzuweisen - um zunächst das Schonvermögen festzustellen und sich dann die Unverwertbarkeit nachweisen zu lassen, wenn sich der Leistungsempfänger darauf beruft. Darauf hat auch das SG Dresden in seinem Beschluss vom 2. März 2010, Az.: S 32 AS 320/10 ER in der Sache des Petenten hingewiesen. Kommt der Leistungsempfänger dieser Pflicht zur Mitwirkung nicht nach, erfolgt nach entsprechender Belehrung bei fortgesetzten unwirtschaftlichem Verhalten die Absenkung der Leistungen nach § 31 Abs. 4 Nr. 2 SGB II (siehe Urteil des BSG vom 27. Januar 2009, Az.: B 14 AS 42/07 ER, juris Rdnr. 24).

3. Verstoß gegen § 67a Abs. 5 SGB X

Erfolgt die Datenerhebung nicht beim Betroffenen oder einer Stelle nach § 35 SGB I und hat der Betroffene keine Kenntnis von der Datenerhebung bei einem Dritten, so ist er unter den Voraussetzungen des § 67a Abs. 5 SGB X über die Speicherung, die Identität der verantwortlichen Stelle sowie über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Sieht die verantwortliche Stelle von einer Unterrichtung unter den Voraussetzungen des Satzes 2 Nummern 2 oder 3 ab, hat sie die Gründe schriftlich festzulegen.

Der Petent ist in keinem einzigen Fall der Datenerhebung bei einem Dritten in der nach § 67a Abs. 5 SGB X gebotenen Weise unterrichtet worden. Dies stellt für sich genommen einen zusätzlichen datenschutzrechtlichen Verstoß dar.

Für die unter Fall 10 beschriebene Aufforderung an den Petenten, sämtliche mit der Vertretung seiner rechtlichen Interessen beauftragten Anwälte sowie den Notar gegen-

über dem Amt von der Schweigepflicht zu entbinden, kommt entgegen der Auffassung des Amts § 60 SGB I nicht als Rechtsgrundlage in Betracht. Die Vorschrift enthält keine Befugnis zur Datenerhebung, wie § 35 Abs. 2 SGB I zu entnehmen ist. Sie regelt lediglich die Verpflichtung - besser: Last - des Antragstellers, leistungserhebliche Tatsachen mitzuteilen. Die Grenze der Mitwirkungspflicht des Betroffenen zieht § 67a Abs. 1 Satz 1 i. V. m. Abs. 2 Satz 1 SGB X, der zugleich Rechtsgrundlage für eine Datenerhebung sein kann, d. h. die *Erforderlichkeit* als Ausfluss des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes. Danach ist die Erhebung von Sozialdaten nur zulässig, soweit dies zur Aufgabenerfüllung der erhebenden Stelle erforderlich ist. Die Sozialdaten sind beim Betroffenen zu erheben (siehe dazu bereits oben).

Unabhängig davon, dass das Amt das Vorliegen dieser Voraussetzungen (insbesondere im Hinblick auf die vorrangige Erhebung beim Betroffenen) nicht dargelegt hat bzw. nicht hat darlegen können, ist die Forderung an den Betroffenen, seinen Anwalt oder den Notar von der Schweigepflicht gegenüber der Behörde zu entbinden, unzulässig, wenn die Forderung - wie geschehen - als Bedingung für die Gewährung von Sozialleistungen formuliert ist. Zwar ist der Empfänger von Sozialleistungen verpflichtet, an der Aufklärung des leistungserheblichen Sachverhalts mitzuwirken, die Mitwirkungspflicht - besser: -last - findet jedoch dort ihre Grenze, wo die Behörde Auskünfte aus dem Vertrauensverhältnis zwischen einem Anwalt (der gerade zur Vertretung des Leistungsempfängers gegenüber der Behörde bevollmächtigt ist) und seinem Mandanten einholen will.

Ich habe bei der optierenden Kommune zumindest erreichen können, dass sie an ihrer ursprünglich vertretenen Rechtsauffassung, wonach die Behörde ein Wahlrecht dahingehend habe, dass sie im Rahmen ihrer Aufgabenerfüllung die Datenerhebung beim Betroffenen selbst oder über Dritte betreiben dürfe, ausweislich ihrer Stellungnahme zu meiner Beanstandung nicht mehr festhält. Im Übrigen zeigte sie sich allerdings weiterhin uneinsichtig.

10.2.10 Datenverwendung im Zusammenhang mit der Einschaltung Dritter in die Erfüllung von Aufgaben des SGB II-Leistungsträgers; Schweigepflichtentbindung

Zur Umsetzung der Leistungserbringung nach § 16a Nrn. 2 und 4 SGB II - es handelt sich dabei um Kommunale Eingliederungsleistungen betreffend Schuldner- und Suchtberatung - hat mir eine sächsische Großstadt die von ihr für die SGB II-ARGEn entworfenen „Handakten“ zur datenschutzrechtlichen Prüfung vorgelegt.

Ich bin zu dem Ergebnis gelangt, dass die in diesen Leitfäden beschriebenen Datenübermittlungen zwischen den SGB II-Behörden und der Sozialhilfebehörde bzw. den Schuldner- und Suchtberatungsstellen auf der Grundlage des § 69 Abs. 1 Nr. 1 SGB X, § 50 Abs. 1 SGB II jeweils in dem Umfang zulässig sind, in dem dies zur Erfüllung der Aufgaben der dort genannten Sozialleistungsträger oder von ihnen beauftragter Dritter *erforderlich* ist. Eine Einwilligung in diese Datenübermittlungen ist daher nicht erforderlich und darf auch schon deswegen nicht eingeholt werden.

Soweit die Übermittlung von Sozialdaten durch Personen erfolgen soll, die unter § 203 Abs. 1 StGB fallen - etwa Berater für Suchtfragen in einer Beratungsstelle, § 203 Abs. 1 Nr. 4 StGB - machten sich diese jedoch strafbar, wenn sie nicht zuvor von ihrer Schweigepflicht entbunden worden sind. Gemäß § 203 Abs. 1 StGB werden die dort genannten Personen bestraft, wenn sie unbefugt fremde Geheimnisse offenbaren. Die Befugnis zur Offenbarung können diese Personen, auch wenn sie als Amtsträger bei und im Auftrag einer Behörde nach § 35 SGB I arbeiten, nicht auf § 69 Abs. 1 Nr. 1 SGB X stützen, weil diese Regelung zwar als Befugnisnorm im Sinne des § 203 Abs. 2 StGB in Betracht kommt, nicht aber als solche des Absatzes 1 der Regelung. Vielmehr ist die Befugnis zur Offenbarung nur gegeben, wenn der sonst Schweigepflichtige aufgrund besonderer Gesetze zur Offenbarung verpflichtet ist. Dies gilt etwa im Fall des § 138 StGB, wobei § 139 Abs. 3 Satz 2 StGB auch hier eine Straflosigkeit bestimmter Berufsgruppen regelt (vgl. Schönke/Schröder/Lenkner, § 203 StGB Rdnr. 29).

Eine solche spezifische Regelung zur Offenbarung enthält § 69 Abs. 1 Nr. 1 SGB X nicht. Es bedarf daher in den Fällen, in denen Sozialdaten übermittelt werden sollen, die von Personen nach § 203 Abs. 1 StGB erhoben worden sind (Suchtberatung, Schuldnerberatung durch Anwälte etc.) einer Schweigepflichtentbindungserklärung.

Damit eine Erklärung zur Entbindung von der Schweigepflicht der Regelung des § 67b Abs. 1 und 2 SGB X bzw. den allgemeingültigen Anforderungen an eine wirksame Einwilligungserklärung entspricht, muss Folgendes in der Entbindungserklärung enthalten sein:

1. Name und Anschrift des Betroffenen,
2. Name desjenigen, der von der Schweigepflicht entbunden werden soll bzw. eine konkrete Bezeichnung der Personen.
3. Soweit möglich, sind die Daten, die übermittelt werden sollen, konkret in der Erklärung anzugeben bzw. zu bezeichnen (z. B. Ergebnis der Schuldnerberatung, Aufstellung der Vermögensverhältnisse etc.). Ist dies wegen des Umfangs der Unterlagen nicht möglich, so sind diese dennoch präzise und ihrer Art nach abschließend zu beschreiben.

4. Der Zweck der Datenübermittlung ist anzugeben (Wofür werden die Daten verwendet?).
5. Der Empfänger (Institution) der Daten ist namentlich zu nennen.
6. Der Erklärung muss zu entnehmen sein, ob eine einmalige oder wiederkehrende Datenübermittlung beabsichtigt ist.
7. Der Betroffene ist über sein Recht zum Widerruf der Erklärung zu belehren und auch darüber, an wen er den Widerruf richten kann.
8. Dem Betroffenen ist eine Ablichtung seiner Einwilligungserklärung anzubieten.

Ferner habe ich darauf hingewiesen, dass meines Erachtens die Kenntnis einzelner Feststellungen aus den Schuldner- bzw. Suchtberatungen für die Erfüllung der Aufgaben der SGB II-ARGE nicht erforderlich sind. In der Regel dürfte die Übermittlung des Ergebnisses genügen. Sollte die Erforderlichkeit der Übermittlung nicht gegeben sein, ist auch die Übermittlung auf Grundlage einer Einwilligung nicht zulässig.

Ist es für die Aufgabenerfüllung der Sozialhilfebehörde oder der SGB II-ARGE erforderlich, die Daten weiter zu übermitteln, ist § 76 Abs. 2 Nr. 1 SGB X zu beachten, soweit die Sozialdaten von einem Arzt oder einer in § 203 Abs. 1 bis 3 StGB genannten Personen zugänglich gemacht worden sind.

10.2.11 Unberechtigte Datenweitergabe an Bundesministerium

Im Rahmen der Bearbeitung einer Eingabe betreffend das Handeln einer SGB II-Stelle habe ich erfahren, dass das BMAS wegen eines Schreibens des Petenten an die Bundesministerin den Leistungsfall des Petenten und damit seine Sozialdaten betreffend, eine schriftliche Stellungnahme des SMS eingeholt hat. Ungeachtet der Unzuständigkeit des BMAS hat das SMS auf dessen Aufforderung hin die erbetene Stellungnahme zur Person des Petenten, den Einzelheiten seines Leistungsfalles und dessen Bearbeitungsstand übermittelt.

Die in der Stellungnahme des SMS mir gegenüber geäußerte Rechtsauffassung, die Befugnis, dem BMAS solche Informationen zu übermitteln, stütze sich auf die Einwilligung des Petenten, teile ich nicht: Diese Vorgehensweise käme ohnehin 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. 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.

Bei einer wie hier erfolgten Aufforderung um Sachverhaltsprüfung handelt es sich jedoch, was die Wirkung des Verfahrens betrifft, immer auch um die Überprüfung be-

hördlichen Handelns in einem konkreten Einzelfall. Dieses hoheitliche Handeln der öffentlichen Gewalt bedarf auch einer entsprechenden gesetzlichen Grundlage. Denn Kraft des verfassungsrechtlichen Grundsatzes des Vorbehalts 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 (13/10.2.15 unter 4.3 sowie 14/10.2.6; vgl. auch Menzel DuD 2008, 401).

Es bedarf mithin einer gesetzlichen Erlaubnis, für die Zwecke einer fachgesetzlichen Bewertung personenbezogene Daten zu verarbeiten. Die sich aus gesetzlichen Vorschriften ergebende auch *instanzielle* Zuständigkeit der Behörde ist dabei 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.

Eine entsprechende Erlaubnis für die Verarbeitung personenbezogener Daten im Rahmen der Abgabe einer fachgesetzlichen Bewertung einer Eingabe findet sich in § 14 LJHG - dessen Voraussetzungen allerdings im betreffenden Fall offensichtlich nicht erfüllt waren.

10.2.12 Weitergabe von Name und Anschrift von Pflegeeltern durch das Jugendamt an die leiblichen Eltern

Pflegeeltern eines Kindes, das im Wege der sogenannten Bereitschaftspflege nach § 42 SGB VIII von der Pflegefamilie aufgenommen worden war, haben sich an mich gewandt, nachdem sie erfahren hatten, dass das Jugendamt Name und Anschrift der Pflegefamilie der leiblichen Mutter mitteilen, also übermitteln, wollte. Die Pflegefamilie hat mir überzeugend dargelegt, dass der Stiefvater des Kindes gegenüber dem Jugendamt gedroht habe, das Kind mit Gewalt aus der Pflegefamilie herausholen zu wollen.

Ich habe dazu folgende Rechtsauffassung vertreten:

Gemäß § 42 Abs. 3 Satz 1 SGB VIII hat das Jugendamt in den Fällen einer Inobhutnahme - etwa weil das Kind nach § 42 Abs. 1 Satz 1 Nr. 1 SGB VIII um Obhut bittet oder eine dringende Gefahr für das Wohl des Kindes nach § 42 Abs. 1 Satz 1 Nr. 2 SGB VIII die Inobhutnahme erfordert - die Personensorge- oder Erziehungsberechtigten un-

verzüglich von der Inobhutnahme zu unterrichten. Von der Unterrichtung ist nach einleuchtender Auslegung des Gesetzes in der Kommentarliteratur im Regelfall auch die Mitteilung des gegenwärtigen Aufenthaltsortes des Kindes (z. B. Name und Anschrift der Einrichtung) umfasst. Etwas anderes gilt den Kommentaren zufolge ebenso einleuchtenderweise ausnahmsweise dann, wenn dadurch eine unmittelbare und schwerwiegende Gefährdung des Wohles des Kindes droht (siehe dazu: Schellhorn/Fischer/Mann SGB VIII, § 42 Rdnr. 21; Wiesner SGB VIII, § 42 Rdnr. 38); dies muss meiner Auffassung nach auch den Fall umfassen, dass das Kindeswohl dadurch gefährdet wird, dass es wie hier mittels gegenüber den Pflegepersonen ausgeübter Gewalt aus deren Obhut entfernt zu werden droht.

Abgesehen davon wäre es natürlich unzumutbar für Pflegeeltern, ihre Aufgabe unter erkennbarer Gefahr für Leib oder Leben zu übernehmen. Auch deswegen schließt das Achte Buch des Sozialgesetzbuches (Kinder- und Jugendhilfe) eine Übermittlung eines Sozialdatums, also hier des Namens und der Anschrift, aus, d. h. verbietet die Weitergabe, wenn durch die Übermittlung der Erfolg einer zu gewährenden Jugendhilfeleistung infrage gestellt würde: § 64 Abs. 2 SGB VIII. So wie mir der Fall geschildert worden ist, war das hier der Fall, zumal die Pflegeeltern begründete Einwendungen geltend gemacht haben (Schellhorn/Fischer/Mann, Rdnr. 75 zu §§ 61 bis 68, Wiesner/Mörsberger, Rdnr. 15 zu § 64 SGB VIII).

Kurz: Dem Gesetz lässt sich nicht entnehmen, dass das Jugendamt ausnahmslos verpflichtet ist, Namen und Anschrift der Pflegeeltern mitzuteilen. Im Gegenteil: Hier schien das klare Verbot des § 64 Abs. 2 SGB VIII einzugreifen.

Ob im jeweiligen Einzelfall eine solche Gefährdung droht, muss das Jugendamt selbst beurteilen. Ich habe den Pflegeeltern in ihrem Fall geraten, dem Amt hierfür alle Tatsachen mitzuteilen, die für die Entscheidung relevant sind (auch Aussagen des Kindes etc.).

10.2.13 Erhebung eines erweiterten Führungszeugnisses der Ehegatten von Tagespflegepersonen

Erneut habe ich einen Datenschutzverstoß eines Jugendamtes im Zusammenhang mit der Datenerhebung bei Tagespflegepersonen feststellen müssen (s. bereits 14/10.2.19). So hat das Jugendamt einer sächsischen Großstadt von Ehegatten von Tagespflegepersonen ein erweitertes Führungszeugnis verlangt.

Ich habe die Stadt darauf hingewiesen, dass ich eine Rechtsgrundlage für die Erhebung solcher Daten nicht erkennen kann. Zwar mag es durchaus wünschenswert sein, dass auch Familienmitglieder von Tagespflegepersonen hinsichtlich einschlägiger Vorstrafen

überprüft werden können, jedenfalls soweit sie Umgang mit den Tageskindern pflegen, doch bedürfte es für eine solche Datenerhebung einer gesetzlichen Grundlage. (Dies gilt im Übrigen auch für die Datenerhebung nach einer Einwilligung der Betroffenen, vgl. 14/10.2.19.) Ich habe die Stadt aufgefordert, die Datenerhebung in Form der Beibringung eines erweiterten Führungszeugnisses von Ehegatten oder sonstigen Familienmitgliedern der Tagespflegepersonen zu unterlassen.

Das Jugendamt hat sich für seine Praxis auf die Empfehlungen des Landesjugendamtes Sachsen zu Leistungen der Jugendhilfe in Form der Kindertagespflege vom 26. November 2009 berufen, wo es unter 3.2.1 heißt: „Die persönliche Eignung der Tagespflegeperson ist unter Berufung auf § 72a SGB VIII auch durch Vorlage eines Führungszeugnisses nachzuweisen. Gegebenenfalls kann das Führungszeugnis auch von anderen Familienangehörigen über 18 Jahren, die sich im Hause der Tagespflegeperson aufhalten, verlangt werden.“ Auch das Landesjugendamt nennt für die Erhebung dieser personenbezogenen Daten keine Rechtsgrundlage.

Die Stadt hat sich ferner auf die „Praxismaterialien“ des BMFSFJ und des Deutschen Jugendinstitutes zur „Eignung von Tagespflegepersonen in der Kindertagespflege, Nummer 2, Oktober 2009“ gestützt, in denen es unter 5.2.8.1 als „zielführend“ empfohlen wird, auch von den übrigen Mitgliedern der Tagespflegefamilie ein polizeiliches Führungszeugnis einzuholen. Auch in diesen Materialien (die übrigens auch eine - andere - Datenerhebung auf der Grundlage einer [lediglich] *analogen* Anwendung des § 72 a SGB VIII als erlaubt ansehen) wird keine Rechtsgrundlage für diese Datenerhebung angegeben.

Den BfDI habe ich um seine Rechtsauffassung hierzu gefragt verbunden mit der Bitte, darüber unterrichtet zu werden, was er gegebenenfalls beim BMFSFJ in dieser Sache erreicht hat. Eine Rückmeldung habe ich bisher leider nicht erhalten.

Das SMK, welches seitens der Stadt in die Angelegenheit eingeschaltet worden war, hat mir mitgeteilt, dass es meiner Rechtsauffassung zustimme und die Stadt aufgefordert habe, meinen Ausführungen zu folgen.

10.2.14 Datenerhebung eines Trägers der freien Jugendhilfe im Rahmen des Abschlusses eines Betreuungsvertrags bei der Aufnahme eines Kindes in eine Kindertageseinrichtung

Ich bin von betroffenen Eltern davon in Kenntnis gesetzt worden, dass bei Abschluss des Betreuungsvertrags für die Aufnahme ihres Kindes in einer Kindertageseinrichtung auf dem Gebiet einer sächsischen Großstadt der betreffende freie Träger der Kinder-

tageseinrichtung unter anderem Angaben zur Staatsangehörigkeit, zum Beruf und zur Arbeitsstelle der Eltern erfragt hat.

Die Stadtverwaltung hat mir auf meine Anfrage hierzu wie folgt geantwortet:

„*Die Datenerhebung ist in § 62 SGB VIII für die Jugendhilfe geregelt. Danach dürfen Daten nur erhoben werden, wenn sie für die Erfüllung der Erziehungsaufgabe in der Einrichtung erforderlich sind.*

Wird - schriftlich oder mündlich - also nach Religion, Einkommen, Krankheiten, Geschwistern gefragt, muss klar sein, inwieweit diese Daten notwendig (also nicht nur nützlich) sind, um die Erziehung des Kindes in dieser Einrichtung erfüllen zu können. Fragen nach dem Beruf der Eltern sind daher aus unserer Sicht unzulässig. Ebenso ist die Frage nach einer Krankenversicherung nicht notwendig, da die Abrechnung mit der Krankenkasse nicht Sache des Trägers ist. Die Frage nach dem Hausarzt ist dagegen zulässig, um ihn bei einem Unfall sofort verständigen zu können. Ebenso zulässig ist die Frage nach ansteckenden Krankheiten, aber auch nach Aids, weil bei einer Rauferei oder einem Biss eine Übertragung nicht auszuschließen ist. Fragen nach dem Einkommen sind nur dann zulässig, wenn der Kindergartenbeitrag nach dem Einkommen gestaffelt ist.

Die Frage nach Religion oder Nationalität ist aus unserer Sicht zulässig, weil diese Informationen für die Vorbereitung von Festen von Bedeutung sind. Die Fragen nach der Arbeitsstelle sind nur insofern zulässig, wenn es sich um die Erreichbarkeit der Eltern (Telefonnummern) während der Betreuungszeiten in der Einrichtung handelt, um in evtl. Notfällen die Eltern zu erreichen… .“

Ich habe mich diesen Rechtsausführungen angeschlossen.

10.2.15 Anforderung von Unterlagen durch das Amt für Ausbildungsförderung wegen einer Rückzahlungsprüfung

Ich bin im Jahr 2010 um eine datenschutzrechtliche Überprüfung der Anforderung von Sozialdaten durch ein Amt für Ausbildungsförderung gebeten worden. Die Antragstellerin war vom BAföG-Amt aufgefordert worden, alle Lohnbelege, Bescheide und Arbeitsverträge der letzten fünf Jahre, konkret ab dem Zeitpunkt der erstmaligen Bewilligung von Ausbildungsförderung, vorzulegen, was jedoch nach Auffassung des Rechtsbeistands der Antragstellerin mangels hierfür erforderlicher Rechtsgrundlage rechtswidrig gewesen sein soll.

Ich bin, nachdem ich das BAföG-Amt angehört hatte, zu folgendem Ergebnis gekommen:

Die Datenerhebung seitens des Amts für Ausbildungsförderung in Bezug auf die Anforderung fehlender Unterlagen (Nachweise) hat ihre Rechtsgrundlage in § 20 Abs. 1 Nr. 3 BAföG. Danach ist ein Bewilligungsbescheid unter den dort genannten Voraussetzungen aufzuheben und der Förderungsbetrag zu erstatten, weil der Auszubildende Einkommen im Sinne des § 21 BAföG erzielt hat, das bei der Bewilligung von Ausbildungsförderung nicht berücksichtigt worden ist, jedoch bei einer tatsächlichen Berücksichtigung zu einem niedrigeren Förderungsbetrag geführt hätte. Ob der Auszubildende dabei die fehlende Berücksichtigung zu vertreten hat, ist unerheblich (Urt. des BVerwG vom 8. Juni 1989, 5 C 38/86, gefunden in juris, dort unter Rdnr. 16).

Für die Durchführung einer derartigen (Rückzahlungs-)Prüfung ist das Abfordern von Einkommensunterlagen, soweit diese den Bewilligungszeitraum (kurz: BWZ) betreffen, datenschutzrechtlich nicht zu beanstanden (da zur Aufgabenerfüllung des Amts erforderlich). Nach Mitteilung des BAföG-Amts hatte die Petentin erstmals für den BWZ 11/2005 bis 03/2006 Ausbildungsförderung beantragt und erhalten.

Da § 20 Abs. 1 Satz 1 Nrn. 3 und 4 BAföG nach der Rechtsprechung des Bundesverwaltungsgerichts als abschließende Regelung vertrauensschutzunabhängiger Rückabwicklung des Förderungsrechtsverhältnisses anzusehen ist, ist somit für die Vorschrift des § 48 SGB X und mithin auch für eine entsprechende Geltung der Jahresfrist des § 45 Abs. 4 Satz 2 SGB X kein Raum (Urt. des BVerwG vom 19. März 1992, 5 C 41/88, Rdnr. 13; Urt. des BVerwG vom 8. Juni 1989, 5 C 38/86; Urteil des BVerwG vom 6. Dezember 1984, 5 C 1/83, allesamt gefunden in juris).

Eine entsprechende Datenerhebung seitens des Ausbildungsamts durch das Abfordern von Einkommensunterlagen könnte lediglich dann als nicht erforderlich und mithin unzulässig angesehen werden, wenn eine solche Prüfung der Verwirkung unterläge, hier also die Antragstellerin aufgrund eines besonderen Verhaltens der Behörde nach Treu und Glauben nicht mehr damit zu rechnen brauchte, dass das Amt eine derartige nachträgliche Überprüfung noch durchführen werde (zu den Anforderungen an das Vorliegen einer Verwirkung siehe Kommentierung in: Ramsauer/Stallbaum/Sternal, BAföG-Kommentar, 4. Auflage 2005, § 20 Rdnr. 8 ff. mit Rspr.-Nachweisen). Hierfür waren meines Erachtens jedoch keinerlei Anhaltspunkte erkennbar.

Das Abfordern der Unterlagen war also rechtens gewesen. Den Rechtsbeistand der Petentin habe ich von meiner Rechtsauffassung allerdings nicht überzeugen können.

10.2.16 Erhebung von Daten über die Ausgaben für Lebenshaltung im Wohngeldverfahren

Eine Wohngeldstelle hat von einem Petenten im Rahmen der Antragstellung eine Aufstellung seiner sämtlichen Ausgaben wie Kosten für Ernährung, Bekleidung, Versicherung, Strom, Rundfunk- und Fernsehgebühren, Pkw etc. gefordert. Der Petent sah dies als unverhältnismäßig an (hierzu unter 1.). Zudem hat die Sachbearbeiterin der Wohngeldstelle telefonisch Kontakt mit der für den Petenten zuständigen ARGE aufgenommen, um den Grund für die Einstellung von Leistungen nach dem Sozialgesetzbuch Zweites Buch zu erfahren (hierzu unter 2.).

1. Mit der sogenannten Plausibilitätsprüfung von Anträgen auf Wohngeld habe ich mich bereits in 8/10.2.5 befasst. Danach kommt eine Auflistung aller Ausgaben, aufgeschlüsselt nach den einzelnen Kosten für Ernährung, Unterkunft, Versicherung/Kfz etc., dann in Betracht, wenn die Angaben des Antragstellers auf die Plausibilität des Verhältnisses zwischen Einnahmen und Ausgaben zu überprüfen ist. Datenschutzgerecht ist diese Prüfung im Rahmen eines Gesprächs durchzuführen, dessen Ergebnisse in dem Vordruck „Gesprächsprotokoll über die Plausibilitätsprüfung“ festzuhalten sind. Nachweise über jede einzelne Ausgabe sind nicht zu erbringen (anders beim Einkommen), da die Plausibilitätsprüfung allein dem Zweck dient, die versteckten Einnahmen zu ermitteln.

   Dieses Verfahren ist in dem mir geschilderten Fall nicht eingehalten worden. Insbesondere die pauschale Anforderung einzelner Nachweise über die monatlichen oder täglichen Ausgaben hat gegen § 67 Abs. 1 SGB X i. V. m. §§ 13 ff. WoGG, wonach die Erhebung von Sozialdaten nur zulässig ist, soweit sie - wie in diesem Fall - zur Feststellung des Einkommens erforderlich ist, verstoßen.

   Dass der Antragsteller angegeben hatte, er lebe derzeit von seinem Vermögen, erschien zunächst plausibel, so dass meines Erachtens noch nicht einmal eine Plausibilitätsprüfung angezeigt gewesen war. Dies zu beurteilen ist jedoch die Fachbehörde eher in der Lage als ich. Sollte danach eine Plausibilitätsprüfung erforderlich sein, sind die mit dem SMI abgestimmten Musterschreiben zu verwenden.

   Das Verlangen des Nachweises über den Verkauf eines Hauses, einschließlich des dabei erzielten Erlöses, ist datenschutzrechtlich zulässig. Gemäß § 15 WoGG ist das Jahreseinkommen des Antragstellers zu ermitteln. Dazu können gemäß § 15 Abs. 1 Satz 2 WoGG auch die Verhältnisse vor dem Zeitpunkt der Antragstellung herangezogen werden. Gibt der Antragsteller an, über kein Einkommen zu verfügen, weist sein Konto jedoch ein relativ hohes Habensaldo auf, darf die Behörde ermitteln, ob

dieses Vermögen aus einem Einkommen herrührt. Ist dies - etwa bei einem Verkaufserlös - nicht der Fall, kann die Behörde einen Nachweis dafür verlangen, dass es sich bei dem Vermögen nicht um solches aus einem Einkommen handelt. Diese Erhebung ist gemäß § 67a Abs. 1 Satz 1 SGB X zur Aufgabenerfüllung erforderlich.

2. Die Übermittlung (Mitteilung, dass der Petent Wohngeld beantragt hat) und die Erhebung (zur Frage, nach dem Grund dafür, dass keine Leistungen nach dem Sozialgesetzbuch Zweites Buch bestehen) von Sozialdaten der Wohngeldstelle an die bzw. bei der ARGE war ebenfalls datenschutzrechtlich unzulässig.

   Gemäß § 67a Abs. 2 SGB X sind die Sozialdaten beim Betroffenen zu erheben. Die Erhebung bei den in § 35 SGB I genannten Stellen (also auch bei der ARGE) ist nach § 67a Abs. 2 Nr. 1 SGB X ausnahmsweise erlaubt. Dessen Voraussetzungen liegen jedoch schon insoweit nicht vor, als dem Petenten ausweislich der Akte keine Gelegenheit gegeben wurde, zu erklären, warum er den Antrag auf Leistung nach dem Sozialgesetzbuch Zweites Buch nicht gestellt hat. Diese Klärung hätte keinen unverhältnismäßigen Aufwand erfordert. § 65 Abs. 1 Nr. 3 SGB I ist keine Rechtsgrundlage für eine Datenübermittlung oder -erhebung. Die Vorschrift würde in diesem Fall eine generelle Ausnahme zu den Regelungen des Sozialgesetzbuches Zehntes Buch darstellen und so etwa den Grundsatz der Datenerhebung bei dem Betroffenen aushebeln. Stattdessen begrenzt sie lediglich die Mitwirkungspflichten des Leistungsempfängers. Die Regelungen über den Sozialdatenschutz gelten für alle Sozialgesetzbücher und werden durch die einzelnen Regelungen der anderen Gesetzbücher konkretisiert. Die Regelungen des Sozialgesetzbuches Erstes Buch und des Sozialgesetzbuches Zehntes Buch stehen jedoch nebeneinander, weil sie einen anderen Regelungsinhalt haben. Das Sozialgesetzbuch Erstes Buch kann als allgemeiner Teil des Sozialgesetzbuches daher keine Konkretisierung der Regelungen der §§ 67a ff. SGB X enthalten, die ebenfalls allgemein für alle anderen Sozialgesetzbücher gelten.

10.2.17 Verzicht auf Übersendung der Einwilligungserklärung zur Schweigepflichtentbindung an den um Auskunft gebetenen Arzt im Rahmen von Verfahren nach § 69 SGB IX

Ich bin angefragt worden, ob es aus Gründen der Verfahrenserleichterung gestattet werden kann, im Rahmen eines Feststellungsverfahrens nach § 69 SGB IX auf die Übersendung der Einwilligungserklärung (im Original oder in Kopie) an den um Auskunft gebetenen Arzt zu verzichten und stattdessen den schriftlichen Hinweis gegenüber dem Arzt ausreichen zu lassen, dass die Schweigepflichtentbindung dem zuständigen Amt vorliegt.

Ich halte eine derartige Verfahrensweise hinsichtlich des Nachweises einer Schweigepflichtentbindung durch die Versorgungsverwaltung aus datenschutzrechtlicher Sicht für vertretbar.

Gemäß § 69 Abs. 1 Satz 3 SGB IX i. V. m. § 12 Abs. 2 Satz 3 KOVVfG hat das Landratsamt oder die kreisfreie Stadt als die für die Feststellungen nach § 69 SGB IX zuständige Stelle (§ 15a SächsAGSGB) die Einwilligung einzuholen.

Das SG Frankfurt hat in einer Entscheidung klargestellt, dass ein Gericht dem als Zeuge benannten Arzt nicht im Einzelnen darzulegen hat, inwieweit der Patient ihn gegenüber dem Gericht, also für das gerichtliche Verfahren, von der ärztlichen Schweigepflicht entbunden hat. Es sei vielmehr Sache des Gerichts, von Amts wegen zu prüfen, in welchem Umfang der Arzt von der Schweigepflicht entbunden worden ist. Es genüge, wenn das Gericht dem Arzt mitteilt, dass eine entsprechende Erklärung vorliegt. Ist das der Fall, dann ist der Arzt nicht berechtigt, das Zeugnis mit dem Argument zu verweigern, das Gericht habe ihm gegenüber die Schweigepflichtentbindung nicht nachgewiesen. Nicht der Zeuge entscheidet danach über den Umfang seiner Zeugnispflicht und seine Berechtigung zur Zeugnisverweigerung, sondern allein das Gericht. Auf dessen Auskunft, die Schweigepflichtentbindung liege vor, kann sich der Arzt verlassen (Beschluss v. 24. September 1998, Az: S-4/SF-4798, gefunden in: juris).

Dasselbe gilt meiner Rechtsauffassung nach auch für die Einholung der notwendigen Schweigepflichtentbindung seitens einer Behörde. Falls daher dem Arzt eine ggf. vorliegende Beschränkung einer Schweigepflichtentbindungserklärung nicht mitgeteilt wird oder eine solche insgesamt nicht vorliegen sollte, dies jedoch dem Arzt von der Daten erhebenden Stelle - wie hier - schriftlich zugesichert wird, fehlt es im Hinblick auf § 203 StGB an einem vorsätzlichen und mithin an einem strafbaren Handeln des Arztes.

In datenschutzrechtlicher Hinsicht ist es daher unter dieser Voraussetzung nicht notwendig, dass der Arzt eine Kopie der Schweigepflichtentbindungserklärung erhält, da der Sozialleistungsträger die Verantwortung für die Richtigkeit der Angaben („Schweigepflichtentbindungserklärung liegt vor“) in seinem Gesuch trägt und der Arzt sich auf die Versicherung der öffentlichen Stelle verlassen darf.

Die Pflicht des Arztes, bei Vorliegen eines entsprechenden Ersuchens für jeden Fall konkret zu prüfen, welche Daten er übermittelt, bleibt hiervon unberührt. Der Arzt trägt (weiterhin) die Verantwortung dafür, dass er nur die zur Feststellung einer Schwerbehinderung erforderlichen Daten an das Versorgungsamt übermittelt. Beispielsweise

dürfte die Übermittlung der vollständigen Krankengeschichte in der Regel daher nicht erforderlich sein.

Im Hinblick auf diese meine Rechtsauffassung hatte ich bereits 2007 die damalige Rechtsaufsichtsbehörde über die Versorgungsämter gebeten, sicherzustellen, dass denjenigen Ärzten, die Zweifel am Vorliegen der Einwilligungserklärung anmelden, eine Kopie der Erklärung des Antragstellers übersandt wird. Eine Anfrage aus dem Jahr 2010 habe ich zum Anlass genommen, auch die nunmehr zuständige Rechtsaufsichtsbehörde (§ 15a Abs. 1 Satz 3 SächsAGSGB) ebenfalls darauf hinzuweisen.

10.2.18 Die weitere Entwicklung des Sächsischen Kindergesundheits- und Kinderschutzgesetzes

Das neue Sächsische Kindergesundheits- und Kinderschutzgesetz ist im Juli 2010 in Kraft getreten (GVBl. S. 182) und hat das Sächsische Kindergesundheits- und Kinderschutzgesetz vom 19. Juni 2009 (GVBl. S. 379) abgelöst (siehe hierzu ausführlich 14/10.2.2).

Nach § 7 des Gesetzes ist 15 Monate nach Inkrafttreten des Gesetzes dem Landtag ein Bericht über die Umsetzung und die Auswirkungen sowie den Weiterentwicklungsbedarf der in diesem Gesetz vorgesehenen Maßnahmen zum Schutz von Kindeswohl und Kindergesundheit zu erstatten. Soweit möglich, geschieht dies auf der Grundlage einer wissenschaftlichen Evaluation. Darüber hinaus sollen entsprechende fachliche Beiträge, insbesondere des Landesjugendamtes und der Jugendämter, Eingang in den Bericht finden. Auch ich bin zu beteiligen.

Eine entsprechende Evaluation ist in Rheinland-Pfalz zum dortigen Kinderschutzgesetz bereits im November 2010 veröffentlicht worden (siehe hierzu unter 17.2.2.2 Fn. 24). Danach sind dort im Jahre 2009 rund 258.000 Datensätze, dabei 26.435 Meldungen über nicht bestätigte oder nicht wahrgenommene Früherkennungsuntersuchungen verarbeitet worden. Durch Nutzung dieser Daten ist lediglich in sechs Fällen eine Kindeswohlgefährdung aufgedeckt worden, die den Jugendämtern nicht ohnehin, also ohne das Betreiben des betreffenden Registers, d. h. der Überwachung der Teilnahme an den Früherkennungsuntersuchungen, bekanntgeworden ist. Der Nutzungsgrad bzw. die Trefferquote liegt demnach bei ‚brutto' reichlich *0,002 %*.

Nach ersten mir bekannt gewordenen Hinweisen betreffend die Evaluation des Sächsischen Kindergesundheits- und Kinderschutzgesetzes kann der Schluss gezogen werden, dass im Freistaat Sachsen noch kein Fall von Kindeswohlgefährdung im Rahmen des Einladungs- und Erinnerungswesens identifiziert werden konnte.

Auf die weitere Entwicklung der Anwendung dieses Gesetzes kann man daher sehr gespannt sein.

10.3 Lebensmittelüberwachung und Veterinärwesen

10.3.1 Auskunftserteilung und Akteneinsicht in Veterinär- und Tierschutzangelegenheiten

Mehrfach wandten sich Betroffene, die sich als Hinweisgeber oder Anzeigeerstatter in Tierschutzangelegenheiten zu erkennen gaben, an mich und gaben an, dass die Veterinärschutzämter ihre Daten gegenüber Tierhaltern offenbart hätten. Zumeist habe es sich dabei um Fälle der Akteneinsichtnahme durch den Tierhalter oder einen von diesem beauftragten Rechtsbeistand gehandelt.

Ob bei der Auskunft oder Akteneinsichtnahme der Hinweisgeber oder Anzeigeerstatter mitgeteilt werden darf oder geheim gehalten werden muss, richtet sich nach den Umständen des Einzelfalls und nach dem Verfahrensstand. In Bezug auf die gesetzlichen Grundlagen ist entscheidend, ob ein Verwaltungs-, Ordnungswidrigkeiten- oder Strafverfahren betrieben oder außerhalb eines bereichsspezifisch geregelten Verfahrens gehandelt worden ist.

Vor und nach einem Verwaltungsverfahren ist das Sächsische Datenschutzgesetz maßgebend. § 18 SächsDSG gewährleistet dem Betroffenen, hier also dem Tierhalter, Auskunft und nach Absatz 3 Satz 1 Akteneinsicht, wenn eine Akte zur Person des Betroffenen geführt wird. Gemäß Absatz 5 Nr. 3 sind bei der Auskunft und Akteneinsicht allerdings die berechtigten Interessen Dritter, hier also des Hinweisgebers, abzuwägen. Eine Auskunft oder Einsichtnahme hat zu unterbleiben, wenn die Drittinteressen gegenüber denen des Auskunftsersuchenden überwiegen (vgl. 9/10.2.10). Eine Preisgabe des Hinweisgebers oder des Anzeigeerstatters hat auch zu unterbleiben, wenn die Behörde noch die Eröffnung des Verwaltungsverfahrens prüft und nicht klar ist, ob der Hinweisgeber oder Anzeigeerstatter - worauf es ankommt - redlich ist. Auch nach einem durchgeführten Verwaltungs- oder Bußgeldverfahren kann Auskunft und Akteneinsicht gewährt werden, wenn das berechtigte Interesse des Hinweisgebers oder Anzeigeerstatters nicht überwiegt. Berücksichtigt werden kann dabei auch die schon erfolgte Offenbarung von Daten in einem vorhergehenden Verwaltungs- oder Bußgeldverfahren. Die Fälle der Auskunft und Einsichtnahme nach dem Sächsischen Datenschutzgesetz sind aber eher selten. Zumeist ist nach dem Verwaltungsverfahrensgesetz oder dem Ordnungswidrigkeitengesetz in Verbindung mit der Strafprozessordnung zu verfahren. Die Auskunftsvorschriften des Sächsischen Datenschutzgesetzes gelten während dieser Verfahren nicht parallel (§ 2 Abs. 4 SächsDSG).

Nach Verwaltungsverfahrensrecht besteht ein Akteneinsichtsrecht bei - nicht abgeschlossenen - Verwaltungsverfahren zur erforderlichen Geltendmachung oder Verteidigung der rechtlichen Interessen (§ 29 VwVfG). Allerdings sind auch nach dieser Vorschrift berechtigte Interessen der Beteiligten oder dritter Personen zu berücksichtigen. Daher ist jeweils zu prüfen, ob der Dritte als Hinweisgeber oder Anzeigeerstatter gegenüber dem beteiligten Tierhalter genannt werden darf. Zunächst ist hierfür das „berechtigte Interesse“ des Hinweisgebers oder Anzeigeerstatters maßgeblich. Das berechtigte Interesse wird immer dann zu bejahen sein, wenn der Anzeigeerstatter oder Hinweisgeber redlich ist, d. h. wenn er z. B. aufgrund der Umstände davon ausgehen durfte, dass der Tierhalter gegen Tierschutzvorschriften verstoßen hat. Die Informanten, die leichtfertige Behauptungen, Nachreden vom Hörensagen oder bösgläubig Unterstellungen an Behörden übermitteln, sind dagegen in aller Regel in ihrem Geheimhaltungsinteresse als nur eingeschränkt schutzwürdig anzusehen. Darüber hinaus wird aber entscheidend sein, ob die Angaben des Hinweisgebers oder Anzeigeerstatters als Grundlage für eine Verwaltungsentscheidung dienen sollen. Ist das der Fall, sind diese Personen auch gegenüber dem beteiligten Tierhalter namentlich zu bezeichnen. In nicht wenigen Fällen auftretender Verstöße gegen den Tierschutz kann aber dann auf die Benennung der Hinweisgeber und Anzeigeerstatter verzichtet werden, wenn die Feststellungen der Amtstierärzte für die behördlichen Maßnahmen allein bereits ausreichen. Dies sollten die Veterinärbehörden beachten.

Bei Bußgeld- und Strafverfahren richtet sich der Akteneinsichtnahmeanspruch nach § 46 OWiG i. V. m. § 147 StPO. Das Recht steht dem Verteidiger zu, der den zur Kenntnis genommenen Inhalt der Akte an den Beschuldigten weitergeben darf. Der Hinweisgeber oder Anzeigeerstatter wird, soweit es auf dessen Kenntnisse angekommen ist, als Beweismittel zu benennen sein. Auch im gerichtlichen Verfahren selbst können letztendlich Hinweisgeber und Anzeigeerstatter bekannt werden.

10.4 Rehabilitierungsgesetze

In diesem Berichtszeitraum nicht belegt.

11 Landwirtschaft, Ernährung und Forsten

11.1 Verarbeitung personenbezogener Daten von Subventionsempfängern in der Landwirtschaft

Im Wege der Transparenzinitiative der EU ist die Brüsseler Verwaltung bemüht, die Bürger zu informieren, wie über die EU verwaltete Steuergelder Verwendung finden. Das Anliegen an sich erscheint positiv. Jedoch sollten die Empfänger von Subventionen namentlich im Internet veröffentlicht werden. Bei den Agrarbeihilfen für Landwirte begann man mit der Durchsetzung dieses Vorhabens mit der Verordnung Nr. 1290/2005. Der Datenschutzbezug bei der Veröffentlichung von namens- und adressbezogenen Angaben in Verbindung mit konkreten Beihilfebeträgen ist evident. Die Daten waren nach der Verordnung unterschiedslos zu veröffentlichen, ob es sich um große Agrargesellschaften oder um Kleinbauern handelte, auch unabhängig von dem Beihilfebetrag. Das hielt ich für zu wenig differenziert und unverhältnismäßig.

Nachdem ich mich im Zusammenwirken mit der Staatsregierung frühzeitig um eine datenschutzverträgliche Veröffentlichungspraxis bemühte, kam die Wende von gerichtlicher Seite - durch den Europäischen Gerichtshof (vgl. 3.1) - unerwartet.

Das SMUL konnte daraufhin die Veröffentlichung wieder einstellen.

12 Umwelt und Landesentwicklung

12.1 Gesetz über die Geodateninfrastruktur im Freistaat Sachsen

In meinem letzten Tätigkeitsbericht hatte ich bereits auf ein vorzubereitendes Gesetz, das den Umgang mit Geodaten in Sachsen regelt, hingewiesen (vgl. 14/12.1 und 14/16.1.14). Der Sächsische Landtag verabschiedete im Mai 2010 das Gesetz über die Geodateninfrastruktur im Freistaat Sachsen (Sächsisches Geodateninfrastrukturgesetz). Das europäische Recht regelt mit der sogenannten INSPIRE-Richtlinie die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für behördliche, wirtschaftliche und private Nutzungen. Die Richtlinie war in Sachsen europarechtlich umzusetzen. Ziel der Gesetzgebung ist das Verfügbarmachen von georeferenzierbaren Angaben, Daten mit Raumbezug. Hierbei können wegen der Beziehbarkeit der Raumkoordinaten auf Adressen und natürliche Personen die Geodaten personenbezogen sein, so dass die gesetzlichen Regelungen zur Nutzung von Geodaten auch angemessene Datenschutzregelungen zu enthalten haben (vgl. auch die Entschließung der DSK unter 14/16.1.14).

Bei dem Gesetzgebungsverfahren wurde ich von der Staatsregierung und in den Landtagsausschüssen beteiligt und erhielt dadurch die Gelegenheit, noch datenschutzrechtliche Verbesserungen zu erreichen. Eine pauschalierende Unterscheidung von personenbezogenen Daten, die generell nicht schutzwürdig sein sollten, konnte vermieden werden. Darüber hinaus erscheint mir die gesetzgeberische Beschränkung des Zugangs der Öffentlichkeit, wenn personenbezogene Daten offenbart und dadurch schutzwürdige Interessen Einzelner beeinträchtigt werden, gelungen (vgl. § 8 Abs. 4 SächsGDIG). Vorbildhaft ist aus meiner Sicht auch die weitgehende Beteiligung Betroffener, wenn die Veröffentlichung einer großen Anzahl von gleichartigen Geodaten in einem Massenverfahren vorgesehen ist. Im Rahmen eines Bekanntmachungs- und Anhörungsverfahrens erhalten die Betroffenen dennoch Gelegenheit, Gehör und Berücksichtigung zu finden (§ 8 Abs. 5 SächsGDIG). Auch haben Private, die Behörden freiwillig Informationen überlassen, bei vorgesehenen Veröffentlichungen durch die Behörden ihre Einwilligung zu erteilen (§ 8 Abs. 6 SächsGDIG).

Noch ist die breite Nutzung von Geodaten seitens der Behörden und der Wirtschaft in einem frühen Stadium. Das wird sich ändern. E-Governance-Anwendungen, erkennbare Bemühungen der Verwaltung für einen offeneren Umgang mit den eigenen Datenbeständen und neue Geschäftsfelder und -modelle im Bereich der Wirtschaft mit ihrer eigenen Dynamik werden dazu beitragen. Ich bin zuversichtlich, dass sich das sächsische Gesetz nachhaltig bewähren wird.

12.2 Die Zulässigkeit sogenannter „Solarkataster“

In sächsischen Städten und Gemeinden wird zum Teil erwogen, sogenannte „Solarkataster“ einzuführen. Dabei geht es um die Möglichkeit der Nutzbarmachung von Grundstücksflächen - insbesondere von Dachflächen - zur Gewinnung von Solarstrom. In Rede stehen vor allem Internetveröffentlichungen zu derartigen Informationen. Auf Grundlage des Sächsischen Geodateninfrastrukturgesetzes können Umweltinformationen allgemein zugänglich gemacht werden (vgl. 12.1).

Ein Angebot an die Öffentlichkeit im Hinblick auf die Geeignetheit von Grundstücks- und Dachflächen zur Solarstromgewinnung bedeutet aber auch, dass den Wert berührende Informationen zu konkreten Grundstücken publiziert werden können. Wegen des Personenbezugs der georeferenzierten grundstücks- und adressbezogenen Angaben, ist daher grundsätzlich zu gewährleisten, dass nur erforderliche Angaben - insbesondere über das Internet - veröffentlicht werden. Die Veröffentlichungsweise und die Daten, die bekanntgemacht werden und zur Information „erforderlich“ sein sollen, sollten geeigneterweise abschließend in einer Satzung festgelegt werden. Zu den ohnehin allgemein zugänglichen Angaben wie Straße und Hausnummer oder Luftaufnahmen können so noch aggregierte Informationen hinzukommen, z. B. die „Geeignetheit“ oder „Nicht-Geeignetheit“ einer Grundstücksfläche.

Soweit Informationen mit weiter- und tiefergehenden Auskünften angereichert werden sollen, z. B. mit dem erreichbaren finanziellen oder dem Solarstrom-Ertrag, wird man eine Erforderlichkeit zur Veröffentlichung auch über eine Satzung nur bedingt herstellen können. Damit ist auch in Frage gestellt, ob es genügt, wenn die Behörden, um weitergehende Solarpotenzialinformationen gerichtsfest veröffentlichen zu können, die Einräumung einer Widerspruchsmöglichkeit der betroffenen Eigentümer, Grundstücksbesitzer oder sonst berechtigten Personen gegen die Bekanntmachung vorsehen oder ob nicht dann eine vor Veröffentlichung einzuholende Einwilligung in jedem Einzelfall erforderlich ist.

Auch im Hinblick auf die Darstellungsweise der Solarkatasterangaben werden sich, insbesondere bei bildlicher Darstellung, was die Auflösung, die Bildpunkte und den Maßstab betrifft, Fragen und Probleme ergeben, bei denen meine Behörde ebenfalls berät.

12.3 Wasserbuch

Im letzten Berichtszeitraum hatte ich das SMUL auf den leicht zugänglichen Abruf von personenbezogenen Daten aus dem Wasserbuch aufmerksam gemacht und Bedenken

angemeldet. Die Einsichtnahme in das Wasserbuch ist gemäß § 106 Abs. 1 Satz 1 SächsWG zwar jedermann gestattet. Einzelne Betroffene sind aber über das dafür eingerichtete Internetangebot leicht zu recherchieren und können mit Namen und Adressen sogar listenweise zusammengestellt werden.

Die Daten zu den Inhabern von Wasserrechten sind unstreitig auch Umweltinformationen im Sinne des Sächsischen Umweltinformationsgesetzes. Im Hinblick auf die Frage, ob die datenschutzrechtlichen Anforderungen des § 6 SächsUIG, wonach sich Einschränkungen bei der Datenverarbeitung zum Schutz privater Belange ergeben, auch in dem bereichsspezifischen Wasserrecht zu gelten haben oder die wasserrechtlichen Bestimmungen als spezieller anzusehen sind, konnte mit dem Staatsministerium noch keine Einigung erzielt werden. Das Konkurrenzverhältnis zwischen Wasser- und Umweltinformationsrecht ist rechtlich und gesetzlich als weitgehend ungeklärt zu betrachten.

Jedenfalls hat mir das Staatsministerium zugesagt, bei der anstehenden Novellierung des Sächsischen Wassergesetzes zu prüfen, ob personenbezogene Daten aus dem Internetangebot des Wasserbuchs herausgenommen und die Recherchierbarkeit eingeschränkt werden kann.

13 Wissenschaft und Kunst

13.1 Datenschutz zugunsten des Wissenschaftlers im Verhältnis zur Hochschule - Klage der TU Dresden gegen eine Beanstandung aus dem Jahre 2003 rechtskräftig abgewiesen

Die in 11/13.3 auf S. 150 bis 153 ausführlich dargestellte, seinerzeit auch dem Landtag zugeleitete und von diesem in einer Plenarsitzung (vom 11. September 2003, Plenar-Protokoll S. 6 473 bis 6 475) so gut wie einhellig gebilligte Beanstandung einer Hochschule hatte die heftige Gegenwehr des damaligen Rektors bzw. der Hochschule ausgelöst: Ein strafrechtliches sowie ein zivilrechtliches Verfahren sind in den Jahren 2003 bis 2004 gescheitert. Der daneben unternommene Versuch, die Beanstandung von der Verwaltungsgerichtsbarkeit rechtlich aus der Welt schaffen zu lassen, hat sich auf eine Verletzung der Wissenschaftsfreiheit der Hochschule stützen wollen. Dieser Versuch ist nach einem anfänglichen Erfolg vor dem VG Dresden im Jahre 2007 (Az: 1 K 1158/04) nunmehr vor dem OVG gescheitert (Urt. v. 21. Juni 2011 - Az: 3 A 224/10). Das Gericht hat entschieden, dass die Beanstandung keinen Eingriff in den Wissenschaftsbetrieb der Hochschule (also deren Teilhabe am Grundrecht der Wissenschaftsfreiheit) dargestellt hat und dass die Hochschule auch keine rechtsverletzende Rufschädigung hat geltend machen können, nur weil die Beanstandung seinerzeit „pointiert“ und „prägnant“ formuliert worden ist.

Vor allem hat das Gericht die Auffassung der Vorinstanz zurückgewiesen, dass die Beanstandung eine Zuständigkeitsüberschreitung gewesen sei, weil der Rektor als Verfasser und der Staatsminister als Empfänger des relevanten Schreibens bei dem Vorgang nicht als Amtsträger, sondern als Privatleute gehandelt hätten. Dem ist eben gerade nicht so gewesen.

Solche - zum Glück insgesamt seltenen - gerichtlichen Streitigkeiten verursachen erheblichen Verwaltungsaufwand in meiner Behörde. Dieser ist aber erforderlich, um eine notwendige Klärung zu erlangen. Der Text des - nur zum Teil in RDV 2011, 249 wiedergegebenen - Urteils ist nachstehend unter 17.2.1 abgedruckt.

13.2 Datenschutzkontrollzuständigkeiten im Hinblick auf die Software-Entwicklung durch staatliche Hochschulen

Der BfDI hat eine Eingabe an mich weitergeleitet, in der der Petent darauf hinwies, dass eine sächsische Fachhochschule ein Entwicklungs-Vorhaben betreibe, in dem Software zur Ausforschung der sogenannte Browser-Historie programmiert werde, und zwar dergestalt, dass dann personenbezogene Daten zum Kunden- bzw. Interessentenverhalten

bei der Internet-Nutzung gewonnen werden können, die zielgerichtete Werbung im Bereich des Internet-Versandhandels ermöglichen würden.

Ich habe dem BfDI mitteilen müssen, dass ich aufgrund der Zuständigkeiten meiner Behörde nach dem Sächsischen Datenschutzgesetz keine Befugnis zum Handeln gegenüber der Fachhochschule habe, weil diese, als unter § 2 Abs. 1 SächsDSG fallende öffentliche Stelle, im Falle der Richtigkeit der von dem Hinweisgeber gemachten Angaben keine personenbezogenen Daten verarbeitet, so dass der Vorgang nicht unter § 1 SächsDSG fällt; Letzteres galt auch für die Hilfestellung, die gegebenenfalls die Fachhochschule durch Entwicklung entsprechender IT-Programme für private Dritte für deren späteres Verarbeitungshandeln leisten würde. Aus diesem Grund schied auch eine (vom BfDI erwogene) Behandlung im Arbeitskreis „Medien“ der DSK unter Zuständigkeitsgesichtspunkten aus.

Die Frage, inwieweit staatliche Hochschulen befugt sind, Entwicklungs-Vorhaben durchzuführen, die zu einem möglicherweise in der Bundesrepublik Deutschland nach derzeit geltendem Recht nicht einsetzbaren Produkt führen (das jedoch etwa für das Ausland lizenziert werden könnte), ist eine Rechtsfrage der allgemeinen Hochschul-Rechtsaufsicht, weswegen ich auch das SMWK von der Angelegenheit unterrichtet habe.

Aus der - anderen - Zuständigkeit meiner Behörde aus *§ 38 BDSG* ergibt sich nach dem Bundesdatenschutzgesetz keine Befugnis, mit der jedem behördlichen Tätigwerden notwendig zukommenden Amtsautorität (Ausübung öffentlicher Gewalt) auf die Entwickler von IT-Programmen einzuwirken, auch - und zugleich zumal - wenn es sich um öffentliche Stellen handelt. Insbesondere hat sich aus § 38 BDSG keine Befugnis ergeben, von der Hochschule genauere Auskünfte über ihr Vorhaben zu verlangen.

Inwieweit das SMWK der Angelegenheit nachgegangen ist, habe ich nicht erfahren. Dem Hinweisgeber habe ich mitzuteilen gehabt, dass ihm keine Auskunft über die Behandlung der Angelegenheit zu erteilen war.

13.3 Befragung von Elternvertretern und Eltern im Rahmen der Erstellung eines „Schulführers“

Ich bin davon in Kenntnis gesetzt worden, dass Elternvertreter, vor allem aber auch Eltern von Schülern der Klassenstufen 6, 9 und 11 an sächsischen Gymnasien unter Beteiligung von Mitarbeitern der Fakultät Erziehungswissenschaften der TU Dresden befragt werden sollten, um - so das Anschreiben der Initiatoren - den Eltern von Grund-

schülern der 4. Klasse beim anstehenden Schulwechsel Hilfestellung bei der Auswahl des „richtigen“ Gymnasiums zu geben.

Ausweislich des Anschreibens an die Elternratsvorsitzenden der betreffenden Gymnasien sollte es sich dabei um eine anonyme Befragung handeln. Hierzu wurden die Elternvertreter „um die gesicherte Weitergabe der vorbereiteten Umschläge und Informationen an die Elternsprecher dieser Jahrgangsstufen“ gebeten. Eine Angabe dazu, wer genau die Daten erhebende Stelle ist, war den mir vorliegenden Unterlagen nicht zu entnehmen. Jedenfalls wurde der Eindruck erweckt, dass die ausgefüllten Fragebögen als solche von der Hochschule ausgewertet werden sollen.

Als für die TU Dresden nach § 2 Abs. 1 SächsDSG zuständige Datenschutzkontrollbehörde habe ich vorsorglich darauf aufmerksam gemacht, dass wissenschaftliche Forschung betreibende öffentliche Stellen sich nur an solchen Verarbeitungen möglicherweise personenbezogener bzw. personenbezogen gewesener Daten beteiligen dürfen, die auch soweit es das Handeln anderer beteiligter Kooperationspartner betrifft datenschutzrechtlich einwandfrei ausgestaltet sind.

Im vorliegenden Fall habe ich angenommen, dass die mit dem Fragebogen erhobenen Daten ab Empfang durch die TU Dresden in der Tat als anonym anzusehen sind. In der vorhergehenden Phase der Befragung war das jedoch nicht ohne Weiteres der Fall. Vielmehr hing dies davon ab, ob es hinreichend gesichert war, dass die Daten nach Ausfüllen des Fragebogens (vermutlich ja:) an der Schule, also bis zum Eingang bei der TU Dresden, keinem Dritten, insbesondere nicht Lehrern oder Elternvertretern zugänglich waren; diese verfügten nämlich über erwartbares Zusatzwissen im Hinblick auf Merkmalsausprägungen zu einigen Fragen aus dem Fragebogen, das die Anonymität des Fragebogeninhaltes entfallen ließe.

In dem betreffenden Anschreiben an die Elternvertreter fanden sich keinerlei Aussagen, wie der Rücklauf der ausgefüllten Fragebögen an die TU Dresden im Einzelnen konkret erfolgen sollte. Eine Überprüfung, ob es sich also tatsächlich - wie behauptet - um eine anonyme Befragung der Eltern handelt, war mir nicht möglich.

Ich habe die TU Dresden aufgefordert mir mitzuteilen, in welcher Weise die Weitergabe der ausgefüllten Fragebögen und deren Weiterleitung an die Fakultät im Einzelnen erfolgen und wie sichergestellt werden sollte, dass dabei insbesondere keine Einsicht in die ausgefüllten Fragebögen seitens der Schulleitung bzw. der Lehrer erfolgen kann. Entsprechende Abmachungen, die dazu mit den anderen beiden beteiligten Stellen, also der Zeitung und dem Landeselternrat, getroffen worden sind, sollten mir ebenfalls zur Verfügung gestellt werden. Welche Informationen die befragten Personen, insbesondere

die Eltern, zur Frage des datenschutzgerechten Datentransportes der ausgefüllten Fragebogen zur TU erhalten sollten, bat ich ebenfalls mitzuteilen.

Durch das Antwortschreiben der TU Dresden sind meine datenschutzrechtlichen Bedenken nicht ausgeräumt worden.

Dies betraf insbesondere die Frage, wie sichergestellt worden ist, dass keine Einsicht in die ausgefüllten Fragebögen seitens der Schulleitung bzw. der Lehrer oder auch anderer Eltern möglich war. Soweit erkennbar, sind dazu keine konkreten Abmachungen zwischen der TU Dresden, der Zeitung und dem Landeselternrat getroffen worden. Die TU Dresden hat mir diesbezüglich keinerlei Ausführungen gemacht und keine Unterlagen vorgelegt, obwohl ich danach gefragt hatte. Die Universität schrieb nur vage von „Empfehlungen“, die sie gegeben hätte.

Darüber hinaus war die von der TU Dresden mir gegenüber abgegebene Zusicherung, dass Lehrer und Schulleiter zu keinem Zeitpunkt in die Erhebung involviert (gewesen) seien, falsch:

Aus den in meiner Behörde zu dem betreffenden Projekt eingegangenen Eingaben ergab sich vielmehr, dass es vorgekommen war, dass die Fragebögen beim Schulsekretariat abgegeben werden konnten, ja sogar abgegeben werden sollten. In einem Fall waren die ausgefüllten Fragebögen sogar von dem Klassenlehrer eingesammelt worden, sodass selbstverständlich auch die Vollständigkeit des Klassensatzes kontrolliert werden konnte.

In einem mir geschilderten Fall war nach Angaben des Petenten zudem auch erst auf ausdrückliche Nachfrage eines Elternteils auf die Freiwilligkeit der Befragung hingewiesen worden!

Es war daher festzustellen, dass der Rücklauf der Fragebögen nicht in einer Weise organisiert worden war, die die zugesicherte Anonymität des Fragebogeninhaltes durchweg in der gebotenen Weise gesichert hätte. Somit hatte sich die Hochschule die Daten - unter Ausnutzung von Beschaffungsmöglichkeiten eines Dritten - gerade nicht auf datenschutzrechtlich einwandfreie Weise, sondern wegen ihrer Verantwortung auch für die Beschaffungsphase unter Verstoß gegen Datenschutzrecht beschafft.

Die weiteren mir gegenüber gemachten schriftlichen Ausführungen der TU Dresden dazu, inwieweit bei verschlossenen Umschlägen ein zwischenzeitliches - unterstellt: unbefugtes - Öffnen bemerkt werden könnte, gingen leider vollständig am Problem vorbei. Dieses bestand nämlich wie bereits erwähnt darin, dass keine zureichenden Maßnahmen getroffen worden waren, durch die abgesichert worden wäre, dass die einzelnen Eltern

tatsächlich den von ihnen ausgefüllten Fragebogen in den Umschlag stecken und diesen verschließen konnten, bevor sie den Fragebogen aus der Hand gaben. Somit war eben *nicht* in hinreichendem Maße ausgeschlossen, dass vom Inhalt der ausgefüllten Unterlagen Dritte - andere Eltern, Elternvertreter oder insbesondere auch Mitarbeiter der Schule - Kenntnis erhalten konnten. Dies war um so mehr zu bedenken, als ein selbst „gutwilliges“ Mitwirken von Personen aus dem Bereich der Schule beim Einsammeln der Fragebögen gerade aufgrund des von der TU Dresden zitierten Schreibens der Sächsischen Bildungsagentur, welche offensichtlich die Schulleiter ausdrücklich gebeten hatte, die Elternvertreter an der Schule bei der Durchführung der Elternbefragung organisatorisch zu unterstützen, nicht ausgeschlossen werden konnte.

Im Übrigen handelte auch der als weiterer Initiator der Befragung beteiligte (Landes-)Elternrat hierbei nicht als Privatperson(en), sondern auf der Grundlage der Bestimmungen der Elternmitwirkungsverordnung als „öffentliche Stelle“ im Sinne des § 2 SächsDSG (so auch die Rechtsauffassung des SMK) und unterlag damit - ebenso wie die gesamte Aktion - den strengen Bestimmungen für Datenverarbeitung durch öffentliche Stellen. Dazu gehört insbesondere auch § 9 Abs. 2 Nr. 1 SächsDSG, wonach bei der Verarbeitung personenbezogener Daten durch entsprechende Maßnahmen zu gewährleisten ist, dass nur Befugte diese Daten zur Kenntnis nehmen können. Diese Bestimmung war vorliegend offenkundig nicht eingehalten worden.

Fazit: Den von der TU Dresden vorgelegten Ausführungen war nichts zu entnehmen, was Anlass gewesen wäre, meine Rechtsauffassung im Hinblick auf das vorliegend zum Einsatz gekommene ungesicherte Verfahren des Rücklaufs der Fragebögen unter Einschaltung der Schulen zu ändern.

Da der Rücklauf der Fragebögen zu diesem Zeitpunkt bereits weitestgehend abgeschlossen war, sah ich in dieser Angelegenheit keinen weiteren Bedarf für einen Gedankenaustausch mit der Universität, habe ihr jedoch mitgeteilt, dass ich mich im Wiederholungsfalle nicht in der Lage sähe, von einer förmlichen Beanstandung abzusehen.

13.4 Nutzung von Adressdaten durch Bibliotheken für das Versenden von Erinnerungs-E-Mails an Ausleiher

Ein Petent war der Auffassung gewesen, dass das Angebot einer sächsischen Bibliothek, den Nutzer über den Ablauf der Leihfrist ausgeliehener Bücher kurz zuvor per E-Mail zu benachrichtigen, datenschutzrechtlich unzulässig sei.

Ich bin bei meiner rechtlichen Prüfung zu einem anderen Ergebnis gekommen:

Die betreffende Bibliothek in ihrer Rechtsform als Anstalt des öffentlichen Rechts unterliegt als öffentliche Stelle des Freistaates Sachsen dem Sächsischen Datenschutzgesetz. Gemäß § 4 Abs. 1 SächsDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn dieses Gesetz oder eine andere Vorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat. Gemäß § 12 Abs. 1 SächsDSG ist das Erheben personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

Gesetzliche Aufgabe dieser Bibliothek ist u. a. auch die Vermittlung der für Lehre, Forschung und Studium an einer sächsischen Hochschule erforderlichen Literatur und anderer Informationsträger. Wie die dazugehörige Leihe von Literatur an die Nutzer erfolgt, ist in der Benutzerordnung geregelt.

Für die Abwicklung der Bücherleihe stellt die Bibliothek dem Nutzer zwei Möglichkeiten der Benachrichtigung (Erinnerung an Ablauf der Leihfrist, Vormerkbenachrichtigung, Rückforderung nach Ablauf der Leihfrist) zur Verfügung. Er kann wählen, ob er per E-Mail benachrichtigt werden soll oder per Post. Wählt er die Benachrichtigung per Post, muss er seine E-Mail-Adresse nicht bekanntgeben, allerdings auch die Portogebühren zahlen.

Die Benachrichtigung des Nutzers und die dafür erhobenen Adressdaten sind für die Aufgabenerfüllung der Bibliothek erforderlich. Dies gilt zunächst für die Benachrichtigung, dass ein vorgemerktes Medium zur Verfügung steht, als auch für die Rückforderung der Medien nach Ende der Leihfrist. Aber auch die Erinnerung an den Ablauf der Leihfrist ist für die Aufgabenerfüllung erforderlich. So kann in einem viel größeren Umfang gewährleistet werden, dass ausgeliehene Bücher rechtzeitig zurückgegeben werden, als mit dem bloßen Hinweis auf das Ende der Leihfrist bei der Ausleihe. Zwar ist die Bibliothek nicht zu einer Erinnerung an das Ende der Leihfrist verpflichtet, dies ist jedoch auch keine Voraussetzung für die Erforderlichkeit zur Aufgabenerfüllung im Sinne des Datenschutzrechts.

Für die Aufgabenerfüllung nicht erforderlich ist die Erhebung der E-Mail-Adresse, da die genannten Benachrichtigungen auf dem Postweg erfolgen können. Die Erhebung der E-Mail-Adresse für eine alternative elektronische Benachrichtigung ist jedoch gemäß § 4 Abs. 1 Nr. 2 SächsDSG zulässig. Danach ist die Verarbeitung personenbezogener Daten auch erlaubt, soweit der Betroffene eingewilligt hat. Eine solche Einwilligung stellt die Wahl der Benachrichtigungsart auf dem Anmeldeformular der betreffenden Bibliothek dar. Diese erfüllt auch die Voraussetzungen des § 4 Abs. 3 und 4 SächsDSG. Das Formular erklärt die beabsichtigte Datenverarbeitung und ihren Zweck. Die Folgen der Weigerung werden ebenso transparent (Versand per Post). Das Schriftformerfor-

dernis ist bei der herkömmlichen Anmeldung dadurch gewahrt, dass der Nutzer eine Benachrichtigungsart wählen kann. Die elektronische Einwilligung im Rahmen der Online-Anmeldung ist als Form ebenfalls angemessen, da sie sich von der herkömmlichen Anmeldung nur insofern unterscheidet, als die Wahl der Benachrichtigung nicht angekreuzt, sondern per Mausklick gewählt wird.

Die Freiwilligkeit der Einwilligung wird auch nicht dadurch ausgeschlossen, dass die Alternative des Postversandes dem Nutzer mit den Kosten des Portos in Rechnung gestellt wird. Anders als bei einem E-Mail-Versand entstehen bei dem Postversand Auslagen, die die Bibliothek in Rechnung stellen kann. Es handelt sich daher nicht um eine Gebühr, die allein den Zweck haben soll, die Nutzer von der Wahl dieser Alternative abzuhalten.

Ist die Angabe der E-Mail-Adresse somit freiwillig, ist die Bibliothek nicht verpflichtet, eine E-Mail, die sie an den Nutzer schickt, so zu gestalten, dass aus ihr der Empfänger nicht hervorgeht. Durch die Wahl der Alternative kann sie davon ausgehen, dass der Nutzer auch damit einverstanden ist, dass eine an ihn gerichtete E-Mail personenbezogene Daten enthält, er also namentlich angesprochen wird. Die Möglichkeit der Kenntnisnahme durch den Provider kann der Nutzer mit der Wahl des Postversandes gleichwertig umgehen.

Der Datenverarbeitung auf Einwilligungsgrundlage steht hier auch nicht der Vorbehalt des Gesetzes entgegen: Die Anschrift für elektronische Post tritt neben die Wohnanschrift als Anschrift für herkömmliche Post. Für die (zusätzliche) Verwendung der Anschrift für elektronische Post auf Einwilligungsgrundlage zur Aufgabenerfüllung bedarf es keiner zusätzlichen gesetzlichen Ermächtigung (Präzisierung zu 13/10.2.15 unter 4.3).

13.5 Datenaustausch zwischen Hochschule und Studentenwerk in BAföG- und Mietangelegenheiten

Mit einer Anfrage zur Zulässigkeit der Datenweitergabe seitens einer Hochschule an das zuständige Studentenwerk, konkret um die Übermittlung von Studentendaten in Miet- und BAföG-Angelegenheiten zwecks Überprüfung der Anspruchsvoraussetzungen bin ich ebenfalls befasst gewesen. Das SMWK hatte - so war mir mitgeteilt worden - eine solche Datenübermittlung für rechtens erklärt und diese auf § 14 Abs. 4 Satz 2 SächsHSG i. V. m. § 3 SächsDSG gestützt. Nun war man an meiner Rechtsauffassung hierzu interessiert.

Ich habe wie folgt geantwortet:

Juristisch müssen zwei Aspekte berücksichtigt werden: Zum einen muss das Studentenwerk in den genannten Fällen (BAföG, siehe nachfolgend unter 1., und Mietangelegenheiten, siehe unter 2.) befugt sein, die Daten der Studenten bei der Hochschule zu *erheben*, zum anderen muss die Hochschule befugt sein, die betreffenden Studentendaten an das Studentenwerk zu *übermitteln*. Beide Aspekte hängen natürlich miteinander zusammen, müssen jedoch rechtlich getrennt voneinander betrachtet werden.

1. In Angelegenheiten nach dem Bundesausbildungsförderungsgesetz ist das Studentenwerk als zuständige Stelle (§ 40 Abs. 2 BAföG, § 109 Abs. 5 SächsHSG) berechtigt, die zur Bearbeitung eines BAföG-Antrags erforderlichen Daten gemäß §§ 68 SGB I, 67 a SGB X zu erheben.

   Dabei ist das Studentenwerk unter den Voraussetzungen des § 67a Abs. 2 SGB X berechtigt, nicht nur gemäß Absatz 1 der Vorschrift beim Betroffenen selbst, sondern auch bei Dritten Daten zu erheben, soweit dieser wiederum zur Übermittlung an das Studentenwerk berechtigt ist.

   Eine solche, ausdrücklich normierte, Befugnis der Hochschule zur Übermittlung an das Studentenwerk ergibt sich aus § 47 BAföG. Die dort genannten Angaben (wegen des Grundsatzes des Vorbehalts des Gesetzes jedoch *nur* die dort genannten) darf das Studentenwerk ohne Mitwirkung des betroffenen Studenten bei der Hochschule abfragen, also erheben, und die Hochschule auch dann an das Studentenwerk übermitteln. Die in § 47 BAföG geregelte Auskunftspflicht stellt die entsprechende Übermittlungsbefugnis dar.

2. Hinsichtlich der Verarbeitung von Studentendaten betreffend die Überprüfung von Anspruchsvoraussetzungen in Mietsachen (wobei ich davon ausgegangen bin, dass es sich hierbei um die Entscheidung bezüglich der Zuteilung eines Wohnheimplatzes gehandelt hat) gilt:

   Eine entsprechende Datenerhebungsbefugnis des Studentenwerks (als für die Vergabe von Wohnheimplätzen zuständige Stelle gemäß der einschlägigen Benutzungsordnung für die Wohnheime des betreffenden Studentenwerks) ergibt sich aus § 14 Abs. 4 Satz 2 SächsHSG.

   Die - aus meiner Sicht allerdings alles andere als normenklare - Vorschrift lässt sich wohl mit Müh und Not dahingehend auslegen, dass das Studentenwerk berechtigt sein soll, die für die Erfüllung seiner Aufgaben nach dem Sächsischen Hochschulgesetz erforderlichen Daten verarbeiten, mithin also insbesondere auch erheben zu dürfen (zur Definition des Verarbeitens von Daten siehe § 3 Abs. 2 SächsDSG). Vor-

liegend handelt es sich um die Erfüllung einer Aufgabe nach § 109 Abs. 4 SächsHSG (Betrieb von Studentenwohnheimen).

Es verbleibt somit die Frage, ob eine entsprechende Datenübermittlungsbefugnis seitens der Hochschule besteht, im Rahmen eines solchen Verfahrens Daten - ohne Mitwirkung des Antragstellers - an das Studentenwerk zu übermitteln.

Eine solche Rechtsvorschrift ist mir derzeit nicht ersichtlich. Insbesondere ist die von Seiten des SMWK hierfür angeführte Regelung des § 14 Abs. 4 Satz 2 SächsHSG nicht einschlägig. Sie betrifft, wie bereits dargelegt, lediglich Datenverarbeitungsbefugnisse des Studentenwerks, jedoch nicht solche der Hochschule.

Die Hochschule betreffend müsste sich eine Datenverarbeitungsregelung aus § 14 Abs. 2 und 3 SächsHSG ergeben. Dies ist nicht der Fall, insbesondere umfasst der in § 14 Abs. 1 Satz 1 SächsHSG genannte und eindeutig abschließend normierte Aufgabenkatalog nicht die Mitwirkung der Hochschule betreffend Mietangelegenheiten seiner Studenten.

Das SMWK habe ich über meine abweichende Rechtsauffassung in Kenntnis gesetzt und gebeten mich wissen zu lassen, wenn es meine Rechtsauffassung nicht teilen sollte.

Eine Reaktion seitens des SMWK ist ausgeblieben.

13.6 Forschungsvorhaben „Privateigentümer von Mietwohnungen in Mehrfamilienhäusern“ des Instituts für Wohnen und Umwelt (IWU) im Auftrag einer Bundesbehörde

Im Rahmen eines im Auftrag des Bundes durchgeführten Forschungsvorhabens ist die Grundsteuerstelle einer sächsischen Großstadt durch das Bundesamt für Bauwesen und Raumordnung (Geschäftsbereich des BMVBS) gebeten worden, in dessen Auftrag gestaltete Fragebögen an Eigentümer von Wohn-Liegenschaften zu versenden; ausgefüllt sollten die Fragebögen dann von den Eigentümern an ein privatrechtlich organisiertes (Forschungs-)Institut in Hessen gesandt werden.

Zur Gewinnung einer zu befragenden Stichprobe, also der Bestimmung der Fragebogenempfänger, sollten bei der sächsischen Grundsteuerstelle Anschriften von Gebäuden, die der Stadt bereits vom Forschungsinstitut geliefert werden sollten, anhand von der Grundsteuerstelle einzugebender Angaben zu den betreffenden Wohngebäuden (tatsächliche und rechtliche Verhältnisse) mittels vom Forschungsinstitut zur Verfügung gestellter Software als zur Zielgruppe der Untersuchung gehörig ausgesucht werden. Dazu sollten dann die Anschriften der Liegenschaftseigentümer ermittelt werden, denen so-

dann durch die Grundsteuerstelle der Fragebogen mit der Bitte um anonyme Rücksendung, eben an das private Forschungsinstitut, übermittelt werden sollten.

Ich habe hierzu, nachdem mich der städtische Datenschutzbeauftragte eingeschaltet hatte, folgende rechtliche Bewertung abgegeben:

Es handelte sich um eine Verarbeitung personenbezogener Daten, genauer gesagt um eine *Nutzung* personenbezogener Daten: Offensichtlich ist dies bei der Verwendung der Wohnanschriften der Eigentümer zum Zwecke des Versandes an den Adressaten (auch wenn dies ohne Übermittlung an einen Dritten geschieht; explizit zur Adressmittlung Dammann in Simitis, BDSG, 6. Aufl. § 3 Rdnr. 154). Darüber hinaus würden aber auch die einzugebenden zusätzlichen Daten der Wohnliegenschaften, die für die Grundsteuerstelle Daten der ihr bekannten Eigentümer, also personenbezogen sind, durch Eingabe in das Auswahlprogramm genutzt.

Die Zulässigkeit der Verarbeitung dieser Daten richtet sich abschließend nach den Vorschriften der §§ 30 ff. AO i. V. m. § 4 Abs. 1 Nr. 1 SächsDSG, da die Daten Angaben über Verhältnisse einer Person darstellen, die in einem Steuerverwaltungsverfahren bekannt geworden sind. Das Steuergeheimnis schützt nach § 30 AO sowohl gegen die unbefugte Offenbarung als auch gegen die Verwertung, d. h. jegliche Nutzung zu Zwecken außerhalb des Besteuerungsverfahrens (dies folgt im Umkehrschluss aus der Erlaubnis des Verwendens nach § 31 Abs. 3 AO, so Drüen in Tipke/Kruse, AO § 30 Rdnr. 53).

Es kann dabei dahinstehen, ob den Regelungen des Steuergeheimnisses nach §§ 30 ff. AO ein genereller Anwendungsvorrang gegenüber den Datenschutzgesetzen des Bundes und der Länder zukommt (Urteil des BFH vom 8. Februar 1994, VII R 88/92, gefunden in juris, Rdnr. 14) oder diesen subsidiäre Bedeutung in durch die Abgabenordnung ungeregelten Bereichen zukommen soll (so Drüen in Tipke/Kruse, AO, § 30 Rdnr. 5 f. m. w. N.). Nach beiden Auffassungen sind jedoch die ausdrücklich normierten Verwendungs- und Offenbarungsbefugnisse nach den §§ 30 ff. AO als dem Sächsischen Datenschutzgesetz vorrangige und abschließende bereichsspezifische Regelungen anzusehen.

Ein Rückgriff auf die Forschungsklausel des § 36 Abs. 1 SächsDSG als Erlaubnisnorm scheidet aus diesen Gründen aus. Es ist davon auszugehen, dass die Abgabenordnung gewolltermaßen - im Unterschied zu vielen Spezialgesetzen - keine Vorschriften über die Datenverwendung zu Forschungsvorhaben enthält, was im Sinne einer Negativregelung zur diesbezüglichen Unanwendbarkeit des Landesdatenschutzgesetzes führt (vgl. zur Sperrwirkung für die Datenschutzgesetze infolge „absichtsvollen Regelungsverzichtes“ Beschluss des BFH vom 4. Juni 2003, VII B 138/01, gefunden in juris, Rdnr. 19).

Bei dem beabsichtigten Heraussuchen geeigneter Liegenschaften und der anschließenden Adressmittlung handelte es sich in datenschutzrechtlicher Hinsicht nach der Terminologie der Abgabenordnung um eine „*Verwendung*“ von Eigentümerdaten; für deren Zulässigkeit bedarf es einer ausdrücklichen gesetzlichen Erlaubnis.

Die Zulässigkeit der Verwendung von Grundsteuerdaten richtet sich nach § 31 Abs. 3 AO.

§ 31 Abs. 3 AO setzt voraus, dass die Nutzung der streitgegenständlichen Daten zur Erfüllung sonstiger öffentlicher Aufgaben erfolgt.

Eine solche, zur Sicherung des in § 30 AO normierten Steuergeheimnisses aufgrund des Grundsatzes des Vorbehalts des Gesetzes erforderliche gesetzlich zugewiesene Aufgabe des Bundesamtes für Bauwesen und Raumordnung ergibt sich meiner Auffassung nach aus dem Aufgabenkatalog des § 2 BABauRaumOG. Danach betreibt das Bundesamt für Bauwesen und Raumordnung zur Erledigung seiner Aufgaben nach Absatz 4 der Vorschrift auch wissenschaftliche Forschung auf den Gebieten der Raumordnung, des Städtebaus und des Wohnungswesens.

§ 31 Abs. 3 AO erlaubt jedoch nach seinem eindeutigen Wortlaut lediglich die Verwendung von *Namen* und *Anschriften* von Grundstückseigentümern, nicht aber diejenige weiterer Angaben zu Besteuerungsgrundlagen. D. h.: Eine darüber hinausgehende Nutzung weiterer Angaben zu den Grundstückseigentümern (zu den ihnen jeweils gehörenden Grundstücken) ist vom Umfang der Erlaubnis des § 31 Abs. 3 AO nicht umfasst (Albers in Hübschmann/Hepp/Spitaler, AO, § 31 Rdnr. 31; vgl. auch Drüen in Tipke/Kruse, AO, § 31 Rdnr. 9). Die beschriebene Nutzung der Liegenschafts-Anschriften („Gebäudeadressen“) sowie derjenigen sich auf die Liegenschaft beziehenden Daten, um deren zusätzliche „Angabe“, also Eingabe in das zur Verfügung gestellte Programm, das Forschungsinstitut bittet, wäre eine Nutzung von Daten, die über den Namen und die Anschrift der Grundstückseigentümer, also über das von § 31 Abs. 3 AO Erlaubte, hinausgingen.

Demnach wäre eine Teilnahme der Stadt (städtische Grundsteuerstelle) an der Untersuchung wegen Verstoßes gegen geltendes Datenschutzrecht (hier in Gestalt des Steuergeheimnisses) rechtswidrig gewesen.

In intensiver Abstimmung mit dem privaten Forschungsinstitut, das keinesfalls auf die Teilnahme der beiden sächsischen Großstädte an dem Vorhaben verzichten wollte, konnte dann aber doch noch eine Lösung gefunden werden: Dies ist dadurch geschehen, dass nunmehr im Adressmittlungsverfahren keinerlei Auswahl - und damit diesbezügliche Datennutzung - von Immobilien durch die Grundsteuerstellen erfolgen sollte; auf

das Aussortieren nicht-relevanter Immobilien durch die sächsischen Grundsteuerstellen sollte also verzichtet werden.

Damit entfiel der Rechtsverstoß. Denn (allein) die Nutzung der Anschrift der Immobilie („Gebäudeadresse“) durch die Grundsteuerstelle ist von § 31 Abs. 3 AO noch gedeckt (vgl. ausdrücklich Albers in Hübschmann/Hepp/Spitaler, AO, § 31 Rdnr. 31 mit Fn. 2; auch der Kommentierung von Drüen in Tipke/Kruse, AO, § 31 Rdnr. 9 lässt sich dies als Sinn des § 31 Abs. 3 AO entnehmen, weil die Kommentierung nämlich voraussetzt, dass im Falle der ersten Tatbestandsvariante des § 31 Abs. 3 AO, nämlich der *Verwaltung anderer Abgaben*, wie auch im zweiten Tatbestandsfall, der *Erfüllung sonstiger öffentlicher Aufgaben*, am Beispiel der Baubehörden nach Sinn und Zweck der Vorschrift die Nutzung der Gebäudeanschrift selbst vorausgesetzt ist, damit die Vorschrift einen praktischen Anwendungsbereich hat).

Gegen das geänderte Verfahren und nach Änderung einiger Formulierungen im Anschreiben an die Eigentümer habe ich keine datenschutzrechtlichen Einwände mehr geltend gemacht.

13.7 Datenschutzrechtliche Vorgaben für die Verwendung von Daten aus Zeitzeugen-Interviews in wissenschaftlichen Arbeiten

Der Dekan einer Fakultät einer sächsischen Universität hatte im Hinblick auf die Durchführung von Dissertationsvorhaben mit zeitgeschichtlicher Thematik datenschutzrechtliche Fragen, die sich so haben formulieren lassen:

(a) Sind Wiedergaben von Teilen (d. h. wörtliche Zitate) oder ist die Wiedergabe von Angaben aus Interviews mit Zeitzeugen einwilligungsabhängig, d. h. dürfen die betreffenden Zitate oder Angaben (ausdrücklich) einer mit Namen genannten Person zugeordnet werden oder dürfen sie eine aufgrund von im Leserkreis der Dissertation erwartbaren Zusatzwissens erkennbare Auskunfts-Person betreffen, sofern diese Person keine Einwilligung erklärt hat?

(b) Welche Einwilligungserfordernisse gelten hinsichtlich der Wiedergabe von Angaben der Interviewpartner über namentlich benannte oder aus anderen Gründen individualisierbare *Dritte*?

Mit folgenden rechtlichen Überlegungen habe ich versucht, der Fakultät, insoweit sie zuständige Verwaltungsstelle für die Durchführung von Dissertationsverfahren ist, hinreichende Leitlinien an die Hand zu geben:

(1) Zunächst zum rechtlichen Rahmen:

(1.1) Die nach Hochschulrecht für die Durchführung des Promotionsverfahrens zuständigen öffentlichen Stellen dürften eine Verantwortung dafür haben, dass ihnen vorgelegte wissenschaftlichen Arbeiten nicht durch ihre Weitergabe im weiteren Gang des Promotionsverfahrens und erst recht nicht nach dessen Abschluss durch die - tatsächlich stattfindende oder als dem Wissenschaftsbetrieb eigen zu unterstellende - Veröffentlichung des Textes der wissenschaftlichen Arbeit (als Übermittlung seines Inhaltes an einen unbegrenzten Empfängerkreis) zu Rechtsverletzungen durch rechtswidrige Verarbeitung personenbezogener Daten führen.

(1.2) Das bedeutet: Die mit der Durchführung des Promotionsverfahrens betrauten öffentlichen Stellen innerhalb der Hochschule haben eine sich aus öffentlichem Recht ergebende diesbezügliche Verantwortung, unmittelbar schon was die Verarbeitung der in der Dissertation genannte Personen betreffender Daten innerhalb des Promotionsverfahrens, aber auch mittelbar, was die spätere unter Privatrecht fallende Veröffentlichung der Dissertationsinhalte angeht.

(2) Zu Frage a:

(2.1) Die Wiedergabe von Interviewinhalten ist nur insoweit zulässig, als die Interviewten eingewilligt haben. In der Bereitschaft des betreffenden *Zeitzeugen*, ein Interview zu geben, wird man sicherlich, sofern nicht besondere Umstände dagegensprechen (z. B. Befragung nach strafbarem Handeln), das Einverständnis mit einer (personenbezogenen) *Aufzeichnung* (datenschutzrechtlich: Speicherung) des Interviewinhaltes sehen können, nicht jedoch ohne Weiteres ein Einverständnis damit, dass das Interview ganz oder teilweise in der wissenschaftlichen Arbeit auch personenbezogen, also unter Erkennbarkeit des Interviewten, wiedergegeben (datenschutzrechtlich: übermittelt) wird.

(2.2) Zumindest deswegen muss ein sich auf den gesamten Text des Interviews beziehendes schriftliches Einverständnis des Interviewten vorliegen, welches sich ausdrücklich auf die Veröffentlichung von Wiedergaben aus dem Interview bezieht.

(2.3) Die „Promotionsbehörde“, so kann man die betreffenden Stellen durchaus nennen, hat auch das Recht, sich von dem Doktoranden diese Einwilligungen nachweisen, d. h. vorlegen zu lassen. Dies nicht nur, um eigene Verantwortung für Rechtsverletzungen zu vermeiden, sondern meiner Auffassung nach auch deswegen, weil die auch rechtlich ordnungsgemäße Gewinnung der Daten, aus denen die wissenschaftlichen Aussagen der wissenschaftlichen Arbeit gewonnen werden, Bestandteil der wissenschaftlichen Leistung sind, zu deren Beurteilung die das Promotionsverfahren durchführende Stelle berufen ist (es handelt sich, wenn man so will, um juristische Labor-Bedingungen, die vom Prüfling auf Verlangen nachzuweisen sind).

(2.4) Die Veröffentlichung von Daten, die für die wissenschaftliche Aussage und deren Nachprüfbarkeit *innerhalb des veröffentlichten Textes* nicht erforderlich sind, also Namen von Interviewten, auf deren Identität es wissenschaftlich nicht ankommt, oder aber auch solcher zusätzlichen Angaben (zu zwar aus wissenschaftlichen Gründen individualisierbar zu nennenden Zeitzeugen), die aber für das wissenschaftliche Ergebnis nicht von Bedeutung sind, wie etwa Anschriften der betreffenden Personen, mag rechtswirksam Gegenstand einer - sich explizit darauf beziehenden! - Einwilligung sein können; ihre Veröffentlichung hielte ich gleichwohl jedoch für eine Fehlleistung in wissenschaftlicher Hinsicht.

(Selbstverständlich gilt für die Unterlagen, in denen die Rohdaten gespeichert werden und die möglicherweise für wissenschaftliche Kontrolluntersuchungen anderen Wissenschaftlern - außerhalb von Veröffentlichungen - zur Verfügung zu stellen sind, anderes.)

(3) Zu Frage b:

Äußert sich ein Interviewter - und dies dürfte vermutlich immer ein namentlich genannter Interviewter sein - in der wiedergegebenen Äußerung über einen individualisierbaren Dritten, so handelt es sich primär um eine Angabe über den Interviewten, nämlich diejenige, dass er über den betreffenden Dritten das Wiedergegebene ausgesagt habe.

Die Verantwortung für diese Äußerung des Interviewten über einen Dritten trägt primär der Interviewte.

Sofern der den Interviewinhalt insofern wiedergebende Verfasser der wissenschaftlichen Arbeit sich eindeutig davon fernhält, sich die Äußerung des Interviewten über den Dritten im Kontext der Wiedergabe zu eigen zu machen („relata refero“), trifft meiner Auffassung nach die das Dissertationsvorhaben durchführende Stelle keine datenschutzrechtliche Verantwortlichkeit gegenüber dem Dritten, sofern die Einwilligung des Interviewten hinreichend eindeutig auch diesen Teil des Interviews umfasst und außerdem die individualisierbare Nennung des betreffenden Dritten dem Forschungszweck dient.

Denn es kann als Leitlinie dienen, was § 10 Abs. 4 Satz 2, 2. HS SächsArchivG für die Benutzung personenbezogenen Archivgutes für die Zwecke von Forschungsvorhaben bestimmt, nämlich: „*Soweit der Forschungszweck dies zulässt, sind die Forschungsergebnisse ohne personenbezogene Angaben aus dem Archivgut zu veröffentlichen.*“

Die Reaktion des Dekans hat erkennen lassen, dass diese Leitlinien dem betreffenden Promotionsausschuss als einleuchtend und brauchbar erschienen sind.

13.8 Verarbeitungsbefugnisse behördlicher Datenschutzbeauftragter

Ein Internet-Portal, welches die Bewertung von Hochschullehrern zum Gegenstand hat, hatte es sich, möglicherweise um datenschutzrechtlich weniger angreifbar zu sein, zur Aufgabe gemacht, die von ihm erfassten Lehrkräfte über die von ihm diese betreffend verarbeiteten Daten dadurch zu unterrichten, dass es diese Daten jeweils dem behördlichen Datenschutzbeauftragten der betreffenden Hochschule übermittelte, damit dieser die Daten an die jeweilige Lehrkraft weitergeben sollte. Dies sollte angeblich „aus Gründen des Datenschutzes“ geschehen, aber auch zu dem Zweck, die Daten, insbesondere hinsichtlich der „elektronischen Erreichbarkeit“ der einzelnen Dozenten, zu aktualisieren; diese Verfahrensweise sei mit der für das Bewertungsportal örtlich zuständigen Aufsichtsbehörde (§ 38 BDSG) abgesprochen.

Ein aufmerksamer Datenschutzbeauftragter einer sächsischen Hochschule hat sich an diese Absprache des Bewertungsportals mit dessen Aufsichtbehörde nicht gebunden gesehen, dem Portal gegenüber Zweifel an der Rechtmäßigkeit von dessen Verarbeitungshandeln geäußert und mich vorsichtshalber nachrichtlich unterrichtet.

Ich habe umgehend die Datenschutzbeauftragten der staatlichen Hochschulen im Freistaat Sachsen gebeten, für den Fall, dass sie eine solche Zusendung vom Bewertungsportal erhalten hätten, die Daten nicht an die einzelnen Dozenten weiterzuleiten, sondern zu sperren und dies dem Portal mitzuteilen.

Die Begründung für dieses Verlangen, dem Wunsch des Bewertungsportals, den an der Hochschule tätigen Lehrkräften die vom Bewertungsportal als von ihm über diese verarbeitet übermittelten Daten zu Unterrichtungszwecken weiterzugeben, nicht zu entsprechen, habe ich dann nachgeliefert:

Die Aufgaben und Befugnisse der behördlichen Datenschutzbeauftragten sächsischer Hochschulen richten sich, sieht man von ihrer allgemeinen Rechtsstellung nach Absatz 3 der Vorschrift ab, nach § 11 Abs. 4 SächsDSG, modifiziert in § 36 Abs. 6 Satz 2 und 3 SächsDSG. Der Aufgabenkatalog ist abschließend.

Die vom Bewertungsportal gewünschte Tätigkeit des Hochschul-Datenschutzbeauftragten fiel offenkundig unter keine der im Gesetz genannten Aufgaben, insbesondere auch nicht unter die allgemeine Aufgaben-Formulierung des Absatzes 4 Satz 1 der Vorschrift, wonach *der Datenschutzbeauftragte die Aufgabe hat, die öffentliche Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen*. (Unterstützen sollte er ja gerade das Bewertungsportal, nicht etwa seine Hochschule als öffentliche Stelle.)

Mangels entsprechender Aufgabe wäre es ein *Datenschutzverstoß* gewesen, wenn der (behördliche) Datenschutzbeauftragte der Hochschule den Wunsch des Bewertungsportals erfüllt hätte. Denn die gewünschte Tätigkeit hätte in der Verarbeitung personenbezogener Daten bestanden (nämlich jeweils des Datums, dass über den betreffenden Dozenten im Bewertungsportal die genannten Daten gespeichert und zur Einsichtnahme im Internet bereitgehalten wurden). Es mag sein, dass die betreffenden Daten allgemein zugänglichen Quellen zu entnehmen waren; dies hätte am Fehlen der Verarbeitungsbefugnis jedoch nichts geändert (arg. § 12 Abs. 2 Satz 1, Abs. 3 SächsDSG; dies dürfte in anderen Bundesländern nach dortigem Datenschutzrecht nicht anders sein).

Der behördliche Datenschutzbeauftragte (einer Hochschule) ist eben nicht „Freund und Helfer“ in allen datenschutzrechtlichen Lebenslagen für Hochschulbedienstete; vielmehr übt er ein Amt mit bestimmten Aufgaben und daran anknüpfenden Befugnissen namentlich auch zur Verarbeitung personenbezogener Daten aus.

Diese Befugnis kann auch nicht durch eine *Einwilligung* des Betroffenen (in derartigen Fällen könnte es sich um eine mutmaßliche Einwilligung handeln) erweitert werden: Kraft des verfassungsrechtlichen *Grundsatzes des Vorbehaltes des Gesetzes* (vgl. Art. 20 Abs. 3, 2. HS GG i. V. m. der Grundrechtsbindung, Art. 1 Abs. 3 GG, und dem Demokratieprinzip, Art. 20 Abs. 1 GG) dürfen Träger öffentlicher Gewalt nicht in größerem Maße ihnen im Gesetz nicht ausdrücklich zugewiesene Aufgaben mit Hilfe einer lediglich durch Einwilligung der Betroffenen gerechtfertigten Verarbeitung personenbezogener Daten an sich ziehen und erfüllen und dazu durch Verarbeitung personenbezogener Daten in Grundrechte eingreifen (vgl. 13/10.2.15 unter 4.3; bestätigt 14/10.2.17 unter [2];[inzwischen auch Menzel DuD 2008, 401]).

Ich habe daher die betreffenden Hochschul-Datenschutzbeauftragten gebeten, die ihnen vom Portal übermittelten Daten gemäß § 20 Abs. 1 Nr. 1 SächsDSG zu löschen, sofern dies noch nicht geschehen war.

Auch von der für das Bewertungsportal örtlich zuständigen Landesdatenschutzaufsichtsbehörde sind keine Einwände gegen meine Rechtsauffassung erhoben worden.

13.9 Gewinnung von Probanden mittels Adressmittlung: Erinnerungs-Möglichkeiten auch ohne Datenübermittlung

Im Hinblick auf das Vorhaben eines Soziologie-Lehrstuhles, Studenten aller sächsischen Hochschulen zu Studiensituation und Studienqualität im Freistaat Sachsen (zugleich zugunsten eines von der Staatsregierung geplanten „Hochschulberichtes“) zu befragen, ist von Forscherseite mir gegenüber geltend gemacht worden, dass es für die

wissenschaftlich erfolgreiche Durchführung des Forschungsvorhabens (im Sinne des § 36 Abs. 1 SächsDSG) erforderlich sei, dass die Namen und Anschriften der zu befragenden Stichproben-Angehörigen (samt Hochschule sowie Studienfach) seitens der Hochschulverwaltung *übermittelt* würden und man die Datenverwendung nicht auf die Durchführung des bloßen Adressmittlungsverfahrens durch die Hochschulverwaltung (sc. zugunsten der Forscher als Empfänger der Befragungs-Daten) beschränken dürfe. Das bedeutete konkret: Die Verwaltung der einzelnen Hochschule sollte nach Vorgaben der Forscher selbst (sc. nach Vorgaben von Forscher-Seite) aus ihren Studentendaten eine Stichprobe ziehen und dann die genannten Daten den Forschern übermitteln; unzulänglich wäre es nach Auffassung der Forscher gewesen, wenn die Hochschule stattdessen lediglich als Adressmittler tätig geworden wäre, also den Angehörigen der von ihnen gezogenen Stichprobe eine Nachricht hätte zukommen lassen, der die Einladung der Forscher zur Teilnahme an der Befragung beigefügt gewesen wäre.

Die Forscher haben für die von ihnen geltend gemachte wissenschaftliche Notwendigkeit der Datenübermittlung, die gegenüber der bloßen Datennutzung durch die Hochschule zugunsten der Forscher einen schwerwiegenderen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt, mir gegenüber Folgendes ins Feld geführt:

(1) Es ist Ergebnis der (empirischen) soziologischen Forschung betreffend soziologische Befragungen, dass eine zwei- bis dreifache Mahn- bzw. Erinnerungsaktion bei postalischen Befragungen die Rücklaufquote um 50 bis 60 v. H. der Erst-Antworter, also ganz beträchtlich, erhöht.

(2) Eine hypothetische Mahnung bzw. Erinnerung durch den Adressmittler - der ja über den Nicht-Rücklauf aus datenschutzrechtlichen Gründen in der Regel, und gerade im vorliegenden Fall, nicht unterrichtet werden soll - wäre wenig nützlich, weil bei der Verwendung von Fragebögen eine erneute Zusendung eines Fragebogens wegen der Notwendigkeit der Vermeidung von Doppel-Beantwortungen ausscheide, vielfach die erste Post mit dem Fragebogen jedoch beim Befragten nicht mehr vorhanden sei, wenn er erinnert bzw. gemahnt wird. Bei Online-Befragungen gelte Entsprechendes: Unerkennbare Mehrfach-Antworten ein und derselben Person werde dort durch die Übermittlung von Schlüssel-Zeichenfolgen für die Eingabeberechtigung vermieden - und das lasse sich im Adressmittlungsverfahren ohne die eben zu vermeidende Unterrichtung des Adressmittlers (im Beispielsfall: der Hochschulverwaltung) nicht bewerkstelligen.

(3) Als weniger überzeugend habe ich die Argumentation der Forscher beurteilt, dass das nach soziologischer Methodenlehre zur Steigerung der Antwortbereitschaft notwendige Maß an *personalisierender Ausgestaltung* (konkret: Anrede mit dem Namen) der schriftlichen Ansprache des Probanden durch den Forscher im Adressmittlungsver-

fahren nicht möglich sei. Ich habe argumentiert, dass das aus datenschutzrechtlichen Gründen ohnehin erforderliche eigene Anschreiben des Adressmittlers ja durchaus in diesem Sinne ‚persönlich' gehalten werden könne - womit sich die Behörde, als diejenige Stelle, welche über die Probandendaten verfügt, natürlich von sich aus[12] in der Praxis oft wenig Mühe geben wird - und dass sich diese Wirkung auch auf das Anschreiben des eigentlichen Daten-Interessenten (also des Forschers) übertragen werde.

(4) Gewichtig waren die Argumente der Forscher insoweit, als sie Beispiele aus der soziologischen Literatur vorgelegt haben, die belegen, dass die Nicht-Antworter bei einer Befragung die *Stichprobe* gewissermaßen sachlich *verzerren* (in der englischsprachigen Fachliteratur „nonresponse bias"). Konkreter: Es reicht nicht aus, einfach die Roh-Stichprobe zu erhöhen, um bei einer geringeren Rücklaufquote am Ende eine genügend hohe Netto-Stichprobe von Antwortern zu haben. Vielmehr ist es so, dass die Nicht-Antworter bestimmte für die Fragestellungen der Befragung relevante Eigenschaften (auch: Auffassungen oder Einstellungen) haben, die sich von denjenigen der Antworter unterscheiden, was zur Folge hat, dass die Ergebnisse aus der Netto-Stichprobe (Antworter) nicht repräsentativ und somit unzutreffend und irreführend sind, mithin einen statistischen Fehler aufweisen, der nur sehr eingeschränkt zuverlässig herausgerechnet werden kann, weil man nicht von vornherein alle auf die Antwortbereitschaft einwirkenden jeweils befragungsthemarelevanten Einflussgrößen quantitativ zutreffend kennt. Dieser Effekt wird eben durch die Wirkung zwei- bis dreifacher Mahnung oder Erinnerung stark vermindert, d. h. das wissenschaftliche Ergebnis wird entsprechend stark verbessert.

Im Jahre 2005 habe ich mich, nach Studium der mir von den Forschern zur Verfügung gestellten soziologischen Literatur, diesen Argumenten (vor allem K.-H. Reuband, Möglichkeiten und Probleme des Einsatzes postalischer Befragungen, Kölner Zeitschrift für Soziologie und Sozialpsychologie 2001, 307 bis 333, namentlich 319 bis 325; ferner etwa Dillman Mail and Internet Surveys. The Tailored Design Method, New York 2000, 149 ff.) nicht verschlossen und keine datenschutzrechtlichen Einwände dagegen geltend gemacht, wenn für das Forschungsvorhaben „Hochschulbericht Sachsen" im Jahre 2005 die Verwaltungen sächsischer Hochschulen den Forschern die Namen, Anschriften und auch die studierten Fächer von (sc. stichprobenangehörigen) Studenten sächsischer Hochschulen übermittelten, statt lediglich als Adressmittler tätig zu werden.

Ich habe seinerzeit aber schon darauf hingewiesen, dass ich nach Ende der damals mit dem SMWK und der Forschergruppe geführten Verhandlungen durch Hinweis von technischer Seite zu einer neuen Erkenntnis gekommen sei, die für künftige, gleich-

[12] Den Text des Anschreibens können aber selbstverständlich die Forscher ausarbeiten und, als Vorschlag, der Behörde zur Verfügung stellen.

artige Vorhaben die Beschränkung auf das Adressmittlungsverfahren als geboten erscheinen lasse: Es gibt, soweit ersichtlich, zumindest für Online-Befragungen wie im vorliegenden Fall nämlich die Möglichkeit, dass die Probanden durchaus auch im Wege der Adressmittlung, also vonseiten der Hochschulverwaltung selbst, wiederholt angeschrieben und bedingt („Für den Fall, dass Sie bisher nicht geantwortet haben, bitten wir/die Forscher Sie …“) erinnert werden können und dass dieser Erinnerung die vorher von der Hochschulverwaltung dem betreffenden Probanden individuell (aus dem von den Forschern zur Verfügung gestellten diesbezüglichen Kontingent an derartigen Zeichenfolgen) zugeordnete Kennung (Schlüssel-Zeichenfolge) für die Eingabeberechtigung bei der Online-Befragung erneut mitgeteilt wird (oder auch eine Staffelung der Schlüssel-Zeichenfolge vorgenommen wird, dergestalt, dass die für jeden Probanden vorgesehenen drei Eingabeberechtigungs-Kennungen so voneinander abhängig sind, dass die nachrangige nur dann tatsächlich zur Eingabe der Daten berechtigt, wenn nicht von der vorrangigen schon Gebrauch gemacht worden ist).

Kurz: Auf diese Weise lassen sich (bedingte) Erinnerung und Schutz vor unberechtigter Mehrfach-Eingabe auch innerhalb des bloßen Adressmittlungsverfahrens miteinander verbinden.

Es kann nicht zweifelhaft sein, dass sich eine solche Verfahrensweise in derartige Software einbauen lässt.

Ich habe seinerzeit keinen Grund zu Zweifeln an der Angabe gehabt, dass das Programm, dessen Nutzung sich die Forscher bereits vertraglich gesichert hatten, damals diese Möglichkeit nicht aufgewiesen hat und dass den Forschern auch kein anderes Programm bekannt gewesen ist, welche die oben genannte Möglichkeit bot. Angesichts des Umstandes, dass das Forschungsvorhaben in einem sehr engen Zusammenhang zu demjenigen Zweck bestanden hat, zu dem die von den Forschern gewünschten Daten seitens der Hochschulverwaltung erhoben und gespeichert worden waren, habe ich meine verbliebenen restlichen Bedenken gegen die Erforderlichkeit der *Datenübermittlung* und somit meine Zweifel daran, dass der Vorteil, den die Übermittlung für die Erreichung des Forschungszweckes darstellen würde, höheres Gewicht habe als die durch die Übermittlung im Unterschied zur bloßen Adressmittlung zusätzlich eintretende Grundrechtsbeeinträchtigung, zurückgestellt. Ich habe die Forscher jedoch darauf hingewiesen, dass sich aufgrund dieser ‚technischen’ Möglichkeit abzeichne, dass in Zukunft angesichts der Möglichkeit, eine Online-Befragung im Wege des Adressmittlungsverfahrens unter Einbeziehung der Mitteilung der individuellen Kennungen (Eingabeberechtigungs-Zeichenfolgen) durch den Adressmittler durchzuführen, die diesem eben vorher kontingentweise durch die Forscher zur Verfügung gestellt worden sind, auch die methodologischen Erkenntnisse der Umfrageforschung zur *Stichproben-Ver-*

zerrung durch *Nicht-Antworter* eine Datenübermittlung - statt der bloßen Adressmittlung - *nicht erforderlich* machen.

Ich habe daher der Forschergruppe geraten, im Hinblick auf künftige Vorhaben einschlägige Softwareentwickler auf dieses Desiderat aufmerksam zu machen.

Nunmehr ist man wegen einer Neuauflage einer solchen Befragung wieder mit der Bitte um Einverständnis mit der Datenübermittlung durch die Hochschulen an die betreffenden Forscher an mich herangetreten. Ich habe demgegenüber auf die oben dargelegte Möglichkeit einer forschungsunschädlichen Beschränkung auf das Adressmittlungsverfahren hingewiesen und bin auf die Reaktion gespannt. Ich gehe davon aus, dass die Datenschutzbeauftragten des Bundes und der Länder meine Auffassung teilen werden.

(Auch für herkömmliche postalische Befragungen lässt sich eine derartige Lösung finden: Wenn der Adressmittler dem Stichprobenangehörigen einen Fragebogen mit spezieller Kennung zuordnet, kann er den Erinnerungen jeweils einen papierenen Fragebogen mit je nach Erinnerungsstufe verschiedener Farbe beifügen. Dann können die Forscher, auch wenn sie die Fragebögen maschinell einlesen, Mehrfach-Beantwortungen erkennen und ausscheiden.)

14 Technischer und organisatorischer Datenschutz

14.1 Neue Musterdienstvereinbarung zur privaten Internetnutzung und Überarbeitung der Musterdienstvereinbarung zur Internetnutzung

Aufgrund zahlreicher Nachfragen von Personalräten aus den Behörden habe ich eine Musterdienstvereinbarung zur datenschutzgerechten Ausgestaltung der privaten Internetnutzung durch Mitarbeiter von Behörden erarbeitet. Die Musterdienstvereinbarung zur Internetnutzung (ohne Gestattung der privaten Nutzung) wurde dabei ebenfalls um Praxisfälle ergänzt und überarbeitet. Ziel beider Musterdienstvereinbarungen ist die Schaffung von transparenten Regelungen, die für klare Verhältnisse sorgen sollen.

Die beiden Musterdienstvereinbarungen unterscheiden sich hinsichtlich der Befugnisse des Dienstherrn deutlich. Wenn er den Bediensteten das Recht zubilligt, die dienstliche Infrastruktur privat zu nutzen, ist er auch zur Zurückhaltung bei der Kontrolle dieser der Privatsphäre zugehörigen Aktivitäten verpflichtet. Auch wenn dies dem einen oder anderen Leiter nicht schmecken mag, hier gilt, dass Vertrauen in die eigenen Mitarbeiter erbracht werden muss. Die Ausübung der informationellen Selbstbestimmung wäre sonst nicht gewährleistet. Dennoch werden natürlich auch die Interessen der Dienststellen gewahrt, Kontrollen sind weiterhin möglich. Allerdings geschieht dies zuerst ohne Personenbezug, dieser kann erst hergestellt werden, wenn die Internetnutzung über längere Zeit nicht im Sinne der Dienstvereinbarung erfolgt. Zudem erfolgen sämtliche Kontrollen unter Einbeziehung der Personalvertretung und ggf. des Datenschutzbeauftragten. Weiterhin ist für die Dienststellen zu beachten, dass beim Zulassen der Privatnutzung zahlreiche neue Nutzungsformen des Internets, welche bei rein dienstlicher Nutzung in aller Regel verboten sind, legalisiert werden können, beispielsweise soziale Netze, Online-Banking, Online-Shopping, etc. Es sollte im Vorfeld überlegt werden, welche Nutzungsformen erlaubt werden und welche nicht und dies klar in der Dienstvereinbarung geregelt werden. Die Musterdienstvereinbarung für die dienstliche Nutzung wurde um Kommentare ergänzt und stärker praxisorientiert ausgerichtet.

Beide Musterdienstvereinbarungen finden sich auf meiner Internetseite zum Herunterladen.

14.2 Nutzung der dienstlichen E-Mail für private Zwecke

Oft werde ich mit der Frage konfrontiert, inwieweit die dienstliche E-Mail auch für private Zwecke genutzt werden darf. Oft wird diese Frage von Personalräten gestellt, die dies im Rahmen einer geregelten privaten Internetnutzung für die Behördenmitarbeiter

in geringem Umfang gestatten wollen. Ich kann davon jedoch nur abraten. Dies hat zum einen rechtliche, zum anderen sachliche Gründe. Rechtlich ist die öffentliche Stelle bei der Zulassung einer solchen - auch eingeschränkten - Nutzung an das im Telekommunikationsgesetz verankerte Telekommunikationsgeheimnis verpflichtet, welches die Kenntnisnahme der privat stattfindenden Kommunikation stark einschränkt.

Gestattet die öffentliche Stelle die private Nutzung des dienstlichen E-Mail-Zugangs, ist sie geschäftsmäßiger Anbieter von Telekommunikationsdiensten, da sie den Internetzugang für fremde Zwecke zur Verfügung stellt (§ 3 Nr. 6 TKG). Dies hat zur Folge, dass die öffentliche Stelle den Verpflichtungen des Telekommunikationsgesetzes zum Schutz des Fernmeldegeheimnisses (§ 88 TKG) unterliegt. Demnach werden alle Inhalts- und Verbindungsdaten, die Auskunft über die am E-Mail-Austausch Beteiligten geben könnten, vor der Preisgabe geschützt. Weiterhin ist der Einsatz von zentralen SPAM-Filtern rechtlich problematisch wegen des Straftatbestandes der Nachrichtenunterdrückung (§ 206 Abs. 2 StGB).

Sachlich ist die private Nutzung der dienstlichen E-Mail-Adresse ebenfalls kritisch zu bewerten. Anhand der Absenderadresse tritt hier eine Privatperson gegenüber einem Dritten mit dem Attribut der öffentlichen Stelle in der E-Mail-Adresse auf. Dies ist vergleichbar mit der Nutzung des Briefkopfs der öffentlichen Stelle für private Korrespondenz.

Alternativ können die Beschäftigten auf Webmail-Dienste im Rahmen einer gestatteten privaten Internetnutzung zurückgreifen. Soll das Internet auch für private Zwecke genutzt werden dürfen, sollte eine Dienstvereinbarung auf Grundlage der gültigen „Musterdienstvereinbarung zur Ausgestaltung der Internetnutzung mit Erlaubnis der privaten Internetnutzung“ erstellt werden.

Den Eingang privater E-Mails kann der Empfänger nicht ausschließen, insbesondere dann nicht, wenn die E-Mail-Adresse in Webauftritten veröffentlicht ist. Neben einem Verbot des Sendens privater E-Mail-Nachrichten über das dienstliche Postfach, sollte den Beschäftigten empfohlen werden, empfangene private E-Mails unverzüglich nach Kenntnis des privaten Inhaltes zu löschen.

14.3 Administrativer Zugriff auf Postfächer von Bediensteten bei deren Abwesenheit

Ein Personalratsmitglied einer Landesbehörde hat mir einen Vorfall geschildert, bei dem zur Aufrechterhaltung des Dienstbetriebes der administrative Zugriff auf ein Postfach eines Bediensteten bei dessen Abwesenheit für den Vorgesetzten eröffnet wurde.

Dies erfolgte „auf Zuruf“ durch einen der Systemadministratoren. Der betroffene Bedienstete wurde nicht informiert und wurde erst nach seiner Rückkehr in den Dienst durch Auffälligkeiten in seinem Outlook-Postfach auf den Vorfall aufmerksam, da E-Mails, die er noch nicht geöffnet hatte, bereits als gelesen markiert waren. In der Dienststelle ist die Nutzung des E-Mail-Systems ausschließlich zu dienstlichen Zwecken gestattet, insofern ist der Fall anders gelagert als der in 13/5.1.6 geschilderte.

Auch wenn der Zugriff des Arbeitgebers auf dienstliche Dokumente im Interesse eines geregelten Dienstbetriebes ermöglicht werden muss, kann ein solcher Zugriff nicht schrankenlos gewährt werden. Der Grundsatz der Erforderlichkeit besteht immer; Transparenz und Nachvollziehbarkeit des behördlichen Handelns müssen ebenso wie schutzwürdige Interessen der Bediensteten gewahrt werden. Es ist weiterhin auszuschließen, dass ein solcher Zugriff der Verhaltens- und Leistungskontrolle dient. Schutzwürdige Interessen der Bediensteten können sich auch aus dem Empfang privater E-Mails, worauf der Bedienstete unter Umständen gar keine Möglichkeit der Einflussnahme hat, ergeben. Dies ist insbesondere dann der Fall, wenn durch ein hohes Maß an Außenkommunikation die E-Mail-Adressen öffentlich zugänglich sind.

Die von der Behördenleitung vertretene Position, dass ein Zugriff auf das E-Mail-System in Abwesenheit erfolgen kann, ist - bei einer ausschließlich dienstlich erlaubten E-Mail-Nutzung - vom Direktionsrecht des Arbeitgebers gedeckt. Keinesfalls darf ein solcher Zugriff jedoch dauerhaft und undokumentiert erfolgen.

Insbesondere sind die Erforderlichkeit des Zugriffs, die beteiligten Personen und die Dateien, auf die Zugriff gewährt wurde, schriftlich festzuhalten. Der Zugriff sollte durch den Leiter der Informationstechnik autorisiert werden. Der unmittelbare Zugriff sollte im Vier-Augen-Prinzip im Beisein eines Administrators, welcher auch für die Dokumentation verantwortlich ist, erfolgen. Nach Beendigung des Zugriffs ist das Passwort des betroffenen Bediensteten zurückzusetzen, das neue Passwort ist ihm nach Rückkehr im verschlossenen Umschlag zu übergeben. Ebenso ist er über Art und Umstand des Zugriffs zu informieren.

Ich empfehle die Prüfung, ob solche Zugriffe, die stets mit einer Verletzung schutzwürdiger Interessen der Bediensteten verbunden sein können, durch technisch-organisatorische Regelungen auf ein Minimum beschränkt werden können. Sinnvoll ist ggf. die Nutzung von Funktionspostfächern auf Sachgebiets- oder Referatsebene, auf die mehrere Bedienstete Zugriff haben oder die verstärkte Nutzung einer zentralen E-Mail-Poststelle.

Diese Grundsätze sollten in einer Dienstvereinbarung enthalten sein. Einen entsprechenden Entwurf einer Dienstvereinbarung zur E-Mail-Nutzung werde ich in meinem Internetangebot zur Verfügung stellen.

14.4 De-Mail: Erforderlicher Dienst oder Schaffung von Rechtsunsicherheiten

Ein althergebrachter Brauch beim Trinken ist das Anstoßen mit den Gläsern. Der ursprüngliche Sinn war jedoch nicht die Überprüfung der Klangeigenschaften der Trinkgefäße. Vielmehr versicherte man sich im Mittelalter durch das Überschwappen beim Anstoßen, dass man vom Gegenüber keinen vergifteten Wein eingeschenkt bekam. Heute in einer technisierten Umwelt ändern sich die Verfahren. Das Ziel der Herstellung gegenseitigen Vertrauens besteht aber noch immer. Ob dies allerdings immer so gut gelingt, dass das Verfahren über Jahrhunderte hinweg angewandt wird, ist fraglich.

Am 24. Februar 2010 hat der Bundestag das „Gesetz zur Regelung von De-Mail-Diensten“ verabschiedet. Mit den De-Mail-Diensten will die Bundesregierung eine zuverlässige und geschützte Kommunikationsinfrastruktur einführen, die die Vorteile der konventionellen E-Mail mit Sicherheit und Datenschutz verbinden soll. Die Bedenken von Daten- und Verbraucherschützern wurden dabei allerdings nicht vollständig berücksichtigt, so dass derzeit nur wenige Vorteile für den diese Dienste nutzenden Bürger zu erkennen sind.

Die De-Mail bietet nach derzeitigem Erkenntnisstand keine durchgängige Verschlüsselung (Ende-zu-Ende-Verschlüsselung). Zur Überprüfung auf Viren und andere Schadsoftware werden De-Mails in den Rechenzentren der Anbieter von De-Mail-Diensten kurzzeitig entschlüsselt. Auch wenn die zentrale Überprüfung vom Ansatz her lobenswert ist, entstehen durch diese Verfahrensweise jedoch Angriffsmöglichkeiten für einen Missbrauch durch Dritte. Ebenso fehlt bislang ein Konzept für die einfache Einbindung von elektronischen Signaturen zur Sicherstellung der Integrität von Schriftstücken. Durch diese fehlende Funktion verbleibt deren Realisierung wie bisher alleinig beim Bürger, was den zu erwartenden Mehrwert der De-Mail-Dienste erheblich verringert.

Die Nutzung eines De-Mail-Dienstes ist für den Bürger mit gesteigerten Sorgfaltspflichten bei der Postfachnutzung verbunden. Durch das Öffnen des Postfachs erhält der Sender eine Nachricht des Providers über die Zustellung. Behördliche Fristen beginnen dann zu laufen und eine Beweislastumkehr zu Ungunsten des Bürgers tritt in Kraft. Fraglich ist zudem, wie der Diensteanbieter den gesetzlich vorgesehenen Jugend- und Verbraucherschutz sicherstellt, ohne gegen das Fernmeldegeheimnis zu verstoßen.

In der Online-Dokumentenablage des De-Mail-Kontos (in der öffentlichen Diskussion auch „Datensafe“ genannt) sollen Dokumente rechtssicher abgelegt werden können, eine technische Zugriffssicherheit ist jedoch nur durch von den Nutzern selbst zu erbringende Zusatzmaßnahmen (Verschlüsselung) erreichbar. Es ist fraglich, welche dauerhafte Nachhaltigkeit und Zuverlässigkeit der „Datensafe“ vor dem Hintergrund der im Gesetz getroffenen Regelungen zur möglichen Einstellung der Tätigkeit des Dienstanbieters entfalten kann.

Bürgern, die über kein De-Mail-Konto verfügen, dürfen nicht benachteiligt werden. Es ist sicherzustellen, dass staatliche Stellen bei E-Government-Anwendungen nur dort eine persönliche Identifizierung verlangen, wo dies für eine konkrete Dienstleistung auch tatsächlich erforderlich ist.

14.5 Einsatz der elektronischen Signatur in Behörden

Mit der Umsetzung der EU-Dienstleistungsrichtlinie (Richtlinie 2006/123/EG) wurden alle kommunalen sowie etliche staatliche Behörden des Freistaates Sachsen verpflichtet, die elektronische Kommunikation mit Bürgern rechtsverbindlich zu eröffnen. Dazu zählen der gesicherte elektronische Zugang von Dokumenten und die Möglichkeit, Dokumente mit einer qualifizierten elektronischen Signatur nach Signaturgesetz zu unterschreiben. Viele Stellen fühlen sich mit der rechtskonformen Einführung der Verfahren überfordert, zumal die beiden in Sachsen für die EU-Dienstleistungsrichtlinie zuständigen Staatsministerien bisher keine entsprechenden Arbeitshilfen bereitgestellt haben. Daher sollen an dieser Stelle einige grundlegende Anforderungen an den Einsatz der elektronischen Signatur in Behörden erläutert werden.

Die elektronische Signatur bildet die Unterschrift einer Person in einem elektronischen Verfahren ab. Der mit einer elektronischen Signatur Unterzeichnende kann eindeutig identifiziert und die Integrität des unterzeichneten Dokuments kann überprüft werden. Die elektronische Signatur erfüllt somit die Funktion der eigenhändigen Unterschrift auf einem Dokument. In Deutschland erfüllt nach § 2 Nr. 3 SigG lediglich die qualifizierte elektronische Signatur die Anforderungen an die elektronische Form gemäß § 126a BGB und ist damit der händischen Unterschrift gleichgestellt. Derzeit können nur natürliche Personen eine elektronische Signatur beantragen, welche sich bei der Beantragung bei einem Anbieter von elektronischen Signaturen (Trust-Center) vorab authentifizieren müssen. Die Signatur wird auf einer elektronischen Karte gespeichert, für den Signierprozess ist ein Kartenleser erforderlich.

Da davon auszugehen ist, dass die Einführung der elektronischen Signatur unter die Mitbestimmungstatbestände des § 81 SächsPersVG fällt, ist der Abschluss einer Dienst-

vereinbarung mit der jeweiligen Personalvertretung erforderlich. In dieser sind folgende Punkte zwingend zu regeln:

- Bezeichnung der Verfahren, bei denen die elektronische Signatur zum Einsatz kommen soll,
- Beschreibung des Antragsverfahrens und der zuständigen Stellen für Beschaffung und Betreuung der notwendigen Technik und für die Überwachung der Gültigkeit von Zertifikaten,
- Regelungen zu den aufzubringenden Attributen nach § 5 Abs. 2 SigG (Zugehörigkeit des Karteninhabers zur Dienststelle sowie dessen Amts- oder Dienstbezeichnung) sowie Regelungen, falls die Signaturkarte auch für die verschlüsselte E-Mail-Kommunikation genutzt werden soll und somit eine vorgesehene E-Mail-Adresse im Zertifikat einzutragen ist,
- Regelungen zur Sperrung der Signaturkarte und Festlegung der zuständigen Stelle für die Aufbewahrung des Sperrpasswortes, welches das Trustcenter zur Authentifizierung eines Sperrwunsches benötigt,
- Regelungen zur Nutzung der Signatur (ausschließlich für dienstliche Zwecke), zu Unterschriftsbefugnissen, zur Aufbewahrung der Signaturkarte, zur Sicherung der PIN, Maßnahmen bei Verlust,
- Regelungen zum Ein- und Ausgang und zur Verarbeitung und Speicherung von elektronisch signierten Dokumenten.

Es wird deutlich, dass viele Punkte bedacht werden wollen, wenn die elektronische Signatur sicher und rechtskonform in die behördliche Praxis eingeführt werden soll. Meine Behörde befindet sich derzeit in Abstimmung mit der SAKD, um eine Musterdienstvereinbarung für Kommunen zu erarbeiten. Sobald diese vorliegt, wird sie auf dem Internetauftritt meiner Behörde veröffentlicht.

14.6 Evaluierung des anderen sicheren Verfahrens nach § 87a Abs. 6 AO - ElsterOnline

Im Berichtszeitraum wurde ich durch den Vorsitzenden des Arbeitskreises „Technik“ der Datenschutzbeauftragten des Bundes und der Länder über die Evaluierung des „anderen sicheren Verfahrens ElsterOnline“ nach § 87a Abs. 6 AO unterrichtet.

Die Finanzverwaltung stellt für Bürger und Unternehmen zur Übermittlung der Steuerdaten (z. B. Steuererklärung) das elektronische Verfahren „ElsterOnline“ bereit. In § 87a Abs. 3 AO ist vorgesehen, dass die durch Gesetz angeordnete Schriftform für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden durch die elektronische

Form ersetzt werden kann. Das elektronische Dokument ist mit einer qualifizierten elektronischen Signatur (QES) nach dem Signaturgesetz zu versehen.

Mit der QES als Form der „elektronischen Unterschrift“, welche der eigenhändigen Unterschrift gesetzlich gleichgestellt ist, soll gesichert werden, dass eine Manipulation des Inhalts und der Urheberschaft des Dokuments erkannt und unbestreitbar festgestellt werden kann. Der Empfänger des Dokuments kann somit die Echtheit und Unversehrtheit des Dokuments prüfen.

Bislang besteht diese Möglichkeit, die Kommunikation mit der Finanzverwaltung mit einer QES abzusichern, noch nicht. Nach § 87a Abs. 6 AO kann das BMF neben der qualifizierten elektronischen Signatur bis zum 31. Dezember 2011 auch ein „anderes sicheres Verfahren“ zulassen, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Entsprechend des gesetzlichen Auftrags ist die Verwendung des anderen sicheren Verfahrens zu evaluieren.

Die Erwartung ist, dass im Rahmen der Evaluierung Aussagen zum erreichten Datenschutzniveau, Aussagen zu den Rechtsfolgen und eine rechtliche Abwägung beim Einsatz des „anderen sicheren Verfahrens“ im Vergleich zur Anwendung der QES gemacht werden. Auch unter Berücksichtigung der Veränderung der aktuellen Sicherheitsanforderungen und Bedrohungsaspekte seit 2007 ist ein Vergleich mit dem Verfahren der QES notwendig. Eine Differenzierung des erreichten Sicherheitsniveaus zwischen ELSTER-Basis, ELSTER-Plus und ELSTER-Spezial ist dabei zu berücksichtigen.

Die Evaluierung muss insbesondere die Fragen beinhalten, wie die Integrität und Authentizität der übermittelten elektronischen Steuerdokumente mit diesem „anderen sicheren Verfahren“ gewährleistet werden soll, ob das Verfahren zukünftig durch die QES abgelöst wird oder die Anwendung des „anderen sicheren Verfahrens“ über den 31. Dezember 2011 hinaus geplant ist.

Im Rahmen der Evaluierung dieses Verfahrens haben sich die Landesdatenschutzbeauftragten abgestimmt und dem BMF die zu berücksichtigenden Belange des Datenschutzes und der IT Sicherheit mitgeteilt[13].

14.7 Kontrolle eines Serverraumes

Meine Mitarbeiter stellten bei einer unangekündigten technischen Datenschutzkontrolle in einer Bildungseinrichtung fest, dass die technischen und organisatorischen Sicherheitsmaßnahmen nach § 9 SächsDSG zur Zutritts- und Zugangssicherung eines Server-

[13] Tätigkeitsbericht 2009/2010 des BfDI - 23. Tätigkeitsbericht - Deutscher Bundestag Drs. 17/5200, S. 40.

raumes nicht ausreichend umgesetzt waren. Darüber hinaus entsprach die Klimatisierung dieses Serverraums nicht mehr den technischen Anforderungen, so dass sofort Maßnahmen zur Sicherung dieses Raumes veranlasst werden mussten.

Vorgefunden wurde bei dieser Kontrolle ein unverschlossener Serverraum in einem öffentlich zugänglichen Hauptgebäude der kontrollierten Einrichtung. Dieser Serverraum hatte keine Fenster, die Tür zum Treppenhaus und die Fenster auf dem angrenzenden Gang standen dem Vernehmen nach bereits seit längerem zur besseren Belüftung offen. Zur Begründung wurde mir mitgeteilt, dass man seit mehreren Wochen eine erhöhte Wärmeentwicklung beobachte, die zunächst nicht erklärt werden konnte. Um Schaden von der Technik abwenden zu können, habe man die Türen praktisch öffnen müssen.

Als Übergangslösung wurde die Tür des offenstehenden Serverraumes teilweise durch ein Gitter abgesichert, welches von der Rückseite der Serverschränke abmontiert worden war und zufällig in die Türbreite der Eingangstür des Serverraumes passte. Jedoch wäre es ohne Probleme möglich gewesen, diese Absperrung zu überwinden, da derartige Serverschranktüren kein ernsthaftes Zutrittshemmnis darstellen und im konkreten Fall nicht einmal die komplette Türhöhe ausfüllen konnten.

Nachdem die Rückseiten der Serverschränke als „Behelfstür“ für den Gesamtraum zweckentfremdet wurden, war lediglich die Vorderseite dieser Serverschränke noch verschlossen. Damit hätten Unbefugte ohne nennenswerten Aufwand nach Überwindung der provisorischen Absperrung Änderungen an der Technik vornehmen oder die Hardware auch gleich ganz oder in Teilen entwenden können.

Positiv ist zu erwähnen, dass für diesen Raum als Zugangssicherungsmaßnahme ein Bewegungsmelder verbaut war, der nach Öffnen der Absperrung zum Serverraum eine E-Mail auf ein Administratorenkonto versendet hätte. Allerdings war der Besitzer des zugehörigen E-Mail-Kontos zum Kontrollzeitpunkt seit längerer Zeit abwesend und eine Vertreterregelung war nicht eingerichtet. Somit hätte auch niemand auf einen etwaigen Alarm reagieren können.

Nach Prüfung der Sachlage stellte sich heraus, dass die Klimatisierung ursprünglich nur für den Betrieb von zwei Servern dimensioniert war. Zum Zeitpunkt der Prüfung befanden sich jedoch weitere Server im Raum und zusätzlich eine umfangreiche Speichererweiterungseinheit im zweistelligen Terabyte-Bereich, die zusammengenommen für die erhöhte Wärmeentwicklung verantwortlich zu machen waren.

Serverräumen wird man im Allgemeinen schon deshalb eine besondere Schutzwürdigkeit zumessen, weil die installierten Hard- und Softwarekomponenten von erheblichem

materiellem Wert sind. Im vorliegenden Fall ging es jedoch auch um umfangreiche produktive Datenbestände der Einrichtung, für die auch ein hohes Maß an Verfügbarkeit gefordert wurde. Als weiterer und in besonderer Weise zu schützender „Unternehmenswert“ kam dann noch ein wertvolles digitales Archiv hinzu, dessen Datensicherung - wie auch die Sicherung der übrigen Daten - im gleichen Raum gelagert wurde. Damit wären im Havarie- oder Brandfall sowohl die produktiven Daten mit dem genannten Archiv als auch die gesamte Datensicherung verloren gegangen.

Ich habe die Leitung der Bildungseinrichtung auf diese Missstände hingewiesen und die sofortige Errichtung einer angemessenen Zugangssperre, die Erhöhung der Kühlleistung sowie die räumlich getrennte und brandsichere Aufbewahrung der Datensicherungen vereinbart.

Dieses Beispiel veranschaulicht gut die Bedeutung einer umfassenden technischen wie organisatorischen Analyse *vor* der Inbetriebnahme neuer Hard- und Software. Darüber hinaus sollte bei schutzbedürftigen Räumen generell ein Sicherheitskonzept erstellt werden. Eine gute Grundlage dazu bietet der Baustein M 1.58 „Technische und organisatorische Vorgaben für Serverräume“ der IT-Grundschutz-Kataloge des BSI.

14.8 Nutzung von Computer Telephony Integration (CTI)-Lösungen in Behörden

Sogenannte CTI-Lösungen verbinden die Daten von Telekommunikationsanlagen mit den Möglichkeiten der modernen Bürokommunikation. Beispielsweise können Anrufe vom Computer aus gestartet und entgegengenommen, Kontaktdaten können mit Telekommunikationsdaten verknüpft werden und ein Journal hält die geführten Anrufe fest bzw. informiert über entgangene Anrufe. Weiterhin ist es möglich, dass eine CTI-Lösung Präsenzinformationen (am Arbeitsplatz, in Besprechungen etc.) bereitstellen kann. Eine CTI-Lösung speichert also umfangreiche Verbindungsdaten sowohl abgehender als auch eingehender und nicht zustande gekommener Telefonate. Es wird deutlich, dass derartige Daten über das Maß der bislang im Zusammenhang mit Telefonanlagen gespeicherten Informationen weit hinausgehen und prinzipiell zu einer Überwachung von Mitarbeitern geeignet sind. Es ist daher zwingend erforderlich, vor der Einführung einer CTI-Lösung eine Vorabkontrolle durchzuführen und mit dem Personalrat eine entsprechende Dienstvereinbarung abzuschließen.

Probleme ergeben sich unter anderem daraus, dass CTI-Lösungen die Daten von eingehenden Anrufen speichern und diese in Kontaktdatenbanken o. Ä. weiter verarbeitet werden können. Bei einer erlaubten Privatnutzung der dienstlichen Telefonanlage sind davon auch Privatgespräche betroffen. Auch bei einem Verbot der privaten Nutzung der

Telefonie ist ein von außen eingehender Anruf privater Natur nicht zu verhindern. Das Fernmeldegeheimnis nach § 88 TKG kann also in jedem der beschriebenen Fälle einschlägig sein. Aufgrund der rechtlich sensiblen Thematik ist es daher wichtig, ein rechtliches Verwertungsverbot der CTI-Daten zur Leistungs- und Verhaltenskontrolle zu verankern und die Speicherdauer der Daten angemessen kurz zu gestalten. Da derartige Programme zur Unterstützung der laufenden Bürotätigkeit genutzt werden, erscheint mir eine Vorhaltung der Daten von bis zu sieben Tagen als angemessen. Darüber hinaus sind jedem Nutzer Löschrechte einzuräumen, mit denen einzelne Einträge oder die gesamte Telefonhistorie gelöscht werden können.

Einige der am Markt erhältlichen CTI-Lösungen bieten ein Leistungsmerkmal, dass die Nutzer sogenannte Präsenzinformationen im System hinterlegen (z. B. am Platz, im Gespräch etc.). Die Funktion ist auf Tätigkeiten zugeschnitten, wo die individuelle Verfügbarkeit von Mitarbeitern eine unmittelbare Rolle in der Organisation der Arbeit spielt. Ohne dies an dieser Stelle bewerten zu wollen, scheint mir fraglich, ob die Verfügbarkeit eines derartigen Leistungsmerkmals in einer Büroumgebung erforderlich ist. In jedem Falle ist ein rechtswirksamer und technisch untersetzter Ausschluss dieser Nutzungsmöglichkeiten in einer Dienstvereinbarung sowie der zugrunde liegenden technischen Umsetzungsdokumentation festzuschreiben.

An dieser Stelle möchte ich auch allgemein auf die Notwendigkeit hinweisen, dass vor dem Einsatz eines Standardprodukts alle möglichen Funktionen auf den konkreten Einsatz hin geprüft und ggf. wirksam unterbunden werden müssen. Eine bloße „Nicht-Nutzung“ einer derartigen Funktion ist dabei kein adäquates Mittel.

14.9 Leitlinie „Informationssicherheit“ des Freistaates Sachsen

Seit vielen Jahren wird von meiner Behörde auf die Notwendigkeit eines übergreifenden Informationssicherheitsmanagements hingewiesen. In Anbetracht einer immer stärker werdenden Abhängigkeit der Verwaltung von der Technik und der stetig zunehmenden Gefahren, die sich aus deren Nutzung ergeben, ist es wichtig und richtig, das Thema Informationssicherheit zur Chefsache zu erklären. Leider ist die Lage in den Behörden und Einrichtungen des Freistaates derzeit noch sehr inhomogen. Auf entsprechende Defizite hat der SRH bereits im Jahresbericht 2007 hingewiesen. Erfreulich war dann auch die Gründung einer ressortübergreifenden Arbeitsgruppe Informationssicherheit im Jahr 2008, bei der auch meine Behörde vertreten ist. Diese Arbeitsgruppe hat in kurzer Zeit eine umfassende Informationssicherheitsleitlinie erarbeitet und Mitte 2008 in einer abgestimmten Fassung vorgelegt. Dieses Dokument dient der Beschreibung eines ressortübergreifenden Informationssicherheitsmanagements, der dabei verfolgten Strategie und der beteiligten Gremien. Obwohl weitgehender Konsens über die Inhalte herrscht,

wurde diese Leitlinie erst nach dem Berichtszeitraum am 23. August 2011 durch das Kabinett in Kraft gesetzt. Dazwischen lag eine Umressortierung der für IT-Koordination zuständigen Abteilung vom SMI zum SMJus, etliche Abstimmungsschwierigkeiten mit bereits existierenden Gremien über Aufgabenzuschnitte und Zuständigkeiten und eine zeitintensive juristische Normprüfung. Das hat leider nicht zuletzt die Arbeit der wenigen bisher ernannten Informationssicherheitsbeauftragten erheblich erschwert. Die Leitlinie sieht nun vor, dass diesen Informationssicherheitsbeauftragten dauerhaft ein angemessener Anteil ihrer Arbeitszeit für die Erledigung der mit dem Informationssicherheitsmanagement verbundenen Aufgaben zur Verfügung steht. Dies ist eine sehr wesentliche Maßgabe, an deren Umsetzung sich die Ressorts und ihre Behörden in Sachsen werden messen lassen müssen. Ich werde diesen Prozess aufmerksam verfolgen.

14.10 Zugriffsstatistik für den Internetauftritt der Sächsischen Staatsregierung unter sachsen.de

Im letzten Tätigkeitsbericht habe ich zur datenschutzgerechten Gestaltung der Protokollierung von IP-Adressen in Webserver-Logfiles Stellung genommen und auf ein von meiner Behörde entwickeltes Programm zur Maskierung von IP-Adressen verwiesen. Das Programm wird mittlerweile in einer Vielzahl von Behörden eingesetzt, u. a. von der SK für den Internetauftritt der Sächsischen Staatsregierung unter sachsen.de. Da das Verfahren jedoch keine Auswertungsmöglichkeiten bezüglich der Webseitenaktivitäten von Besuchern vorhält, wollte die SK einen Tracking-Dienst mit der Auswertung und Analyse des Nutzungsverhaltens einsetzen.

Ich habe den von der SK vorgeschlagenen Tracking-Dienst anhand bereitgestellter Unterlagen und Aussagen datenschutzrechtlich geprüft. Unter Einhaltung der nachfolgend dargestellten Einstellungen ist eine datenschutzkonforme Besucheranalyse möglich. Die SK ist meinen Vorgaben gefolgt und betreibt den Dienst seit November 2010 aktiv auf www.sachsen.de und den eingebundenen Portalen der sächsischen Ressorts.

1. Verzicht auf die Verarbeitung der IP-Adressen von Besuchern

Nach einhelliger Auffassung der Datenschutzbehörden und einer Reihe einschlägiger Gerichtsurteile stellt die IP-Adresse ein personenbezogenes Datum dar. Auf eine Verarbeitung vollständiger IP-Adressen ist daher zu verzichten. Die Form der Kürzung um die letzten 8 Bit (entspricht dem letzten Block der IPv4-Adresse mit den möglichen Dezimalwerten 0 bis 255) bietet nach derzeitigem Stand der Technik eine hinreichende Form der Anonymisierung.

2. Datensparsame Erhebung von technischen Parametern

Diese durch die Kürzung der IP-Adresse hergestellte Anonymität wird durch das Erheben von weiteren nutzerspezifischen Attributen (Geo-Analyse, Betriebssystem- und Browserspezifikationen) jedoch untergraben. Daher ist eine Betrachtung der Erforderlichkeit der Erhebung der Daten notwendig. Sie hat sich auf die für eine technische Verbesserung des Angebotes signifikanten Daten zu beschränken.

3. Transparenz für Besucher und Einräumung eines Widerspruchsrechts gegen eine Datenerhebung

Die Besucher der Webseiten innerhalb der Domäne sachsen.de sind in geeigneter Form über den Einsatz des Webanalysewerkzeugs und transparent über Art und Umfang der erhobenen Daten zu informieren, ein aktives Widerspruchsrecht bezüglich der Datenerhebung, -verarbeitung und -speicherung ist einzurichten.

4. Abschluss eines Vertrages zur Auftragsdatenverarbeitung

Der Abschluss eines Vertrages zur Auftragsdatenverarbeitung zwischen dem Freistaat Sachsen und dem Tracking-Dienst ist zwingend erforderlich. § 15 TMG verbietet die personenbeziehbare Protokollierung des Nutzungsverhaltens, sofern diese nicht zur Abrechnung erforderlich ist. Da der Freistaat Sachsen als Betreiber der Webseite www.sachsen.de selbst keine Verarbeitung von Nutzerdaten vornimmt, sondern sich für diese Zwecke eines externen Dritten bedient, ist eine Übermittlung der IP-Adresse des Besuchers der Webseite an den Dritten technisch zwingend erforderlich. Zwar findet die Weiterverarbeitung der IP-Adresse nur verkürzt statt, die Übermittlung selbst ist nach Telemediengesetz jedoch gesetzlich nicht vorgesehen. Ein Abschluss eines Vertrages zur Auftragsdatenverarbeitung ist daher zwingend erforderlich. Bei der Datenverarbeitung im Auftrag verbleibt die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber. Die SK unterliegt als öffentliche Stelle im Freistaat Sachsen dem Sächsischen Datenschutzgesetz. Der beauftragte Dritte ist daher, neben den ohnehin geltenden bundesrechtlichen Vorschriften, im Auftragsverhältnis mit dem Freistaat Sachsen zur Einhaltung des Sächsischen Datenschutzgesetzes zu verpflichten.

14.11 E-Government

In den zurückliegenden Berichtszeiträumen hatte ich gegenüber der Staatsregierung regelmäßig meine Forderung nach einem E-Government-Gesetz wiederholt (vgl. 14/14.4, 13/1.6). Insofern besteht weiterhin Handlungsbedarf, insbesondere auch im Hinblick auf die Internetpräsenzen des Freistaates. Die Verwaltungsvorschrift Internet und LandesWeb konnte insofern nur ein erster Schritt sein.

In einem E-Government-Gesetz sollten
- Internetauftritte und deren Kommunikationsbestandteile,
- die E-Mail-Kommunikation zwischen Behörden und Bürgern und zwischen Behörden,
- die elektronische Aktenführung und
- verwaltungsübergreifende Verfahren

im Hinblick auf Zweck, Form, Inhalt und Datenverarbeitung umfassend und weitergehend geregelt werden.

Datenschutzrechtliche und -organisatorische Fragen ergeben sich u. a. zur Speicherung des Internet-Nutzerverhaltens, zur Frage, welche Daten zum Zwecke der Verbesserung der Kommunikation zwischen Bürger und Behörden im Internetauftritt zentral auf Vorrat gespeichert werden dürfen (und durch welche Stellen), zur Verfahrensweise und Datenverarbeitung beim Eingang und der Versendung von elektronischen Nachrichten, zur Bezahlung von Behördenleistungen über das Internet, zur Ausstattung von Mitarbeitern mit Signaturkarten, zur Eigenkontrolle der Behörden bei den Kommunikationsmitteln und neuartigen Verfahren und zu den einzuhaltenden technischen Mindeststandards. Zuständige Behörden wären im Gesetz zu benennen und festzulegen.

Ungeregelt geblieben ist bisher auch die weltweite Veröffentlichung des Sächsischen Amtsblattes über das Internet. Das Amtsblatt enthält z. T. auch personenbezogene Daten, so dass es für die Veröffentlichung einer normenklaren gesetzlichen Grundlage bedarf (§ 4 Abs. 1 SächsDSG). Auch macht es einen Unterschied, ob das Amtsblatt nur als Schriftgut oder über das Internet publiziert wird. Ich habe der Staatsregierung auch das Beispiel einer Betroffenen, deren Namen, Geburtsdaten und vollständige Adresse über das Amtsblatt wegen einer in Abwesenheit des Ehegatten erfolgten Ehescheidung vor Gericht im Amtsblatt bekanntgemacht wurden, mitgeteilt. Rückwirkend wurden die zurückliegenden Amtsblattausgaben aus den Jahren vor 2006 über das Internet veröffentlicht, so dass die Betroffene über Internetsuchmaschinen mit den Angaben leicht zu finden war und sich persönlichkeitsrechtlich beschwert fühlte. Dennoch ist mein Anliegen wohl bisher eher auf Desinteresse gestoßen. Verfahren wird jedenfalls weiterhin „per ordre du mufti“.

Der Staatsbetrieb Sächsische Informatik Dienste, dessen Aufgaben als zentraler IT-Dienstleister in einem E-Government-Gesetz hätte geregelt werden können, hat als funktionale Stelle im Sächsischen Verwaltungsorganisationsgesetz Berücksichtigung gefunden (vgl. § 10 Abs. 1 Nr. 2, Abs. 2 SächsVerwOrgG). Das ist positiv.

15 Vortrags- und Schulungstätigkeit

15.1 Rechtsreferendarsausbildung

Einen wesentlichen und zunehmend wichtigeren Tätigkeitsbereich sehe ich in den Schulungen, die meine Mitarbeiter in den bzw. für die öffentlichen Stellen des Freistaates Sachsen, den Kommunen, den Universitäten etc. durchführen. Datenschutzbewusstsein kann sich nur entwickeln und Datenschutzverstöße aus Unwissenheit können nur vermieden werden, wenn möglichst viele Bedienstete öffentlicher Stellen das erforderliche Wissen über das Recht auf informationelle Selbstbestimmung erwerben und in der Praxis auch anwenden können. Dementsprechend messe ich den internen und externen Schulungen großes Gewicht bei. Von besonderer Bedeutung ist für mich die nun bereits im dritten Jahr durchgeführte Schulung von Rechtsreferendaren, die ich in Zusammenarbeit mit dem Präsidenten des Oberlandesgerichts, Herrn Ulrich Hagenloch, und mit freundlicher Unterstützung des Präsidenten des Sächsischen Landtages, Herrn Dr. Matthias Rößler, im Landtagsgebäude durchführe. Beiden gilt mein besonderer Dank. Sie ermöglichen damit jährlich ca. 60 angehenden sächsischen Volljuristen einen wertvollen Einblick in die Rechtsgrundlagen des Datenschutzes und die Praxis meiner Behörde.

Im Berichtszeitraum habe ich Datenschutzvorträge u. a. bei der Sächsischen Notarkammer gehalten. Meine Mitarbeiter haben dienstlich Datenschutzvorträge bei der Landesdirektion Dresden, der Sächsischen Apothekerkammer, dem Ausbildungszentrum Bobritzsch der sächsischen Justiz, dem EDV-Gerichtstag in Saarbrücken, auf Podiumsdiskussionsveranstaltungen in Würzburg sowie an anderen Stellen gehalten.

Außerdem haben meine Bediensteten im Rahmen von Fortbildungsmaßnahmen der Akademie für öffentliche Verwaltung des Freistaates Sachsen, der Verwaltungs- und Wirtschaftsakademie Dresden, der Verwaltungs- und Wirtschaftsakademie Leipzig, dem Sächsischen Kommunalen Studieninstitut Dresden sowie dem Bildungswerk des SMS staatliche und kommunale Bedienstete in Fragen des Datenschutzes geschult.

Ich sehe all dies insbesondere im Hinblick auf die Stärkung der Datenschutzbeauftragten nach § 11 SächsDSG als dringend erforderlich an. Die internen Datenschutzbeauftragten sind ein wichtiges und unverzichtbares Element der Selbstkontrolle der öffentlichen Stellen. Sie zu stärken und ihre Aufgaben und Befugnisse auch den Dienststellenleitungen verständlich zu machen, ist mir ein besonderes Anliegen.

16 Ordnungswidrigkeitenverfahren

16.1 Übersicht

Der Sächsische Datenschutzbeauftragte ist zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 38 SächsDSG (§ 38 Abs. 3 Satz 1 SächsDSG).

Im Berichtszeitraum sind durch meine Behörde 90 Ordnungswidrigkeitenverfahren abgeschlossen worden.

In 47 dieser Verfahren sind zur Ahndung von Verstößen nach § 38 Abs. 1 Nr. 1 SächsDSG, in denen unbefugt nicht offenkundige personenbezogene Daten
- verarbeitet,
- zum Abruf bereitgehalten oder
- für sich selbst oder einen anderen abgerufen oder auf andere Weise verschafft worden sind,

Bußgeldbescheide gegen die Betroffenen erlassen worden.

Davon sind 11 der 47 Verfahren nach eingelegtem Einspruch gegen den Bußgeldbescheid dem zuständigen Amtsgericht vorgelegt worden. Die Summe der rechtskräftigen Bußgelder belief sich auf insgesamt 6.810 €.

Von den verbleibenden 43 Verfahren sind 42 eingestellt worden. Ein Verfahren ist wegen vorliegender Anhaltspunkte für eine Straftat an die zuständige Staatsanwaltschaft abgegeben worden.

In den Fällen, in denen ein Bußgeldbescheid wegen Verstoßes gegen § 38 Abs. 1 Nr. 1 SächsDSG erlassen worden ist, handelt es sich zum überwiegenden Teil um von den Betroffenen nicht dienstlich veranlasste Abrufe von personenbezogenen Daten in ihnen ausschließlich für dienstliche Zwecke zur Verfügung stehenden, nicht allgemein zugänglichen, elektronischen Informationssystemen. Diese personenbezogenen Daten unterliegen des Weiteren dem Datengeheimnis gemäß § 6 SächsDSG. Demnach ist es den für eine öffentliche Stelle tätigen Personen, die bei der Aufnahme ihrer Tätigkeit über die Verpflichtung auf das Datengeheimnis entsprechend aufgeklärt und belehrt worden sind, untersagt, personenbezogene Daten unbefugt zu verarbeiten. Die Handlung des unbefugten Abrufs personenbezogener Daten stellt folglich zumeist auch eine Verletzung des Datengeheimnisses gemäß § 6 Abs. 1 Satz 1 SächsDSG und somit eine Ordnungswidrigkeit nach § 38 Abs. 1 Nr. 3 SächsDSG dar.

17 Materialien

17.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

17.1.1 Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin: Staatsvertrag zum IT-Planungsrat - Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

17.1.2 Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin: Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglich-

keiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

17.1.3 Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin: „Reality-TV“ - keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

„Reality-TV“-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige „Lieferanten“ für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen - wobei auch schon einmal eine Wohnung zwangsgeöffnet wird - oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger „Unterhaltungssendungen“ ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen „Reality“-Reportagen Abstand zu nehmen.

17.1.4 Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin: Krankenhausinformationssysteme datenschutzgerecht gestalten!

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

17.1.5 Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin: Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem „Europa der Bürger“. Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z. B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen - auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST - im weiteren Verfahren einzusetzen.

17.1.6 Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin: Aktueller Handlungsbedarf beim Datenschutz - Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;
- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;
- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;
- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;
- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;
- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;
- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;
- die Videoüberwachung in Staat und Gesellschaft einzuschränken;
- den Schutz der Meldedaten zu verbessern;
- ein praktikables Datenschutzaudit zu schaffen;

- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

17.1.7 Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart: Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.

- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

17.1.8 Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart: Ein modernes Datenschutzrecht für das 21. Jahrhundert - Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können - soweit erforderlich - in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität

informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

17.1.9 Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart: Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

17.1.10 Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart: Körperscanner - viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über

den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

17.1.11 Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart: Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft

etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden

- die mit der zu evaluierenden Norm intendierten Ziele,
- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,
- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z. B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),
- die Leistung, Wirkung sowie der Erfolg und die Effizienz,
- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

17.1.12 Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. März 2010 in Stuttgart: Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechnungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

17.1.13 Entschließung zwischen der 79. und 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010: Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst wer-

den und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln - etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.

- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn - wie im Entwurf vorgesehen - Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv - und nicht erst auf Nachfrage - darüber aufzuklären, woher die verwendeten Daten stammen.

- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

- Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert

ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

17.1.14 Entschließung zwischen der 79. und 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juni 2010: Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- Vorherige Information der Arbeitnehmer
  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- Keine Speicherung auf Vorrat
  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- Verhindern des unzulässigen Datenabrufs
  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf

nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept
  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

17.1.15 Entschließung zwischen der 79. und 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010: Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsels bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages - RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der

Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

- die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,

- bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und

- auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

17.1.16 Entschließung der 80. Konferenz der der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010 in Freiburg: Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. So muss insbesondere die Kontrolle, ob gesetzliche Anforderungen eingehalten werden, Aufgabe der Datenschutzbehörden bleiben.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung

einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

17.1.17 Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010 in Freiburg: Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die - ggf. gänzlich unverdächtigen - Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

17.1.18 Entschließung der 80. Konferenz der der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010 in Freiburg: Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungs-

systeme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

17.1.19 Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 in Würzburg: Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90 / DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis

  - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
  - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
  - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.

- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.

- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte - Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.

- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien - z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten - erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.

- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.

- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere

  - zu verbieten, die z. B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.
  - für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.

- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.

- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen

  - zur Personalaktenführung - einschließlich der automatisierten Personalaktenführung,
  - zur privaten Nutzung von Telekommunikationsdiensten,
  - zum Thema Whistleblowing,
  - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,
  - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,
  - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

17.1.20 Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17 März 2011 in Würzburg: Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leistungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.
3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.
4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.
5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.
6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.
7. Grundstandards - wie beispielsweise die Revisionssicherheit - sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden oder

b) - eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
   - mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
   - die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.

17.1.21 Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 in Würzburg: Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z. B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100 a, 100 b Strafprozessordnung angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht ge-

forderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit - auch für die Strafverfolgungsbehörden - zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

17.1.22 Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 in Würzburg: Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

17.1.23 Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 in Würzburg: Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens - dringender Handlungsbedarf auf nationaler und europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass - wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[14] - EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim

[14] Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.

klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

17.1.24 Entschließung zwischen der 81. und 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011: Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100g Abs. 2 Satz 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur - wie etwa eine Telekommunikationsüberwachung nach

§ 100a StPO - gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

17.2 Sonstiges

17.2.1 Urteil des Sächsischen Oberverwaltungsgerichtes (3 A 224/10) vom 21. Juni 2011 in der Verwaltungsrechtssache TU Dresden gegen den Sächsischen Datenschutzbeauftragten wegen datenschutzrechtlicher Beanstandung gegenüber der Klägerin

Ausfertigung

Az.: 3 A 224/10 1 K 1158/04

SÄCHSISCHES OBERVERWALTUNGSGERICHT

Im Namen des Volkes

Urteil

In der Verwaltungsrechtssache

der Technischen Universität Dresden vertreten
durch den Rektor
dieser vertreten durch das Justitiariat
[redacted]

- Klägerin -
- Berufungsbeklagte -

prozessbevollmächtigt:
Heinemann & Partner Rechtsanwälte
III. Hagen 30, 45127 Essen

gegen

den Sächsischen Datenschutzbeauftragten
Bernhard-von-Lindenau-Platz 1, 01067 Dresden

- Beklagter -
- Berufungskläger -

wegen

datenschutzrechtlicher Beanstandung gegenüber der Klägerin
hier: Berufung

hat der 3. Senat des Sächsischen Oberverwaltungsgerichts durch den Vorsitzenden Richter am Oberverwaltungsgericht Dr. Freiherr von Welck, die Richterin am Oberverwaltungsgericht Drehwald, den Richter am Verwaltungsgericht Dr. John aufgrund der mündlichen Verhandlung vom 9. Juni 2011

am 21. Juni 2011

für Recht erkannt:

Auf die Berufung des Beklagten wird das Urteil des Verwaltungsgerichts Dresden vom 25. Oktober 2007 - 1 K 1158/04 - geändert. Die Klage wird insgesamt abgewiesen.

Die Klägerin trägt die Kosten des Verfahrens beider Rechtszüge.

Die Revision wird nicht zugelassen.

Tatbestand

1 Die Klägerin wendet sich gegen eine vom Beklagten ihr gegenüber ausgesprochene datenschutzrechtliche Beanstandung, die sich auf ein Schreiben ihres damaligen Rektors vom 19. September 2000 nebst einer Anlage an den damaligen Sächsischen Staatsminister für Wissenschaft und Kunst bezieht.

2 Der Herz-Kreislauf-Zentrum Dresden e. V. (im Folgenden: HKZD) war Träger und Betreiber einer Klink, des Herz-Kreislauf-Zentrums Dresden. Das Herz-Kreislauf-Zentrum Dresden ist von einer Objektgesellschaft errichtet worden. Das Grundstück hierfür wurde im Wege eines Erbbaurechts von einer Stiftung, die von der Unternehmensgruppe [redacted] und weiteren Unternehmen bzw. Privatpersonen gegründet worden war, zur Verfügung gestellt. Der HKZD hat mit der Klägerin eine Rahmenvereinbarung über die Errichtung, den Betrieb und die Nutzung des Herz-Kreislauf-Zentrums Dresden abgeschlossen; hierin sind auch Regelungen über die Grundlagen der personellen Zusammenarbeit, die Zusammenarbeit im Rahmen der medizinischen Konzeption sowie weitere Grundsätze der Zusammenarbeit vereinbart worden. Professor Dr. [redacted] S[redacted] wurde mit Wirkung vom 15. Juli 1995 zum Universitätsprofessor an der Klägerin berufen, hatte mit dem HKZD gleichzeitig einen privatrechtlichen Vertrag über seine Tätigkeit in der Krankenversorgung, der Forschung und Lehre dort abgeschlossen und war für die Dauer seiner Tätigkeit dort als Professor beurlaubt. Professor Dr. S[redacted] war darüber hinaus von Dezember 1994 bis Juli 2001 medizinischer Geschäftsführer des Herz-Kreislauf-Zentrums Dresden mit einer umfassenden Handlungsvollmacht für dieses.

3 Gemäß der Satzung des HKZD sollte ein Mitglied des Aufsichtsrats des Trägervereins zugleich Mitglied der Verwaltungsgremien der Klägerin sein; der damalige Rektor der Klägerin, Professor Dr. [redacted] M[redacted], wurde mehrfach zum Mitglied des Aufsichtsrats gewählt. Vorsitzender des Aufsichtsrats war satzungsgemäß der damalige Staatsminister für Wissenschaft und Kunst, Professor Dr. [redacted] M[redacted]. Am 19. September 2000 übermittelte der damalige Rektor an den damaligen Staatsminister für Wissenschaft und Kunst ein Schreiben, in dessen Anlage Gedanken zur weiteren Strategie des Aufsichtsrats gegenüber dem Herz-Kreislauf-Zentrum Dresden und dessen (Förder-)Verein niedergelegt worden sind („Strategiepapier"). Das Schreiben benutzt den persönlichen Briefbogen des Rektors der Klägerin und ist an den „Vorsitzenden des Aufsichtsrats für das Herz- und Kreislaufzentrum Dresden e. V. Herrn Staatsminister für Wissenschaft und Kunst Professor Dr. [redacted] M[redacted]“ adressiert. Das Strategiepapier, das mit „Gedanken über die weitere Strategie des Aufsichtsrats gegenüber dem Herz- und Kreislaufzentrum Dresden e. V.“ überschrieben ist und als Ersteller den Rektor der Klägerin ausweist, befasst sich mit dem Ziel, die Satzung so zu ändern, dass das Herz-Kreislauf-Zentrum Dresden in eine neue Rechtsform überführt wird und der Verein keinerlei Einwirkungsmöglichkeit auf Vorstand und Geschäftsleitung mehr besitzt, sondern bestenfalls als Förderverein weiter existiert; darüber hinaus soll das Herz-Kreislauf-Zentrum Dresden wissenschaftlich eng an das Universitätsklinikum Dresden gebunden und mögliche Synergien sollen genutzt werden. Da dies mit der gegenwärtigen Besetzung der Mitglieder des Vereins nicht zu bewerkstelligen sei, müssten seitens der Staatsregierung alle möglichen in Betracht kommenden Maßnahmen koordiniert werden, um den Verein zum Einlenken zu zwingen und dessen Zusammensetzung zu verändern. Unter Nummer 5 des Strategiepapiers heißt es wörtlich:

> „Eine Schlüsselfigur im Förderverein ist Herr Professor S[redacted]. Er ist der Strippenzieher hinter den Kulissen. Er entscheidet, wie abgestimmt wird. Er koordiniert die Strategien gegen den Aufsichtsrat. Er genießt offensichtlich Rechtsberatung, die ihm die Stumpfheit der Waffen vermittelt, die dem Aufsichtsrat zur Verfügung stehen.

4 Es wäre deshalb erforderlich,

a) disziplinarische Schritte des Dienstherren gegen seinen Landesbeamten einzuleiten, dabei sollte man lieber zu weit gehen als zu zaghaft sein,

b) Ausschluss aus dem Förderverein durch den eingesetzten Vorstand betreiben,

c) seine wissenschaftliche Leistung zu evaluieren und die Einhaltung seiner Lehrverpflichtungen zu überprüfen, möglichst durch offizielle Peers von außen,

d) alle Möglichkeiten prüfen, ihn als Hochschullehrer zu beurlauben und ihm den Professoren-Titel abzuerkennen.

Auch hier halte ich die Möglichkeit zur Einflussnahme eher für begrenzt. Die Wirkungen werden ebenfalls begrenzt sein. (Man kann doch fragen: Ist wirklich jeder berufene Professor des UKD wissenschaftlich und ärztlich besser als Herr S[redacted]? Dagegen ließe sich, nach meiner Auffassung, mit Erfolg argumentieren.)“

5 Die Anlage ist vom damaligen Rektor der Klägerin handschriftlich unterzeichnet.

6 Nach Durchführung mehrerer Kontrollen im Rektorat der Klägerin beanstandete der Beklagte mit Schreiben vom 11. April 2003 gegenüber der Klägerin, vertreten durch ihren Rektor, die rechtswidrige Verarbeitung von personenbezogenen Daten von Professor Dr. S[redacted] durch das Schreiben vom 19. September 2000 und das Strategiepapier, das dort als „Zersetzungsplan“ bezeichnet wurde. In der Beanstandung wurde zusammenfassend darauf hingewiesen, dass es sich bei den in Nummer 5 des Strategiepapiers enthaltenen Mitteilungen um personenbezogene Daten handele, deren Verarbeitung unzulässig gewesen sei. Die übermittelten Daten hätten Personalaktenqualität i . S. v. § 117 Abs. 1 Satz 2 SächsBG und hätten zu der Personalakte genommen werden müssen. Der damalige Rektor der Klägerin habe in dieser Funktion und nicht als Mitglied im Aufsichtsrat des HKZD gehandelt. Der damalige Staatsminister für Wissenschaft und Kunst sei nicht als Vorsitzender des Aufsichtsrats des HKZD, sondern als Dienstvorgesetzter von Professor Dr. S[redacted] informiert worden. Zudem wurde auf die Pflicht zur Mängelbeseitigung hingewiesen und zur Berichterstattung hierüber eine Frist bis zum 15. Mai 2003 gesetzt. Mit Schreiben vom 7. Januar 2004 forderte der Bevollmächtigte der Klägerin den Beklagten auf, die Beanstandung, soweit sie sich auf die Klägerin beziehe, aufzuheben. Nachdem der Beklagte mit Schreiben vom 15. Januar 2004 dies ablehnt hatte, hat die Klägerin am 5. Mai 2004 Klage erhoben.

7 Zur Begründung hat sie geltend gemacht, dass ihr damaliger Rektor in seiner Funktion als Mitglied des Aufsichtsrats auf dessen Wunsch dem damaligen Aufsichtsratsvorsitzenden seine Vorstellungen über die weitere Strategie des Aufsichtsrats gegenüber dem HKZD persönlich und vertraulich übermittelt habe. Da sowohl der

damalige Rektor wie auch der damalige Staatsminister für Wissenschaft und Kunst in ihrer Eigenschaft als Mitglieder des Aufsichtsrats des HKZD tätig geworden seien, sei der Anwendungsbereich des Datenschutzgesetzes nicht eröffnet, denn bei dem HKZD handele es sich weder um eine öffentliche Stelle i. S. des § 2 Abs. 1 des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz vom 11. Dezember 1991, SächsGVBl. S. 401, in seiner bis zum 8. September 2003 geltenden Fassung - im Folgenden: SächsDSG a. F.) noch sei § 2 Abs. 2 SächsDSG a. F. einschlägig. Weder sei der Staatsminister für Wissenschaft und Kunst Dritter i. S. v. § 3 Abs. 4 SächsDSG a. F., noch sei der Rektor der Klägerin Dienstvorgesetzter der Professoren; dies sei ausschließlich das Staatsministerium für Wissenschaft und Kunst. Ferner habe es sich bei den übermittelten Daten nicht um Daten mit Personalaktenqualität gehandelt; die in dem Strategiepapier getroffenen Feststellungen seien in der vom Staatsministerium für Wissenschaft und Kunst geführten Personalakte von Professor Dr. S[redacted] bereits in vollem Umfang enthalten. Schließlich sei die Klage auch zulässig; insbesondere fehle nicht das Rechtsschutzinteresse, da der Beklagte sein Amt für außerhalb des Datenschutzes liegende Ziele missbraucht und eine datenschutzrechtliche Beanstandung ausgesprochen habe, ohne dass auch nur entfernt die Voraussetzungen dafür gegeben gewesen seien. Auch wenn man davon ausgehe, dass eine solche Beanstandung grundsätzlich keine materielle Rechtswirkung entfalte, sei sie doch für das Ansehen der Klägerin und der für sie handelnden Organe in hohem Maße abträglich.

8 Die Klägerin hat beantragt,

1. festzustellen, dass in dem beanstandeten Schreiben ihres Rektors vom 19. September 2000 keine personenbezogenen Daten im Sinne des Sächsischen Datenschutzgesetzes verarbeitet wurden und die datenschutzrechtliche Beanstandung des Beklagten vom 11. April 2003 ungerechtfertigt war,

2. den Beklagten zu verpflichten, dem Sächsischen Landtag darüber zu berichten, dass die Beanstandung vom 11. April 2003 nicht rechtmäßig gewesen sei.

9 Der Beklagte hat beantragt,

die Klage abzuweisen.

10 Zur Begründung hat er angeführt, die Beanstandung sei einer gerichtlichen Überprüfung entzogen, da sie keine materielle Rechtswirkung für den betroffenen Rechtsträger entfalte. Der damalige Rektor der Klägerin habe nicht als Privat-

person oder als bloßes Organmitglied des HKZD gehandelt, sondern als gesetzlicher Vertreter der Klägerin. Zu personenbezogenen Daten gehörten auch Angaben über die berufliche Betätigung und sonstige, auch private Aktivitäten ebenso wie Werturteile. Als solche seien die Ausführungen in Nummer 5 des Strategiepapiers anzusehen, da es sich hierbei durchweg um die Schilderung persönlicher Verhältnisse von Professor Dr. S[redacted], nämlich um die zugleich auch wertende Darstellung seines Verhaltens in den Gremien des HKZD gehandelt habe. Darüber hinaus seien dessen persönliche Verhältnisse angesprochen worden. Die Daten seien erhoben, gespeichert und an den damaligen Staatsminister für Wissenschaft und Kunst als Dritten übermittelt worden. Die Verarbeitung der Daten habe auch nicht mit § 11 ff. SächsDSG a. F. in Einklang gestanden.

11 Mit Urteil vom 25. Oktober 2007 hat das Verwaltungsgericht Dresden festgestellt, dass in dem beanstandeten Schreiben des damaligen Rektors der Klägerin keine personenbezogenen Daten i. S. d. Sächsischen Datenschutzgesetzes verarbeitet worden seien und die datenschutzrechtliche Beanstandung des Beklagten vom 11. April 2003 ungerechtfertigt gewesen sei. Im Übrigen ist die Klage abgewiesen worden.

12 Statthafte Klageart - so das Gericht - sei die Feststellungsklage gemäß § 43 Abs. 1 VwGO. Die Klägerin habe ein schützenswertes Feststellungsinteresse, auch wenn eine datenschutzrechtliche Beanstandung regelmäßig keine unmittelbaren materiellen Rechtswirkungen für den betroffenen Rechtsträger entfalte. Die regelmäßig hervorgerufene so genannte Prangerwirkung einer Beanstandung sei im vorliegenden Fall aber ausnahmsweise nicht hinzunehmen, weil die Klägerin mit beachtlichen Gründen geltend mache, einer rechtlich nicht mehr gedeckten Prangerwirkung ausgesetzt zu sein, da der Beklagte seine Kompetenz eindeutig überschritten habe. Ein Interesse könne darüber hinaus unter dem Gesichtspunkt angenommen werden, dass die verfassungsrechtlich geschützte Wissenschaftsfreiheit der Klägerin zugleich einen ungestörten Wissenschaftsbetrieb umfasse und letzterer durch die Behauptung des Beklagten, die Leitung der Klägerin verstoße gegen das Datenschutzgesetz, möglicherweise beeinträchtigt werde. Die Beanstandung sei nicht gerechtfertigt gewesen, da das beanstandete Verhalten des damaligen Rektors der Klägerin nicht dem Anwendungsbereich des Sächsischen Datenschutzgesetzes unterlegen habe und in dem Schreiben vom 19. September 2000 keine Daten i. S. d. Sächsischen Datenschutzgesetzes verarbeitet worden seien. Das Schreiben stelle kein Handeln einer öffentlichen Stelle im vorgenannten Sinne dar, da es sich - abgestellt auf den Empfängerhorizont - um einen privaten Schriftwechsel gehandelt habe, der der Klägerin nicht zuzurechnen gewesen sei. Darüber

hinaus seien auch keine personenbezogenen Daten i. S. von § 3 Abs. 2 SächsDSG a. F. verarbeitet worden. Es seien offenkundig keine Daten insbesondere in Bezug auf Professor Dr. S[redacted] enthalten, die für die oder von der Klägerin erhoben oder übermittelt worden seien. Der Verfasser habe lediglich seine Auffassung über die Tätigkeit und Stellung von Professor Dr. S[redacted] im Förderverein geäußert. Da sich die Angaben erkennbar nicht auf die Tätigkeit von Professor Dr. S[redacted] als Universitätsprofessor und ebenso wenig auf außerdienstliche Tätigkeiten bezogen hätten, die für eine dienstrechtliche Beurteilung hätten von Belang sein können, handele es sich auch nicht um Daten mit „Personalaktenqualität“. Schließlich sei das informationelle Selbstbestimmungsrecht von Professor Dr. S[redacted] nicht durch die Vorschläge des Verfassers zum weiteren Vorgehen diesem gegenüber verletzt worden, da darin - abgesehen von dessen öffentlich und damit allgemein bekannter Stellung als Hochschulprofessor - keine persönlichen Daten aufgeführt worden seien. Ein weitergehender Folgenbeseitigungsanspruch bestehe nicht, denn die ungerechtfertigte Beanstandung des Beklagten habe im Sächsischen Landtag unter datenschutzrechtlicher Sicht keine weiteren Nachteile für die Klägerin nach sich gezogen.

13 Gegen das Urteil legte der Beklagte die mit Beschluss vom 3. März 2010 - 3 A 39/08 - zugelassene Berufung ein. Zur Begründung weist er darauf hin, dass die Klage bereits unzulässig sei. Bei der datenschutzrechtlichen Beanstandung handele es sich mangels Regelung eines Einzelfalls auf dem Gebiet öffentlichen Rechts nicht um einen Verwaltungsakt. Für eine allgemeine Leistungsklage fehle die Klagebefugnis analog § 42 Abs. 2 VwGO, ebenso das Feststellungsinteresse gemäß § 43 Abs. 1 VwGO für eine Feststellungsklage. Die Wissenschaftsfreiheit gemäß Art. 5 Abs. 3 GG und Art. 21 SächsVerf, auf die sich die Klägerin als Universität zwar grundsätzlich berufen könne, sei nicht berührt, da ihr gegenüber die datenschutzrechtliche Beanstandung keine rechtserheblichen Wirkungen besitze. Zudem handele es sich bei dem Beanstandungsgegenstand nicht um einen Vorgang der Forschung oder Lehre, sondern allein um einen solchen der Personalverwaltung. Schließlich könne auch die Intensität, mit der sich die Klägerin durch die streitgegenständliche Beanstandung betroffen fühle, nicht zur Rechtserheblichkeit dieses Vorgangs führen; ansonsten würde die Klägerin bevorzugt, die sich mit dem Argument verteidige, der Sächsische Datenschutzbeauftragte habe seine Kompetenz eindeutig überschritten, gegenüber demjenigen, der bescheidener auftrete. Im Übrigen fehle es vorliegend an einer solchen Prangerwirkung. Darüber hinaus handele es sich dem äußeren Schein des Schreibens vom 19. September 2000 nach, aufgrund der Tatsache, dass der damalige Rektor der Klägerin genauso wie der damalige Staatsminister für Wissenschaft und Kunst in ihren amtlichen

Funktionen Mitglieder des Aufsichtsrats des HKZD gewesen seien, der weiteren Tatsache, dass Professor Dr. S[redacted] auch als Beamter und Professor angesprochen worden sei, und schließlich aufgrund der Tatsache, dass diesem gegenüber Maßnahmen empfohlen worden seien, die ihn nur in dieser Rechtsstellung betroffen hätten, auch aus Sicht eines verständigen Empfängers um eine vom Anwendungsbereich des Sächsischen Datenschutzgesetzes erfasste Verarbeitung personenbezogener Daten. Bei den Feststellungen und Werturteilen, die der damalige Rektor der Klägerin zum Ausdruck gebracht habe, habe es sich auch um Personaldaten i. S. v. § 3 Abs. 1 SächsDSG a. F. gehandelt. Auch Werturteile dienten der Darstellung persönlicher oder sachlicher Verhältnisse einer Person und bezweckten gerade auch eine informative Aussage über den Betroffenen. Hiervon ausgehend enthalte das beanstandete Dokument in beträchtlichem Umfang Einzelangaben über persönliche und sachliche Verhältnisse von Professor Dr. S[redacted]. Die Daten seien erhoben, gespeichert und an den damaligen Staatsminister für Wissenschaft und Kunst als einen Dritten übermittelt worden. Bei letzterem handele es sich gemäß § 3 Abs. 4 SächsDSG a. F. um eine Person oder Stelle außerhalb der datenverarbeitenden Stelle, da er nicht Bestandteil der öffentlichen Stelle „TU Dresden“ sei; er sei vielmehr Bestandteil einer funktionell oder sogar organisatorisch anderen Stelle. Dass ihm Aufsichtsbefugnisse über die Klägerin zukämen, ändere an dieser Rechtsstellung nichts. Dies ergebe sich schon aus § 13 Abs. 1 i. V. m. § 12 Abs. 3 Satz 1 SächsDSG a. F. Denn hierin werde die Übermittlung von personenbezogenen Daten i. S. v. § 3 Abs. 2 Nr. 5 SächsDSG a. F. zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen gerade vorausgesetzt. Die Datenverarbeitung sei auch rechtswidrig. Gemäß § 26 SächsDSG a. F. könne er einen entsprechenden Verstoß beanstanden und sei dabei gemäß § 23 Abs. 4 Satz 1 SächsDSG a. F. unabhängig, weisungsfrei und nur dem Gesetz unterworfen. Gemäß § 27 Abs. 2 SächsDSG a. F. habe er den Vorgang auch dem Sächsischen Landtag zuleiten und ihn hierdurch öffentlich machen können. Von einem Amtsmissbrauch oder einer vorsätzlichen Schädigung des Ansehens der Klägerin oder ihres damaligen Rektors könne daher keine Rede sein.

14 Der Beklagte beantragt,

das Urteil des Verwaltungsgerichts Dresden, soweit der Klage stattgegeben wurde, aufzuheben und die Klage insgesamt abzuweisen.

15 Die Klägerin beantragt,

die Berufung zurückzuweisen.

16 Zur Begründung weist sie darauf hin, dass es dem damaligen Sächsischen Datenschutzbeauftragten nur darauf angekommen sei, den damaligen Rektor an den Pranger zu stellen und ihn vorzuführen. Dies habe auch die Staatsanwaltschaft Dresden in ihrem Beschluss vom 16. Oktober 2003 festgestellt. Gemäß Art. 19 Abs. 4 GG seien die Gerichte verpflichtet, Behördenentscheidungen grundsätzlich uneingeschränkt zu kontrollieren. Abgesehen von der Prangerwirkung der Vorgehensweise habe der Beklagte auch in die verfassungsrechtlich geschützte Wissenschaftsfreiheit eingegriffen, da durch Art. 5 Abs. 3 Satz 1 GG auch die Universität als Institution geschützt sei. Die Beleidigungen und ehrabschneidenden Ausführungen des Beklagten hätten der Klägerin sehr geschadet. Sowohl in der gesamten Professoren- als auch in der Studentenschaft hätten Aufregung und Unruhe geherrscht. Neben dem damaligen Rektor seien das gesamte Leitungsgremium und insbesondere die Universität selbst über einen erheblichen Zeitraum geschädigt worden und alle Beteiligten seien über Monate gehalten gewesen, diese Attacken des damaligen Sächsischen Datenschutzbeauftragten zu entkräften. Damit seien wichtige Kräfte gebunden gewesen, die für Forschung und Lehre fördernde Aktivitäten sinnvoller einsetzbar gewesen wären. Im Übrigen verweist sie auf ihr bisheriges Vorbringen.

17 Wegen der weiteren Einzelheiten des Sach- und Streitstands wird auf den Inhalt der Gerichtsakte in diesem Verfahren, der Akten des Verfahrens 3 A 39/08, 1 K 1158/04 des Verwaltungsgerichts Dresden sowie der beigezogenen Behördenakte verwiesen.

Entscheidungsgründe

18 Die Klage hat keinen Erfolg, denn der Klägerin fehlt für das als allgemeine Leistungsklage statthafte Begehren die Klagebefugnis.

19 1. Da die Beanstandung ihrer Rechtsnatur nach kein Verwaltungsakt ist, kommt vorliegend keine Anfechtungsklage in Betracht. Der Rüge des Sächsischern Datenschutzbeauftragten, mit der Verstöße gegen das Sächsische Datenschutzgesetz oder andere Vorschriften über den Datenschutz festgestellt und beanstandet werden, kommt nämlich - anders als etwa bei einer Beanstandung der Rechtsaufsichtsbehörde gemäß § 114 SächsGemO zumindest im Bereich der Selbstverwaltungsangelegenheiten (vgl. hierzu Kopp/Schenke, VwGO, 16. Aufl. 2009, § 42 Rn. 139 m. w. N.) - keine Regelungswirkung zu (BVerwG, Beschl. v. 5. Februar 1992 - 7 B 15/92 -, juris Rn 2; vorausgehend OVG Schl.-H., Urt. v. 16. September 1991 - 1 L 18/91-, juris Rn. 25 f.; Gola/Schomerus, Bundesdatenschutzgesetz, 8. Aufl. 2005, § 25 Rn. 6).

20 Hieran ändert auch nichts, dass gemäß § 26 Abs. 1 Satz 1 SächsDSG a. F. (nunmehr § 29 Abs. 1 Satz 1 SächsDSG) der Datenschutzbeauftragte zur Mängelbeseitigung innerhalb einer von ihm zu bestimmenden angemessenen Frist auffordern konnte. Damit ist dem Beklagten nämlich nicht die Befugnis zum Anlass eines Verwaltungsakts eingeräumt (vgl. hierzu Giesen in: Giesen/Banasch/Naumann/Mauersberger/Dehoust, Kommentar zum Sächsischen Datenschutzgesetz, 1. Aufl. 2011, § 29 Rn. 9 ff.). Anders als in § 25 BDSG und - soweit ersichtlich - in anderen Landesdatenschutzgesetzen kommt dem Sächsischen Datenschutzbeauftragten nach dem Sächsischen Datenschutzgesetz zwar die Kompetenz zu, die betroffene Stelle zur Behebung der festgestellten Verstöße innerhalb einer von ihm zu bestimmenden angemessenen Frist aufzufordern. Bei der hieraus für die betroffene Stelle folgenden Beachtenspflicht handelt es sich aber nicht um die Rechtsfolge eines vom Sächsischen Datenschutzbeauftragten erlassenen Verwaltungsakts, dem Verbindlichkeit auf Grund hoheitlichen Geltungsanspruchs zukommen würde und der nach den Regeln des Verwaltungsvollstreckungsgesetzes vollstreckbar wäre. Vielmehr kann der Sächsische Datenschutzbeauftragte bei Missachtung seiner diesbezüglichen Aufforderung nur die ihm vom Gesetz zur Verfügung gestellten politischen Druckmittel und sein politisches Gewicht einsetzen; daneben kommt auch in Betracht, dass er sich mit der Bitte, diesbezügliche rechtsaufsichtliche Maßnahmen zu ergreifen, an die übergeordnete Stelle wendet. Exekutivbefugnisse, die den Erlass diesbezüglicher Verwaltungsakte umfassten, stehen ihm gemäß § 26 Abs. 1 Satz 1 SächsDSG a. F. (nunmehr § 29 Abs. 1 Satz 1 SächsDSG) hingegen nicht zur Verfügung (ähnlich Zöllner, Der Datenschutzbeauftragte im Verfassungssystem, Berlin 1995, S. 58, der zwar im Einzelfall von einem Verwaltungsakt ausgeht, diesen aber nicht für mit Zwangsmitteln durchsetzbar hält, so dass einer Klage hiergegen das Rechtsschutzbedürfnis fehlen soll). Dies ergibt sich aus der Stellung des Sächsischen Datenschutzbeauftragten als selbstständiges Verfassungsorgan gemäß Art. 57 SächsVerf und als Hilfsorgan von Parlament und Staatsregierung (zu allem Giesen, a. a. O., § 25 Rn. 8 ff.). Soweit dem Sächsischen Datenschutzbeauftragten behördliche Verwaltungsbefugnisse (Beispiele bei Giesen, a. a. O., Rn. 14) zukommen, umfassen sie nach seiner konzeptionellen Stellung im verfassungsrechtlichen Kontrollgefüge aber nicht die Befugnis, im Rahmen seiner datenschutzrechtlichen Kontrollbefugnisse gegenüber Dritten Verwaltungsakte zu erlassen. Auch aus Entstehungsgeschichte und Begründung des Sächsischen Datenschutzgesetzes in seiner ursprünglichen wie auch in der nunmehr geltenden Fassung ergibt sich keinerlei Hinweis darauf, dass dem Datenschutzbeauftragten im Rahmen der Befugnis zur Beanstandung von Datenschutzverstößen vom Gesetzgeber auch die Ermächtigung zum Erlass eines Ver-

waltungsakts eingeräumt werden sollte (vgl. Begründung des Gesetzentwurfs vom 10. Juli 1991, LT-Drs. 1/526, sowie vom 28. März 2003, LT-Drs. 3/6181).

21 Schließlich lässt sich auch aus der mit der Novellierung des Sächsischen Datenschutzgesetzes vorgenommenen Anpassung an die Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) nicht ableiten, dass die mit weitgehend unverändertem Wortlaut in § 29 Abs. 1 Satz 1 SächsDSG übernommene Befugnis nach § 26 Abs. 1 Satz 1 SächsDSG a. F., zur Behebung von datenschutzrechtlichen Verstößen aufzufordern, dem Sächsischen Datenschutzbeauftragten die Ermächtigung zum Erlass eines Verwaltungsakts einräumen sollte (zu diesem Gedanken Giesen, a. a. O., § 29 Rn. 11). Zum einen wäre eine solche inhaltliche, auf der Umsetzung europäischen Rechts beruhende Kompetenzstärkung noch nicht für den hier maßgeblichen § 26 Abs. 1 Satz 1 SächsDSG a. F. festzustellen, weil zum Zeitpunkt von dessen Erlass die EG-Datenschutzrichtlinie noch nicht galt. Zum anderen bedarf es, um dem Sächsischen Datenschutzbeauftragten „wirksame Einwirkungsbefugnisse“ i. S. v. Art. 28 Abs. 3 2. Spiegelstrich EG-Datenschutzrichtlinie einzuräumen, keiner entsprechenden Ermächtigung, da die hierin genannten Befugnisse nicht zwingend den Erlass von Verwaltungsakten zur Mängelbeseitigung erfordern, solange dem Sächsischen Datenschutzbeauftragten - wie hier - andere effektive Mittel zur Verfügung stehen, seinen Anordnungen auf sonstige Weise Durchsetzungskraft zu verschaffen.

22 2. Wegen ihrer Subsidiarität gemäß § 43 Abs. 2 VwGO ist vorliegend nicht - wie vom Verwaltungsgericht Dresden angenommen - eine Feststellungsklage statthaft, sondern eine allgemeine Leistungsklage (hierzu auch BVerwG, a. a. O.). Die Klägerin hat hierzu in der mündlichen Verhandlung vom 9. Juni 2011 klargestellt, dass sie den vor dem erkennenden Senat noch anhängigen Klageantrag in diesem Sinne verstanden wissen will.

23 Der Klägerin fehlt allerdings für die allgemeine Leistungsklage die entsprechend § 42 Abs. 2 VwGO erforderliche Klagebefugnis.

24 Zwar stünde dieser nicht entgegen, dass es sich bei der Klägerin um eine rechtsfähige Körperschaft des öffentlichen Rechts handelt (§ 1 Abs. 1 SächsHSG), da sie - wie etwa eine Gemeinde - dem Beklagten auch außerhalb des behördlichen Binnenbereichs mit wehrfähigen Außenrechtspositionen gegenüberstehen kann. Vorliegend wäre es daher nicht von vornherein ausgeschlossen, dass sich die Klägerin als Grundrechtsträgerin auf ihre Wissenschaftsfreiheit (Art. 5 Abs. 3 GG)

berufen kann (vgl. Art. 19 Abs. 3 GG, hierzu Sachs, in: Sachs, Grundgesetz Kommentar, 5. Aufl. 2009, Art. 19 Rn. 96, und BVerfG, Urt. v. 27. Juli 2004, BVerfGE 111, 226, juris Rn. 125; Bethge, in: Sachs, a. a. O., Art. 5 Rn. 210 m. w. N.). Darüber hinaus könnte grundsätzlich auch eine aus der ehrverletzenden Prangerwirkung der Beanstandung herrührende Verletzung des „guten Rufs“ der Klägerin als Ausfluss der Wissenschaftsfreiheit in Betracht gezogen werden (von BVerwG, Beschl. v. 5. Februar 1992 - 7 B 15/92 -, juris Rn. 4, im Hinblick auf den „guten Ruf“ einer Gemeinde offen gelassen). Jedenfalls ist vorliegend nicht erkennbar, dass von der angegriffenen Beanstandung derartige Wirkungen ausgehen.

25 2.1 Im Hinblick auf die Wissenschaftsfreiheit müsste es sich dafür um einen staatlichen Eingriff in ihre organisatorischen Strukturen handeln, der einer freien wissenschaftlichen Betätigung abträglich ist; hierzu gehört auch die akademische Selbstverwaltung sowie das Promotions- und Habilitationsrecht (zu alledem Bethge a. a. O. m. w. N.). Mit der Rüge einer dem Datenschutz widersprechenden Tätigkeit des damaligen Rektors sind aber diese Bereiche nicht tangiert; der bloße und nicht weiter untermauerte Hinweis der Klägerin, ihre Gremien seien längere Zeit kaum arbeits- bzw. einsatzfähig gewesen, erscheint stark übertrieben. Hinweise darauf, dass die Klägerin in der Folge weniger Studenten oder keine Fördermittel erhalten haben könnte oder aber ihre Attraktivität für Professoren gesunken sei, sind nicht gemacht worden und auch nicht erkennbar.

26 2.2 Gleiches gilt für die vom Verwaltungsgericht Dresden angenommene Prangerwirkung der Beanstandung. Aus der von der Klägerin vorgetragenen Rechtswidrigkeit der Beanstandung allein kann eine solche Wirkung nicht hergeleitet werden (vgl. hierzu BVerwG, a. a. O.). Eine darüber hinausgehende, „den guten Ruf“ der Klägerin verletzende Wirkung kommt der Beanstandung aber nicht zu. Es ist zwar nicht abzustreiten, dass die Beanstandung vom Beklagten in einem bisweilen pointierten und Zuspitzungen enthaltenden Stil abgefasst ist. Mit dem mehrfach hierin verwendeten Begriff des „Zersetzungsplans“ (S. 3, 4 der Beanstandung) sollte aber, was spätestens seit Abgabe einer entsprechenden Erklärung durch den Beklagten mit Schreiben vom 15. Juni 2011 klargestellt ist, nicht der Vorwurf gemacht werden, die Klägerin bzw. ihr damaliger Rektor bediene sich der Methoden des Staatssicherheitsdienstes der ehemaligen DDR. Vielmehr handelt es sich bei dem Begriff - nach nunmehriger Klarstellung - um eine prägnante Umschreibung des gerügten Inhalts des Schreibens vom 19. September 2000.

27 Auch die Rüge der Klägerin, der Beklagte habe sich zu Unrecht auf seine datenschutzrechtliche Kompetenzen gestützt, weil der gerügte Sachverhalt nicht gemäß § 2 Abs. 1 SächsDSG a. F. unter den Anwendungsbereich des Sächsischen Daten-

schutzgesetzes fiele, führt zu keinem anderen Ergebnis. Offen bleiben kann dabei, ob eine Verletzung des „guten Rufs“ zumindest dann denkbar wäre, wenn die Kontrollmittel des Sächsischen Datenschutzgesetzes unter offensichtlicher Missachtung seines Anwendungsbereichs vom Beklagten etwa mit dem Ziel der - auch persönlichen - Diskreditierung herangezogen worden wären; denn vorliegend spricht viel dafür, dass - entgegen der Auffassung des Verwaltungsgerichts Dresden - dessen Anwendungsbereich gemäß § 2 Abs. 1 SächsDSG a. F. eröffnet war. Bei der Beurteilung der Frage, ob sich der damalige Rektor der Klägerin in seiner amtlichen Funktion oder aber als - nicht dem Anwendungsbereich von § 2 Abs. 1 SächsDSG a. F. unterfallendes - Aufsichtsratsmitglied des HKZD an den damaligen Staatsminister für Wissenschaft und Kunst gewandt hatte, ist dabei auf den Empfängerhorizont abzustellen (zu ähnlicher Frage, ob ein Verwaltungsakt vorliegt, vgl. Kopp/Ramsauer, VwVfG, 11. Aufl. 2010, § 35 Rn. 54 ff. m. w. N.). Hiervon ausgehend streitet viel für die Auffassung des Beklagten, dass die in der Beanstandung gerügten Äußerungen der Klägerin zuzurechnen waren: Das Anschreiben wie auch der Briefkopf des Strategiepapiers wiesen den Verfasser als den Rektor der Klägerin aus. Darüber hinaus wurden unter Nr. 5a, c sowie d des Strategiepapiers Maßnahmen vorgeschlagen, die Professor Dr. S[redacted] in seinem Dienstverhältnis zum Freistaat Sachsen betrafen und nur vom damaligen Staatsminister für Wissenschaft und Kunst als dessen Dienstvorgesetzten hätten durchgeführt werden können. Die Vorschläge waren zum Gutteil auf angebliche Kenntnisse gestützt, die der damalige Rektor der Klägerin nur im Rahmen seiner dienstlichen Stellung erlangt haben konnte. Dass diese Sichtweise - zunächst - auch vom Ministerbüro des damaligen Staatsministers für Wissenschaft und Kunst geteilt wurde, zeigt der auf dem Anschreiben vom 19. September 2000 enthaltene Stempel vom 21. September 2000, der eine weitere Bearbeitung als Dienstvorgang nach sich zog; dies entsprach übrigens augenscheinlich der damaligen Handhabung im Ministerium, weil sogar ein offensichtlich allein die Aufsichtsratstätigkeit des damaligen Staatsministers für Wissenschaft und Kunst betreffendes, in unmittelbarem Zusammenhang mit dem Strategiepapier eingegangenes Schreiben des Dekans der Medizinischen Fakultät der Klägerin vom 18. September 2000, in dem auf eine außerordentliche Aufsichtsratssitzung des HKZD vom 27. September 2000 Bezug genommen wurde, mit einer entsprechenden Eingangsverfügung vom 21. September 2000 in den Geschäftsgang genommen und mit einem Aktenzeichen (3-7731.23-0379/83-11) versehen wurde. Schließlich waren der damalige Rektor der Klägerin genauso wie der damalige Staatsminister für Wissenschaft und Kunst auf Grund ihrer amtlichen Stellung geborene Mitglieder des Aufsichtsrats des HKZD, so dass von vornherein ein enger Zusammenhang zwischen amtlicher und im Aufsichtsrat eingenommener Stellung bestanden hatte.

28 2.3 Soweit schließlich die Prangerwirkung aus den Begleitumständen ihrer Behandlung in der Öffentlichkeit, insbesondere aus einem vom damaligen Sächsischen Datenschutzbeauftragten mit der Zeitung „Dresdner Morgenpost“ im Februar 2003 geführten und in anderen Zeitschriften verbreiteten Interview hergeleitet wird, sind diese nicht streitgegenständlich. Mit dem von der Klägerin begehrten Widerruf der Beanstandung könnte daher auch die durch diese Begleitumstände in der Öffentlichkeit möglicherweise verursachte Rufschädigung nicht beseitigt werden.

29 Nach alledem ist daher die Klage unzulässig.

30 Die Kostenentscheidung folgt aus § 154 Abs. 1 VwGO.

31 Die Revision war nicht zuzulassen, da ein Zulassungsgrund nach § 132 Abs. 2 VwGO nicht vorliegt.

Rechtsmittelbelehrung

Die Nichtzulassung der Revision kann durch Beschwerde angefochten werden.

Die Beschwerde ist beim Sächsischen Oberverwaltungsgericht, Ortenburg 9, 02625 Bautzen, innerhalb eines Monats nach Zustellung dieses Urteils einzulegen. Die Beschwerde muss das angefochtene Urteil bezeichnen.

Die Beschwerde ist innerhalb von zwei Monaten nach Zustellung dieses Urteils zu begründen. Die Begründung ist bei dem oben genannten Gericht einzureichen.

In der Begründung der Beschwerde muss die grundsätzliche Bedeutung der Rechtssache dargelegt oder die Entscheidung des Bundesverwaltungsgerichts, des Gemeinsamen Senats der Obersten Gerichtshöfe des Bundes oder des Bundesverfassungsgerichts, von der das Urteil abweicht, oder der Verfahrensmangel bezeichnet werden.

Für das Beschwerdeverfahren besteht Vertretungszwang; dies gilt auch für die Einlegung der Beschwerde und für die Begründung. Danach muss sich jeder Beteiligte durch einen Rechtsanwalt oder einen Rechtslehrer an einer staatlichen oder staatlich anerkannten Hochschule eines Mitgliedstaates der Europäischen Union, eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum oder der Schweiz, der die Befähigung zum Richteramt besitzt, als Bevollmächtigten vertreten lassen.

In Angelegenheiten, die ein gegenwärtiges oder früheres Beamten-, Richter-, Wehrpflicht-, Wehrdienst- oder Zivildienstverhältnis oder die Entstehung eines solchen Verhältnisses betreffen, in Personalvertretungsangelegenheiten und in Angelegenheiten, die in einem Zusammenhang mit einem gegenwärtigen oder früheren Arbeitsverhältnis von Arbeitnehmern im Sinne des § 5 des Arbeitsgerichtsgesetzes stehen, einschließlich Prüfungsangelegenheiten, sind auch Gewerkschaften und Vereinigungen von Arbeitgebern sowie Zusammenschlüsse solcher Verbände für ihre Mitglieder oder für andere Verbände oder Zusammenschlüsse mit vergleichbarer Ausrichtung und deren Mitglieder vertretungsbefugt. Vertretungsbefugt sind auch juristische Personen, deren Anteile sämtlich im wirtschaftlichen Eigentum einer dieser Organisationen stehen, wenn die juristische Person ausschließlich die Rechtsberatung und Prozessvertretung dieser Organisation und ihrer Mitglieder oder anderer Verbände oder Zusammenschlüsse mit vergleichbarer Ausrichtung und deren Mitglieder entsprechend deren Satzung durchführt, und wenn die Organisation für die Tätigkeit der Bevollmächtigten haftet. Diese Bevollmächtigten müssen durch Personen mit der Befähigung zum Richteramt handeln.

Behörden und juristische Personen des öffentlichen Rechts einschließlich der von ihnen zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse können sich durch eigene Beschäftigte mit Befähigung zum Richteramt oder durch Beschäftigte mit Befähigung zum Richteramt anderer Behörden oder juristischer Personen des öffentlichen Rechts einschließlich der von ihnen zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse vertreten lassen.

Ein Beteiligter, der zur Vertretung berechtigt ist, kann sich selbst vertreten.

gez.:
v. Welck Drehwald John

Beschluss

Der Streitwert wird für das Berufungsverfahren auf 5.000,00 € festgesetzt.

Gründe

1 Die Streitwertfestsetzung ergibt sich aus § 47, § 52 Abs. 2 GKG.

2 Dieser Beschluss ist unanfechtbar (§ 152 Abs. 1 VwGO).

gez.:
v. Welck Drehwald John

17.2.2 Aus der Stellungnahme des Sächsischen Datenschutzbeauftragten gegenüber dem BVerfG zu Verfassungsbeschwerden gegen das ELENA-Gesetz

Zu oben 10.2.1

17.2.2.1 Abweichende Auffassung des Sächsischen Datenschutzbeauftragten zur *Frage 1* des Gerichtes

[= „Genügt die Festlegung der von den Arbeitgebern an die Zentrale Speicherstelle zu übermittelnden Daten in § 97 Abs. 1 SGB IV den Anforderungen an das Gebot der Normenbestimmtheit und Normenklarheit?“]

„Abweichend hiervon ist der Sächsische Datenschutzbeauftragte der Auffassung, dass § 97 Abs. 1 Satz 1 bis 3 SGB IV *hinsichtlich des Umfanges der einzumeldenden und zu speichernden Daten* gegen das Gebot der Bestimmtheit und Klarheit von Gesetzen verstößt (in vielem übereinstimmend mit Abschnitt E II 1 [wohl Bl. 52 f. der Gerichtsakte] der Verfassungsbeschwerde 1 BvR 872/10), nachstehend (1) bis (5).

Andererseits hat der Sächsische Datenschutzbeauftragte unter dem Gesichtspunkt der Bestimmtheit und Klarheit nur eingeschränkt Bedenken gegen den für sich betrachteten § 97 Abs. 1 Satz 4 SGB IV (nachstehend [6]).

(1) Die verfassungsrechtlichen Bestimmtheitsanforderungen können für die Verarbeitung personenbezogener Daten durch und für ein *Register*, welches abstrakt, nämlich unabhängig von konkreter Erforderlichkeit für ein aufgrund individueller Entschließung in Gang gesetztes, eben konkretes Verwaltungsverfahren, also einzelanlasslos und *in diesem Sinne*[15] „*auf Vorrat*“, personenbezogene Daten sammelt, nur durch enumeratives Aufführen der Daten (Datensatz-Bestandteile) erfüllt werden.

Das bedeutet: In *diesem Falle* der Erteilung einer gesetzlichen Befugnis zur *vorsorglich anlasslosen* Erhebung reicht eine indirekte Bestimmung des Umfanges der im Gesetz erlaubten bzw. zu erlaubenden Verarbeitungsvorgänge durch mittels des Erforderlichkeits-Erfordernisses stattfindende Anknüpfung an die materiellen Leistungsanspruchsvoraussetzungen (das heißt an die aus dem betreffenden Leistungsgesetz ersichtlichen Voraussetzungen der beantragten bzw. möglicherweise zu beantragenden Sozialleistung), wie sie das Grundprinzip der Erhebungsbefugnis-Generalklausel des § 67a Abs. 1

[15] Nachstehend folgt der Text der in der Entscheidung des Gerichtes vom 2. März 2010 zur Telekommunikationsverkehrsdatenspeicherung verwendeten terminologischen Unterscheidung zwischen „***vorsorglich anlassloser***“ Verarbeitung und der Verarbeitung „***auf Vorrat*** zu unbestimmten“ und auch [sic.!] „noch nicht bestimmbaren Zwecken“ (Rdnr. 213 der Entscheidung), wonach die vorsorglich anlasslose Verarbeitung (offenbar als Oberbegriff gemeint!) einen festgelegten Zweckbezug aufweisen *kann* und in *diesem Falle, also wenn sie dies tut,* keine Verarbeitung ohne (festgelegten) Zweckbezug und damit keine Verarbeitung „auf Vorrat“ ist (welch letztere ausnahmslos verfassungswidrig ist).
Kritisch dazu und mit abweichender Terminologie Klesczewski (Urteilsanmerkung) JZ 2010, 629.

Satz 1 SGB X ist (deren hinreichende Bestimmtheit nicht bestritten ist und nicht bestritten werden soll), *nicht* aus.

(2.1) Dass die Maßstäbe der Bestimmtheit und Klarheit von Verfassungs wegen in dieser Weise unterschiedlich sein müssen, dass also bei der Verarbeitung personenbezogener Daten zu abstrakten, noch nicht konkreten („vorsorglich anlasslos"), wenn auch inhaltlich festgelegten Zwecken (und daher nach der Telekommunikationsverkehrsdaten-Entscheidung[16] des Bundesverfassungsgerichts nicht grundsätzlich verfassungswidrig) für den Datensatz (die Erhebungsmerkmale) eine Aufzählungs-Pflicht besteht, ergibt sich zunächst schon aus der Beobachtung der gesetzgeberischen Praxis: Durchweg sind diejenigen Gesetze, die eben *einzelanlasslos vorsorglich* die Sammlung von Daten in *Registern* vorschreiben, in enumerativer Nennung der Daten ausgestaltet und versuchen nicht, die Daten lediglich dadurch zu bestimmen, dass sie mittels einer aus dem Register-Zweck sich ableitende Erforderlichkeit an eine aus anderen gesetzlichen Vorschriften sich ergebende Erforderlichkeit für die Erledigung einer primären Verwaltungsaufgabe (Treffen einer Einzel-Entscheidung) anknüpfen.

Dies gilt über die oben zur Begründung der Auffassung des Bayerischen Datenschutzbeauftragten genannten fünf Beispiele* hinaus etwa für das
- Einwohnermelderegister, das
- Verkehrszentralregister nach § 28 (Abs. 3!) StVG, das
- Gewerbezentralregister nach § 149 GewO, die
- Krebsregister nach den diesbezüglichen Landesgesetzen (zeitweilig auch nach einem diesbezüglichen Bundesgesetz) und das
- Ausländerzentralregister nach § 3 AZRG,

außerdem auch für zivilrechtsnahe Register wie das Handelsregister und das Vereinsregister, aber auch für das eine gewisse Ähnlichkeit mit der Unterhaltung von Registern aufweisende, seiner Natur nach (einzel-)anlasslose und in einem gewissen Sinne auch vorsorgliche[17] Verarbeitung personenbezogener Daten regelnde *Statistikrecht*; und zwar durchaus auch bei bloßen Sekundärstatistiken (Statistiken im Verwaltungsvollzug) - dabei sind Beispiele aus der Sozialleistungsstatistik

- die Sozialhilfestatistik, § 122 SGB XII,
- die Jugendhilfestatistik, § 99 SGB VIII,
- die Wohngeldstatistik, § 35 WoGG, und
- die BAföG-Statistik, § 55 BAföG;

[16] Rdnr. 213.
* § 24c KWG, §§ 3 ff. BZRG, § 3 ATDG, § 113a TKG [insoweit vom BVerfG nicht beanstandet], Art. 85a BayEUG.

[17] Die genauen Auswertungs-Zwecke stehen zum Zeitpunkt des Erlasses der Norm, aber auch zum Zeitpunkt der Zusammenstellung der Datensätze, die dann zu Auswertungen genutzt werden können, ja noch nicht fest.

- § 52 SGB II ist wegen der Genauigkeit des § 51b SGB II kein Gegenbeispiel.

Vor allem gilt dies aber bei allen Primärstatistiken, bei denen dies durchweg Standard ist, wie das Beispiel des Zensusgesetzes 2011 in § 3 Abs. 1 und 2, § 4, § 5, § 6 und § 7 Abs. 4 zeigt (vgl. ferner etwa das Agrarstatistikgesetz in der Fassung der Neubekanntmachung vom 17. Dezember 2009, BGBl. I S. 3886, passim[18]).

(2.2) Bei der ELENA-Datensammlung handelt es sich in diesem Sinne um ein Register (und um eine *vorsorglich anlasslose* Verarbeitung personenbezogener Daten).

(2.3) Dabei ist das, was nach § 97 Abs. 1 Satz 1 bis 4 SGB IV gemeldet werden soll, *der Gesetzesformulierung nach* über die Erforderlichkeit an in genannten Leistungsgesetzen abstrakt festgelegte Voraussetzungen von Sozialleistungen geknüpft, soll sich also daraus ableiten lassen. Das reicht aber gewissermaßen schon aus System-Gründen für die nötige Bestimmtheit nicht aus. Denn der Datensatz ist schon wegen der zeitlichen Ausdehnung seiner regelmäßig in monatlichen Abständen erfolgenden Übermittlung, Erhebung und der daran anschließenden längerdauernden Speicherung in starkem Maße von diesen Voraussetzungen abgelöst: Die einzelnen Sozialleistungsgesetze sind der (sehr wahrscheinlichen) Möglichkeit einer jederzeitigen Änderung (der Leistungsvoraussetzungen) unterworfen; das Register ist aber von dem wechselnden Inhalt der betreffenden Leistungsgesetze hinsichtlich der Leistungsvoraussetzungen insoweit abgekoppelt, als es zumindest in puncto Speicherung (vgl. § 99 Abs. 4 SGB IV) zeitlich kontinuierlich, d. h. inhaltlich unverändert, über Gesetzesänderungen hinweg betrieben wird, da das Gesetz vielleicht noch den einzumeldenden, zumindest aber den zu speichernden Datensatz nicht in verweisender Abhängigkeit von Leistungsgesetzen in jederzeitiger, ipso iure eintretender Akzessorietät gestaltet, sondern diesen fest, eben ‚abstrakt', bestimmt.

Es handelt sich, was den Datensatz angeht, mithin um ein zumindest hinsichtlich der Speicherung nicht-dynamisiertes Register. Sofern darin kein Verstoß gegen den Bestimmtheitsgrundsatz läge, liegt darin jedenfalls ein Verstoß gegen das Gebot der Erforderlichkeit und der Geeignetheit.

(3) Konkret ergibt sich die mangelnde Bestimmtheit aus Folgendem:

(3.1) Dass Gesetz versucht, den Umfang des registermäßigen, *vorsorglich (einzel-)anlasslos* stattfindenden Sammelns des Datenbestandes durch Anknüpfen an Leistungsgesetze zu bestimmen, vermittelt durch in diesen Leistungsgesetzen ausgesprochene Bescheinigungs- bzw. Auskunftspflichten, die ihrerseits eben Angaben zu Leistungs-

[18] Vgl. zur Problematik ferner 9/5.7.2 unter (3) (a) und (d).

voraussetzungen zum Inhalt haben. Dieser Anknüpfung lassen sich die Erhebungsmerkmale nicht mit der nötigen Bestimmtheit entnehmen, lässt sich also mit der nötigen Bestimmtheit nicht entnehmen, welcher Datensatz genau benötigt wird. Das erhellt weitgehend schon aus der *Misch-Technik* des Gesetzes. Diese lässt nämlich darauf schließen, dass der parlamentarische Gesetzgeber (wie natürlich vorher schon der ministerielle Entwurfsverfasser) sich selbst nicht zugetraut hat, die Datensatzbestandteile (die Erhebungs-Merkmale, statistisch gesprochen: das Erhebungs-Programm) vollständig zu nennen: In Satz 1 des § 97 Abs. 1 SGB IV versucht der Gesetzgeber es mit der allgemeinen Anknüpfung über die Erforderlichkeit an die in § 95 Abs. 1 SGB IV genannten Gesetze, in Satz 2 gibt er erklärtermaßen rudimentär („insbesondere“) an, um welche Daten es sich folglich mindestens handele, in Satz 3 formuliert er vorsorglich - fast schon widersprüchlich dazu - ein Verbot, mehr als das Erforderliche zu verarbeiten - was abschließend aufzuzählen er sich aber selbst eben offenbar nicht in der Lage sieht (ein anderer Grund für das Unterlassen ist nicht erkennbar).

(3.2) Bestätigt wird dieser Eindruck, den der Gesetzestext vermittelt, dadurch, dass die *Gesetzesbegründung* einen zusätzlichen Katalog an Datensatzbestandteilen enthält, den sie aber unter den Vorbehalt dessen stellt, was nach den speziellen Leistungsgesetzen tatsächlich erforderlich ist, und der zusätzlich als bloßer Mindest-Angabenkatalog bezeichnet wird.

Ferner wird dieser Eindruck dadurch bestätigt, dass die *Gesetzesbegründung* angibt, „im übrigen“, nämlich ergänzend zu dem, was sich aus § 97 Abs. 1 SGB IV als „Datenkatalog“, also Datensatz, ableiten lasse, gehe das, was an Daten zu übermitteln sei, aus § 28a Abs. 3 SGB IV hervor. Denn mit dem Wort „Bestimmung“ wird dort der Eindruck erweckt, § 28a Abs. 3 SGB IV leiste einen abschließenden ergänzenden Beitrag zur hinreichenden Bestimmung des Datensatzes. Das ist jedoch, soweit ersichtlich, irreführend. Denn die Einmeldungen in das ELENA-Register, die in § 28a Abs. 1 Satz 2 für den Fall der dort in Satz 1 genannten Ereignisse mit dem in Absatz 3 Satz 1 und 2 bestimmten Inhalt offenbar vorgeschrieben werden (immerhin mit bis auf die durch das „insbesondere“ in Absatz 3 Satz 1 ausgedrückte Einschränkung vollständiger Aufzählung), kommen allem Anschein nach zu denjenigen nach § 97 Abs. 1 Satz 1 und 2 SGB IV hinzu. (Allerdings erweckt die *Begründung* zu § 28 Abs. 1 Satz 2 SGB IV den Eindruck, es würden durch diese Vorschrift gar keine Meldungen an das ELENA-Register vorgeschrieben, sondern nur Modalitäten für die Erfüllung der sich - namentlich inhaltlich - aus § 97 Abs. 1 SGB IV ergebenen Meldepflichten. Die Gesetzesbegründung als Ganzes erscheint insoweit als widersprüchlich.)

(4) Absatz 6 des § 97 SGB IV ist der Versuch, die Aufgabe der Herstellung der hinreichenden Bestimmtheit in die Zukunft zu verlegen und auf die Exekutive zu über-

tragen: Die Auseinandersetzungen, die es Anfang 2010 (vgl. *Anlagen*) über dasjenige gegeben hat, was als Inhalt dieser Verordnung festzulegen sei[19], die diesbezüglichen Unsicherheiten bei den für die Erarbeitung der Verordnung und der konkreten Datensatzvorgaben für die Arbeitgeber maßgeblichen Stellen[20] und die in der Verfassungsbeschwerde 1 BvR 872/10 mit Schriftsatz vom 11. Mai dazu (unter I 1, Bl. 80 der Gerichtsakte) geäußerte Kritik zeigen jedoch, dass der Gesetzgeber bei Schaffung des Gesetzes gerade nicht mit der für die von ihm von Verfassungs wegen vorzunehmende Beurteilung (Grundrechts-Abwägung; Zusammenhang mit *Frage zwei, Teil d*) erforderlichen Genauigkeit konkret übersehen hat, was der Datensatz alles für Merkmale werde umfassen müssen und welchen Grad an Schutzwürdigkeit manche dieser Datensatzbestandteile haben würden.

In diesem Zusammenhang ist es auch bemerkenswert, dass die *Gesetzesbegründung* zu § 97 zu Unrecht behauptet, das Verhältnis der ELENA-DV (nach § 97 Abs. 6 SGB IV) zur gesetzlichen Bestimmung des Umfanges der Einmeldung in das ELENA-Register in § 97 Abs. 1 Satz 1 und 2, Satz 4 SGB IV sei wie dasjenige der DEÜV zu § 28a SGB IV. Das ist unzutreffend: Im Falle des § 28a SGB IV steht der Datensatz im Wesentlichen im Gesetz, die DEÜV ergänzt nur, im Falle der ELENA-DV ist es genau umgekehrt; von der Anwendung einer bewährten *Regelungstechnik*, wie sie die *Begründung* sinngemäß behauptet, kann also keine Rede sein.

(5.1) Die zur Begründung der Auffassung des Bayerischen Datenschutzbeauftragten durchgeführte genauere Untersuchung der aus der Verweisungstechnik des § 97 Abs. 1 Satz 1 SGB IV zu ziehenden Schlussfolgerungen auf den einzumeldenden Datensatz zeigt in den Beispielen 1, 3 und 5 konkret, dass die Ermittlung dessen, was vom Gesetzgeber an Datenübermittlung und -speicherung gewollt ist, zum Teil so schwierig und unsicher ist, dass es an der nötigen Bestimmtheit und Klarheit (Übersichtlichkeit) fehlt, wie sie im Volkszählungsurteil für zum Teil eindeutig weniger schutzbedürftige Daten verlangt worden ist. Namentlich der Umstand, dass in Vorschriften des Sozialgesetzbuchs Drittes Buch, auf die Bezug genommen wird, im Falle des § 94 Abs. 1 Nr. 1 und Nr. 3 auch dort nur mit der „Insbesondere“-Technik gearbeitet und in allen drei Fällen die Konkretisierung des Datensatzes im Gesetz auf die Ebene der behördlichen Vordrucks-Gestaltung verschoben wird, zeigt das Bestimmtheits-Defizit. Dessen Auswirkungen werden durch die Elektronisierung (Automatisierung) der Verarbeitung, die das ELENA-Verfahren mit sich bringt, gegenüber der bisherigen Rechtslage grundrechtseingreifend verstärkt (vgl. Volkszählungsurteil).

[19] Vgl. ferner dazu in der Beschwerdeschrift zu 1 BvR 332/10 S. 31, Bl. 32 der Gerichtsakte, und S. 45, Bl. 46 der Gerichtsakte, mit einem Zitat einer insoweit geradezu entlarvenden Presseerklärung.
[20] Vgl. § 28b Abs. 6 SGB IV. Diese Unsicherheiten gehen im Einzelnen aus mehreren Rundschreiben hervor, die der BfDI seinerzeit an die Landesbeauftragten für den Datenschutz geschickt hat.

(5.2) Überdies ist der konkrete Datenbedarf im Einzelnen auch noch von der Entwicklung der Sozialrechtsprechung abhängig, Anschauungsbeispiele dazu bei Panzer, Sozialversicherungsrechtliche Auswirkungen der Beendigung von Arbeitsverhältnissen, NJW 2010, 11.

(5.3) Dass der Gesetzgeber keine genaue Übersicht über den Datenbedarf (Datensatz) hat, zeigt sich auch in der Unbestimmtheit der Löschungsvorschriften (siehe dazu unten in der Antwort auf *Frage drei* in Abschnitt 2.3; vgl. demgegenüber etwa § 29 StVG).

(5.4) Ergebnis: Der genaue Datenbedarf, wie er über die Anknüpfung an das für die jeweiligen Verwaltungsverfahren Erforderliche dem Erscheinungsbild des Gesetzes nach zunächst bestimmt erscheint, ist bei genauerem Hinsehen nicht sicher feststellbar, zumindest nicht zu überblicken (Verletzung des Klarheits-Gebotes).

(6) Der Sächsische Datenschutzbeauftragte hat unter dem Gesichtspunkt der Bestimmtheit nur eingeschränkt Bedenken gegen den für sich betrachteten § 97 Abs. 1 Satz 4 SGB IV: Die Vorschrift ist seiner Auffassung nach nur potenziell unbestimmt, und zwar aus folgenden Gründen:

Hinsichtlich des Umfanges (des Datensatzes) der dem Arbeitgeber vorgeschriebenen Einmeldung in das ELENA-Register bewirkt die Vorschrift keine Steigerung der Unbestimmtheit bzw. Unklarheit. Zwar beschränkt sie diesen Umfang nicht auf „die Meldung zu den erfassten Nachweisen“, also auf den mit der (kalender-)monatlichen Periodizität nach Absatz 1 Satz 1 zu meldenden Datensatz (welchen Umfang dieser auch immer genau hat); denn sie verweist hinsichtlich des Umfanges des Datensatzes auf diejenigen Normen, die den Arbeitgeber zu solchen ‚Sonder-Meldungen’ (außer der Reihe) verpflichten. Aber sie knüpft damit an - bestehende oder noch nicht bestehende[21] - Vorschriften (§ 28a SGB IV? Der Gesetzesbegründung ist dazu nichts zu entnehmen) an, die den Arbeitgeber etwa dazu verpflichten, aufgrund besonderer Umstände eine sozusagen ‚außerordentliche’ Meldung zu machen - die, mit einem möglicherweise atypischen Datensatz - in das ELENA-Register eingestellt werden soll.

Der Bestimmtheits- und Klarheits-Grad der Vorschrift (des Satzes 4) ist daher genau akzessorisch denjenigen Normen, die den Arbeitgeber zu der ‚Sonder-Meldung’ verpflichten. Solange über diese Vorschrift nichts Näheres bekannt ist, lässt sich der Bestimmtheits- und Klarheitsgrad nicht beurteilen. Wird die Norm nur an und für sich betrachtet, ist sie nicht unbestimmt.

[21] Auffällig das leicht futurische „kann […] werden“ in der *Gesetzesbegründung.*

Die aus dem Gesamtkomplex von Satz 1 bis 3 (auch i. V. m. § 95 Abs. 1 SGB IV) hervorgehende Unbestimmtheit ist dem Satz 4 für sich genommen nicht eigen. Er ist daher nur potenziell, nicht schon aktuell unbestimmt."

17.2.2.2 Ergänzungen des Sächsischen Datenschutzbeauftragten zur *Frage 2d* des Gerichtes, betreffend die *Angemessenheit*

[„Zu den Anforderungen an die Verhältnismäßigkeit der Datenübermittlung durch den Arbeitgeber und der Speicherung der übermittelten Daten durch die Zentrale Speicherstelle: Welches Gewicht hat die zentrale Zusammenführung der Daten? Sind die monatliche Datenübermittlung und die anschließende Datenspeicherung im Hinblick auf die damit verfolgten Ziele angemessen?"]

„Der Sächsische Datenschutzbeauftragte teilt die dargestellte Auffassung des Bayerischen LfD zu *Frage 2* mit Ausnahme der Erwartung konkret verhaltensbeeinflussender Einschüchterungseffekte und macht unabhängig von der Frage, inwieweit überhaupt die Erreichung von auf Kosten des Grundrechts auf informationelle Selbstbestimmung verfolgten Gemeinwohlinteressen, das heißt ein Nutzensaldo in außerdatenschutzrechtlicher Hinsicht, erkennbar und dafür das zentrale ELENA-Register erforderlich (das mildeste Mittel) ist, *ergänzend* geltend, dass in keiner Weise ersichtlich ist, dass das ELENA-Verfahren zur Zeit, aber auch in einer möglich erscheinenden (und angekündigten) Ausbaustufe (auf viele weitere Bescheinigungs-Arten), einen Grad an Nutzung der angemeldeten und gespeicherten Datensätze erreichen wird, der die *Angemessenheit* des mit ELENA verbundenen Grundrechtseingriffes erkennen lässt.

Dem liegen folgende Überlegungen zugrunde:

(1) Ein Gewinn für das Grundrecht auf informationelle Selbstbestimmung ist in die Abwägung kaum einzustellen. Denn der datenschutzrechtliche Vorteil durch das Entfallen einer Kenntnis des Arbeitgebers von einem spezifizierten Bescheinigungsbedarf ist recht gering: In Großunternehmen sind die Verhältnisse anonym, und ein Datenaustausch zwischen Personalabteilung und Fach-Vorgesetzten oder Fach-Kollegen findet mangels Zulässigkeit so gut wie nicht statt; in kleinen Unternehmen sind ohnehin die sozialrechtlich relevanten persönlichen Verhältnisse aufgrund des persönlichen Miteinanders im Betrieb weitgehend bekannt.

Dieser geringfügige Gewinn wird wohl aufgewogen durch die zusätzlichen Belastungen des Grundrechtes durch das Anfallen zusätzlicher Daten beim Arbeitgeber, auf das die Verfassungsbeschwerde 1 BvR 332/10 auf S. 62 unten zu Recht hinweist.

(2) Die Gesetzes-Initiatorin, die Bundesregierung, hat nach jahrelangen aufwendigen Vorbereitungen noch bei der Einbringung in das Gesetzgebungsverfahren in keiner Weise Überlegungen dazu erkennen lassen, wie hoch der *Nutzungsgrad* der vorsorglich anlasslosen Verarbeitung personenbezogener Daten durch Betreiben des ELENA-Registers überhaupt sein würde.

Die Bundesregierung hat lediglich nach diesbezüglicher Kritik des Bundesrates (Stellungnahme vom 19. September 2008, BR-Drs.: 561/08, Nr. 5 bis 7; s. auch Anlage 3 zur BT-Drs.: 16/10492) in ihrer „Gegenäußerung" (BT-Drs.: 16/10492, Anlage 4, vom 17. Oktober 2008)

> „eine hinreichend hohe Wahrscheinlichkeit, dass für die meisten Beschäftigten einmal eine Bescheinigung nach dem Dritten Buch des Sozialgesetzbuches - Arbeitsförderung - (SGB III), dem Wohngeld-Gesetz (WoGG) oder dem Bundeselterngeld- und Elternzeitgesetz (BEEG) auszustellen sein wird",

behauptet und dabei erstmals - wie die Verfassungsbeschwerde 1 BvR 332/10 auf S. 41 mit Recht hervorhebt - bestimmte jährliche Absolutzahlen für die einzelnen von § 95 Abs. 1 SGB IV erfassten Bescheinigungsarten angegeben und die Erhöhung des Nutzungsgrades durch Erweiterung auf andere Bescheinigungs-Arten ab 2015 ins Feld geführt.

Damit fehlt jedoch im Gesetzgebungsverfahren jedes erkennbare Bemühen, ein *Zahlenverhältnis* zwischen den dafür genutzten und der Gesamtanzahl der einzelnen Einmeldungen (also der vor allem monatlichen Datensätze) herzustellen.

Darin liegt ein Fehler bei der Ausübung des gesetzgeberischen Ermessens[22], nämlich ein *Abwägungsdefizit*.

Da, wo die Abwägung anhand schätzbarer Zahlenwerte vorgenommen werden kann, also die Präferenz-Entscheidung damit erleichtert[23] wird, wird vom Gesetzgeber eine vollständige Proportionalitätsschätzung zu verlangen sein.

(3) Auch nach der zu vermutenden *tatsächlichen* Relation zwischen der Anzahl der eingemeldeten Datensätze und der Anzahl der Bescheinigungen erscheint der durch die vorgeschriebene Anmeldung und Speicherung bewirkte Grundrechtseingriff als unangemessen.

[22] Vgl. BVerfGE 81, 70 ff., 90 f.
K. Stern spricht Staatsrecht III/II S. 783 von einer *Pflicht* (Last? wörtlich „Zwang") des Gesetzgebers, den Freiheitseingriff zu *begründen* und zu *rechtfertigen.*

[23] Im Normalfall fehlen solche Zahlen-Stützen. Zu den Schwierigkeiten einer ansatzweise quantifizierenden Darstellung von Grundrechtsabwägungen s. Jansen, Die Abwägung von Grundrechten, Der Staat 36 (1997), 27 ff.

Die diesbezüglichen Berechnungen in der Verfassungsbeschwerde 1 BvR 332/10 auf S. 42 erscheinen als plausibel, und zwar auch darin, dass sie den Anteil der genutzten Daten, mit 10 %, als halb so hoch einschätzen wie den Anteil der genutzten Datensätze (20 %). Auf Letzteres kommt es an: Im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung ist nicht auf die Anzahl der Datensätze abzustellen, sondern auf die einzelnen Datensatz-Bestandteile (einzelne Daten, womit vom Grad der Schutzwürdigkeit der einzelnen Datensatz-Bestandteile noch ganz abgesehen ist); das hebt auch die (Sammel-)Stellungnahme des Bayerischen Landesdatenschutzbeauftragten am Schluss des Abschnittes 1.2 zu Recht hervor.

(4) Für die Beurteilung der verfassungsrechtlichen Angemessenheit des Betreibens eines solchen Registers mit personenbezogenen Daten ist eine solche Prüfung zwar nicht der einzige in die Abwägung einzubeziehende Gesichtspunkt, aber ein unentbehrlicher.

(5) Es liegt nahe, die Angemessenheit solcher Register *abgestuft* zu beurteilen:

(5.1) An die Höhe des Nutzungsgrades werden sicherlich dann, wenn die personenbezogenen Daten (*als geeignet und erforderlich*) für die Erreichung wichtiger Belange wie Gefahrenabwehr oder auch Strafverfolgung, wie etwa

- mit Totalerfassung
  - im Falle des Verkehrszentralregisters (in dem die Speicherung der bloßen Zulassung als solche noch uneingeschränkt vorsorglich anlasslos ist),
  - bei nach der Entscheidung des Gerichtes vom 2. März 2010 verfassungsgemäßer Ausgestaltung auch im Falle einer vorsorglich anlasslosen sechsmonatigen Speicherung von Telekommunikationsverkehrsdaten,
  - im Falle der in vielen Bundesländern geltenden Gesetze zur Überwachung der Teilnahme von Kindern an den Früherkennungsuntersuchungen, z. B. das Sächsische Kindergesundheits- und Kinderschutzgesetz vom 11. Juni 2010, GVBl. S. 182[24], oder

[24] Zur unter dem hier interessierenden Gesichtspunkt im Wesentlichen inhaltsgleichen Vorgängerregelung des Sächsischen Kindergesundheits- und Kinderschutzgesetzes vom 19. Juni 2009, GVBl. S. 379 kritisch 14/10.2 (2009), zur *Angemessenheit* unter E 4.3 und 4.4, S. 123 ff.
Vgl. dort auch in Abschnitt d, S. 131 f. zur Kritik an der Entscheidung des Verfassungsgerichtshofes Rheinland-Pfalz - VGH B 45/08 - vom 28. Mai 2009, die der anlasslosen Totalerfassung durch das dortige Kinderschutzgesetz die verfassungsrechtliche *Angemessenheit* bescheinigt hat. Inzwischen hat sich herausgestellt, dass in Rheinland-Pfalz im Jahre 2009 rund 258.000 Datensätze verarbeitet worden sind, dabei 26.435 Meldungen über nicht bestätigte oder nicht wahrgenommene Früherkennungsuntersuchungen verarbeitet worden sind und durch Nutzung dieser Daten lediglich in sechs Fällen eine Kindeswohlgefährdung aufgedeckt worden ist, die den Jugendämtern nicht ohnehin, also ohne das Betreiben des betreffenden Registers, d. h. der Überwachung der Teilnahme an den Früherkennungsuntersuchungen, bekanntgeworden ist. Der Nutzungsgrad bzw. die Trefferquote liegt demnach bei ‚brutto' reichlich 0,002 %, zuzüglich der möglicherweise eingetretenen günstigen Wirkung einer Erhöhung der Teilnahmequote, und bei reichlich 0,02 % bei den abstrakten 26.435 Verdachtsfällen, vgl. den Bericht des Institut für Sozialpädagogische Forschung Mainz e. V. (ism) „Kinderschutz und Kindergesundheit in Rheinland-Pfalz. Ergebnisse zur Umsetzung des Landesgesetzes zum Schutz von Kindeswohl und Kindergesundheit für das Berichtsjahr 2009", vom November 2010, S. 15 und S. 36, abrufbar unter http://www.masgff.rlp.de/aktuelles/; das genannte Institut hat die URL www.ism-mainz.de.
Vgl. zu der Problematik auch Bartels und Altenkirch JZ 2009, 991, 994 f.

- Regelanfragen betreffend Zuverlässigkeitsvoraussetzungen, als Verwaltungspraxis
- mit zufälliger, einzelanlassloser *Stichprobe*
- im Falle der Ermächtigung zu sogenannter *Schleierfahndung* im Polizeirecht

verarbeitet werden, *vergleichsweise* geringe Anforderungen zu stellen sein.

(5.2) Für Systeme einzelanlassloser Verarbeitung personenbezogener Daten zur Aufdeckung des Sozialleistungsmissbrauches (Sozialleistungs-Betruges) bzw. der Steuerhinterziehung durch Abgleichserlaubnisse[25] bzw. -gebote oder Regelanfragen[26], dürfte ein ähnlicher, aber eher höher (weil strafrechtlich gesehen nur Vermögensdelikte betreffend) liegender Nutzungs- bzw. Treffergrad für die Angemessenheit erforderlich sein.

(5.3) Demgegenüber werden wesentlich höhere Anforderungen an den Nutzungs- bzw. Treffergrad eines Registers zu stellen sein, das wie das ELENA-Register nur der Verwaltungsvereinfachung, also im Wesentlichen nur einer Kostenersparnis für Verwaltungsabläufe dient (und eben nicht die Sicherstellung der Einhaltung und Befolgung der Rechtsordnung zu fördern bestimmt ist oder dafür nützlich wäre).

Das Register ist ja nicht für die Erstellung der Bescheinigungen, also, wie es in den beiden zur *Totalerfassung* zuerst genannten Fallgruppen der Fall ist, für die Erreichung des Verwaltungszweckes, erforderlich, sondern lediglich für die - überdies zumindest nicht gerade exorbitante - kostenmäßige Erleichterung der Erreichung des Verwaltungszweckes.

(6) Gesichtspunkte eines mit der Datensammlung verbundenen (Eindruckes eines) Generalverdachtes oder eines konkretisierten generalisierenden Verdachtes (möglicherweise verbunden mit sogenannter Stigmatisierung, z. B. Fingerabdruck- oder DNS-Register[27]) spielen meiner Auffassung nach im vorliegenden Fall (für die Beurteilung der Angemessenheit) keine Rolle: Die Aufnahme in das Register ist insoweit belastungsfrei.

(7) Man kann sich des Verdachtes nicht unbedingt erwehren, dass das System des ELENA-Verfahrens als technikbegeistertes, der Verbreitung von IT-Technik in der Masse der Bevölkerung dienendes, nämlich die massenweise Benutzung der elektronischen Signatur durchsetzendes, ja aufzwingendes Prestige-Vorhaben mit großem, lang-

[25] Z.B. § 118 SGB XII, § 41 Abs. 4 BAföG. Noch stärker wirken Kontrollmitteilungs-Vorschriften.

[26] Anfang der 90er Jahre ist - zur Beurteilung einer Verwaltungspraxis, die nicht nur rein finanzielle Sachverhalte zu prüfen hatte - zu überlegen gewesen, ob es angemessen sei, wegen einer bei Stichproben ermittelten Trefferquote von 6 bis 8 v. H. für Fälle nach den *Rehabilitierungsgesetzen* im Hinblick auf die in diesen enthaltenen (aus dem Lastenausgleichsrecht übernommenen) Ausschlussgründe eine Regelanfrage beim BStU durchzuführen. Ganz ähnlich ist die ausweislich des FOCUS vom 27. Mai 2008 im Hinblick auf eine ähnlich hohe Trefferquote zunächst nur von Bayern durchgeführte Regelanfrage beim BStU im Hinblick auf Entscheidungen über Anträge auf Zuwendungen (Renten) wegen aus politischen Gründen in der DDR erlittener Haft zu sehen.

[27] Interessant in dieser Hinsicht die Datennutzung für die Fahndungsmethode des „familial searching“ nach britischem Recht (von der Strafprozessordnung offenbar nicht erlaubt), FAZ vom 21. Januar 2011.

jährigem Vorbereitungsaufwand betrieben worden ist, und zwar dergestalt, dass am Ende den Initiatoren genauere, nämlich aussagekräftige Zahlenberechnungen einbeziehende Abwägungsüberlegungen bei der Einbringung des Gesetzes als der Überzeugungskraft des Vorhabens eher abträglich erschienen wären und die Nennung solcher Berechnungen zur Vermeidung eines Abbruches des Unternehmens unterlassen worden sein könnte.“

17.2.3 Verpflichtung auf das Meldegeheimnis

Dienststelle:

Verpflichtung auf das Meldegeheimnis

nach § 9 Abs. 1 des Sächsischen Meldegesetzes (SächsMG) i. d. F. der Bekanntmachung vom 4. Juli 2006 (GVBl. 2006, S. 388 Fsn-Nr.: 26-4); Fassung gültig ab: 1. Januar 2009.

Frau/Herr ……

wird nach vorheriger Unterrichtung gemäß § 9 Abs. 2 SächsMG wie folgt auf die Wahrung des Meldegeheimnisses sowie die sonstigen bei seiner/ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz verpflichtet:

Es ist mir untersagt, personenbezogene Daten ohne entsprechende Befugnis, die sich nach § 4 Abs. 1 SächsMG nur aus einer Rechtsvorschrift (u. a. Gesetz, Rechtsverordnung, Satzung) oder der Einwilligung des Betroffenen ergeben kann, zu verarbeiten, d. h. zu erheben, zu speichern, zu verändern, zu anonymisieren, zu übermitteln, zu nutzen, zu sperren, zu löschen oder sonst zu verwenden.

Hinweise: Die Verpflichtung auf das Meldegeheimnis besteht nach der Beendigung Ihrer Tätigkeit dauerhaft fort.

Aus einer Verletzung des Meldegeheimnisses ergeben sich für Sie dienst-, arbeits-, ordnungswidrigkeiten- oder strafrechtliche Konsequenzen. So kann die unbefugte Verarbeitung personenbezogener Daten nach § 38 SächsDSG mit einer Geldbuße bis zu 25.000 Euro oder nach § 39 SächsDSG als Straftat mit bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe geahndet werden. Unberührt davon bleibt eine mögliche Ahndung nach den §§ 133, 203, 204, 331, 332 oder 353b StGB mit Freiheits- oder Geldstrafe.

Sonstige bei Ihrer Tätigkeit zu beachtende Vorschriften sind insbesondere die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes nach § 9 SächsDSG.

Bereichsspezifisch (z. B. dem Beamtenrecht, Tarifrecht) geregelte Verschwiegenheitspflichten bleiben unberührt.

Ein Exemplar dieser Verpflichtungsurkunde sowie das Merkblatt mit Erläuterungen und dem Text des § 9 SächsMG und der §§ 38, 39 SächsDSG sind ausgehändigt worden.

(Ort) (Datum)

(Unterschrift des Verpflichteten) (Unterschrift des Verpflichtenden)

17.2.4 Merkblatt zur Verpflichtung auf das Meldegeheimnis nach § 9 Abs. 2 Sächsisches Meldegesetz

1. Was versteht man unter der „Verpflichtung auf das Meldegeheimnis“?

Die **Verpflichtung** auf das Meldegeheimnis nach § 9 Abs. 2 SächsMG ist ein förmlicher Akt zu Beginn des Dienst-, Arbeits- oder Auftragsverhältnisses. Sie wird durch den Leiter der öffentlichen Stelle, den Arbeitgeber oder jeweils einen Beauftragten durchgeführt. Sie schließt die wichtige vorhergehende Unterrichtung des Bediensteten oder des Auftragnehmers über das Meldegeheimnis nach § 9 Abs. 1 SächsMG „sowie die sonstigen bei (seiner) Tätigkeit zu beachtenden Vorschriften über den Datenschutz“ ab und hat schriftlich bei Dienstantritt zu erfolgen. Die Urkunde ist in der Personalakte zu verwahren. Bei Arbeitnehmern reicht es nicht aus, eine entsprechende Klausel in den Arbeitsvertrag aufzunehmen. Der Verpflichtungsakt ist nach dem Gesetz durchzuführen. Das Meldegeheimnis gilt auch dann, wenn nicht oder mangelhaft verpflichtet wurde.

Die vorhergehende **Unterrichtung** des Bediensteten sollte durch eine geeignete Person vorgenommen werden. Dies kann der Datenschutzbeauftragte nach § 11 SächsDSG sein. Das Meldegeheimnis ist das Verbot der Verarbeitung personenbezogener Daten ohne entsprechende Befugnis, die sich nach § 4 Abs. 1 SächsMG nur aus einer Rechtsvorschrift (u. a. Gesetz, Rechtsverordnung, Satzung) oder der Einwilligung des Betroffenen ergeben kann. Bei der Unterrichtung sind zumindest dieser Grundsatz der Verarbeitung personenbezogener Daten (Verbot mit Erlaubnisvorbehalt) sowie die sich aus einer Verletzung ergebenden dienst-, arbeits-, ordnungswidrigkeiten- oder strafrechtlichen Konsequenzen eingehend zu erörtern. Wünschenswert ist die Erläuterung der für den konkreten Beschäftigten geltenden spezifischen Rechtsgrundlagen der Datenverarbeitung (z. B. Allgemeine Bestimmungen §§ 4 ff. SächsMG; Schutzrechte des Betroffenen §§ 22 ff. SächsMG). „Sonstige bei ihrer Tätigkeit zu beachtende Vorschriften“ sind die Vorschriften des Sächsischen Datenschutzgesetzes.

2. Wer muss auf das Meldegeheimnis verpflichtet werden?

Die Formulierung: „Wer bei einer Meldebehörde oder einer Stelle, die im Auftrag der Meldebehörde handelt, beschäftigt ist“ umfasst sämtliche Bedienstete einer Meldebehörde (§ 2 Abs. 1 SächsMG, § 4a Abs. 1 Satz 2 SAKDG) und sämtliche Mitarbeiter eines Auftragnehmers nach § 7 Abs. 1 SächsDSG, die Zugang zu personenbezogenen Daten der Meldebehörde haben. Der Begriff „Zugang“ ist weit auszulegen; entscheidend ist die tatsächliche Möglichkeit der Kenntnisnahme von Meldedaten. Auf die konkrete Tätigkeit des Bediensteten oder Mitarbeiters kommt es nicht an. Zugang kann

auch derjenige haben, zu dessen Aufgaben die Verarbeitung personenbezogener Daten nicht gehört. Unter den Begriff fallen mithin neben den regulären Voll- und Teilzeitbediensteten der Meldebehörde und ggf. des Auftragnehmers (z. B. Anbieter von Einwohnermeldeverfahren, externe IT-Dienstleister etc.) auch deren Auszubildende, Gutachter, externe Datenschutzbeauftragte und freie Mitarbeiter. Rechtsgrundlage der Tätigkeit für eine Meldebehörde in diesem Sinne kann ein Beamtenverhältnis, ein Dienst-, Arbeits-, Auftrags- oder Werkvertrag sein. In Auftragsverträgen gemäß § 7 Abs. 2 Satz 2 SächsDSG muss sichergestellt werden, dass der Auftragnehmer seine Mitarbeiter entsprechend zu verpflichten hat. Zu den „im Auftrag der Meldebehörde handelnden Stellen" zählt auch das externe oder ausgegliederte Hilfspersonal der Meldebehörde bzw. des Auftragnehmers, das Zugang zu personenbezogenen Daten der Meldebehörde hat (Reinigungskräfte, Botendienste etc.). Auf die konkrete Wahrscheinlichkeit der Kenntnisnahme durch das Hilfspersonal kommt es nicht an.

3. Was bewirkt die schriftliche Verpflichtung auf das Meldegeheimnis?

Die Verpflichtung auf das Meldegeheimnis bewirkt eine individuelle Rechtspflicht der für die Meldebehörde tätigen Personen, ordnungsgemäß mit den ihnen anvertrauten Meldedaten umzugehen.

Die Regelung des Meldegeheimnisses hat zum einen Hinweisfunktion, indem sie zusätzlich auf Pflichten hinweist, die sich für die Beschäftigten bereits aus den jeweils einschlägigen Vorschriften für die Verarbeitung und sonstige Nutzung von Meldedaten ergeben.

So wird etwa das Verbot der Datenverarbeitung mit Erlaubnisvorbehalt (§ 4 Abs. 1 SächsMG) oder die Erforderlichkeit der Datenerhebung zur Aufgabenerfüllung (vgl. §§ 1, 5 bis 8 SächsMG) zur persönlichen Verpflichtung aller „bei der Meldebehörde beschäftigten Personen, d. h. jedes einzelnen Bediensteten, Mitarbeiters eines Auftragnehmers oder jeder einzelnen externen Hilfskraft.

Zusätzlich zur Hinweisfunktion der Regelung des Meldegeheimnisses regelt § 9 SächsMG die Pflichten des Beschäftigten. Das Meldegeheimnis verbietet den Beschäftigten, sich Meldedaten für eigene private Zwecke zu beschaffen. Benötigt ein Beschäftigter Meldedaten für eigene Zwecke, so muss er wie ein Außenstehender einen Antrag auf Erteilung einer Melderegisterauskunft nach § 32 SächsMG stellen. Über diesen darf der Bedienstete nicht selbst entscheiden.

Verstößt ein Beamter oder Arbeitnehmer im öffentlichen Dienst oder ein Mitarbeiter eines beauftragten Unternehmens gegen das Meldegeheimnis, so eröffnet dies disziplinar-, arbeits-, ordnungswidrigkeiten- oder strafrechtliche Konsequenzen, z. B. nach

§§ 38, 39 SächsDSG[1] oder §§ 203 Abs. 2, 353b Abs. 1 StGB[2]. Strafrechtliche Konsequenzen nach §§ 203 Abs. 2, 353b Abs. 1 StGB werden für externe Hilfspersonen (z. B. Reinigungskräfte) allerdings nur eröffnet, wenn diese zuvor nach § 1 Abs. 1 Nr. 1 und 2 Verpflichtungsgesetz verpflichtet und damit nach § 11 Abs. 1 Nr. 4b StGB Amtsträgern gleichgestellt worden sind.

Die Verletzung des Meldegeheimnisses kann auch Schadensersatzpflichten im Rahmen der Amtshaftung nach Art. 34 GG i. V. m. § 839 BGB bzw. der zivilrechtlichen Haftung nach § 823 Abs. 2 BGB auslösen.

Auszug aus dem SächsMG und dem SächsDSG zur Verpflichtung auf das Meldegeheimnis

§ 9 SächsMG - Meldegeheimnis:

(1) Wer bei einer Meldebehörde oder einer Stelle, die im Auftrag der Meldebehörde handelt, beschäftigt ist, darf personenbezogene Daten nicht unbefugt verarbeiten oder sonst verwenden.

(2) Die in Absatz 1 genannten Personen sind vor der Aufnahme ihrer Tätigkeit über ihre Pflichten nach Absatz 1 sowie die sonstigen bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten und auf deren Einhaltung schriftlich zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

(3) Die Meldebehörden haben die in den Melderegistern gespeicherten Meldedaten nach dem Stand der Technik gegen elektronische Angriffe von außen zu schützen.

§ 38 SächsDSG - Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer

1. unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,
   a) verarbeitet,
   b) zum Abruf bereithält oder
   c) für sich oder einen anderen abruft oder auf andere Weise verschafft,
2. die Übermittlung von personenbezogenen Daten, die durch dieses Gesetz geschützt werden und nicht offenkundig sind, durch unrichtige Angaben erschleicht,

[1] So kann die unbefugte Verarbeitung personenbezogener Daten nach § 38 SächsDSG mit einer Geldbuße bis zu 25.000 Euro oder nach § 39 SächsDSG als Straftat mit bis zu zwei Jahren Freiheitsstrafe oder Geldstrafe geahndet werden.
[2] Möglich wäre eine Ahndung nach den §§ 133, 203, 204, 331, 332, 353b oder 355 StGB mit Freiheits- oder Geldstrafe.

3. nach einer Verpflichtung gemäß § 6 Abs. 2 das Datengeheimnis gemäß § 6 Abs. 1 Satz 1 oder 2 verletzt, wenn die Verletzung nicht mit Strafe bedroht ist,
3a. entgegen § 10 Abs. 3 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
4. entgegen § 11 Abs. 2 Satz 3 den Datenschutzbeauftragten einer öffentlichen Stelle wegen der Erfüllung seiner Aufgaben benachteiligt,
5. als Datenschutzbeauftragter einer öffentlichen Stelle seine Verschwiegenheitspflicht nach § 11 Abs. 5 Satz 1 verletzt, wenn die Verletzung nicht mit Strafe bedroht ist,
6. personenbezogene Daten ohne die nach § 14 Abs. 3 Satz 3 oder nach § 16 Abs. 4 Satz 3 erforderliche Einwilligung oder entgegen § 36 Abs. 3 für einen anderen Zweck verarbeitet,
7. eine Auskunft nach § 18 Abs. 1 unrichtig oder unvollständig erteilt,
8. entgegen § 24 Abs. 1 Satz 3 einen anderen benachteiligt oder maßregelt, weil er von seinem Recht auf Anrufung des Sächsischen Datenschutzbeauftragten Gebrauch gemacht hat,
8a. entgegen § 28 Abs. 1 Satz 1 Nr. 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,
8b. entgegen § 28 Abs. 1 Satz 1 Nr. 2 Einsicht in Unterlagen und Akten oder Zutritt zu den Diensträumen nicht, nicht vollständig oder nicht rechtzeitig gewährt,
9. bei der Datenverarbeitung im Auftrag als Auftragnehmer gegen eine Weisung des Auftraggebers gemäß § 7 Abs. 2 Satz 4 und 5 verstößt,
10. entgegen § 16 Abs. 5 eine vollziehbare Auflage oder eine Vereinbarung nicht, nicht rechtzeitig oder nicht vollständig erfüllt oder
11. entgegen § 36 Abs. 2 die dort bezeichneten Merkmale nicht getrennt speichert.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 25 000 EUR geahndet werden.

(3) Der Sächsische Datenschutzbeauftragte ist Verwaltungsbehörde im Sinne von § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 3 Abs. 6 des Gesetzes vom 12. Juli 2006 (BGBl. I S. 1466, 1470), geändert worden ist, in der jeweils geltenden Fassung. Die Staatsregierung wird ermächtigt, dem Sächsischen Datenschutzbeauftragten durch Rechtsverordnung die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach anderen datenschutzrechtlichen Bestimmungen zuzuweisen. Die Zuweisung bedarf der Zustimmung des Sächsischen Datenschutzbeauftragten.[3]

[3] § 38 geä. durch Artikel 1 des G vom 14. Dezember 2006 (GVBl. S. 530).

§ 39 SächsDSG - Straftaten

Wer eine der in § 38 Abs. 1 Nr. 1 bis 8 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

17.2.5 Einwilligung in die Veröffentlichung von personenbezogenen Daten einschließlich Abbildungen (Fotos) im Internet und in Druckschriften

Das nachstehende Einwilligungsformular kann - natürlich - entsprechend modifiziert werden. Sofern gewünscht, kann es mit den entsprechenden Veränderungen auch für Lehrer und Beschäftigte an Schulen Verwendung finden.

[Schule - Briefkopf]

Einwilligung in die Veröffentlichung von personenbezogenen Daten einschließlich Abbildungen (Fotos) im Internet und in Druckschriften

Sehr geehrte Schülerinnen,
sehr geehrte Schüler,

unsere Schule beabsichtigt, Informationen über die Schule, den Unterricht und Schulveranstaltungen - auch personenbezogen - einer größeren Öffentlichkeit zugänglich zu machen. Texte und Fotos zu Schülern sollen veröffentlicht werden. Neben Klassenfotos sollen auch Abbildungen und Informationen zu Schulfahrten und -ereignissen, Wettbewerben und Projekten verbreitet werden.

Gedacht ist auch an eine Veröffentlichung von personenbezogenen Daten (einschließlich Fotos) im Internet, so dass die Informationen örtlich unbeschränkt abgerufen und über Suchprogramme aufgefunden werden können. Insofern ist nicht ausgeschlossen, dass Dritte die frei verfügbaren Daten verwenden können. Dennoch erbitten wir hierzu Ihre Einwilligung, und falls Sie noch nicht volljährig sein sollten, auch die Ihrer Eltern.

(Schulleiter)
[ ]

Name, Vorname, Geburtsdatum des Schülers
Hiermit willige ich in die Veröffentlichung meiner personenbezogenen Daten einschließlich Fotos in den nachstehenden aufgeführten Medien ein:
o Schuljahresveröffentlichungen
o örtliche Zeitungen und Zeitschriften
o Internetpräsenz der Schule www.[...]

(bitte zutreffendes ankreuzen)

Die Rechteeinräumung zur Veröffentlichung der Abbildungen erfolgt ohne Vergütung und umfasst ein Bearbeitungsrecht, soweit diese Bildveränderungen nicht entstellend

sind. [*Optional - sofern Namensangaben zu Klassenfotos erfolgen sollen*: Klassenfotos werden lediglich mit alphabetischen Namenslisten versehen; ansonsten werden Fotos keine Namensangaben beigefügt.]

Ton-, Video-, Webcam- und Filmaufnahmen sind von dieser Einwilligung nicht umfasst.

Die Einwilligung kann jederzeit gegenüber dem Schulleiter widerrufen werden. Bei Druckschriften ist ein Widerruf ausgeschlossen, nachdem der Druckauftrag erteilt ist. Erfolgt kein Widerruf, gilt die Einwilligung zunächst zeitlich unbeschränkt, d. h. über das Schuljahr und über die Schulzugehörigkeit hinaus.

Ihre Einwilligung ist freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen Ihnen keinerlei Nachteile.

_____

[Ort, Datum]

_____

[Unterschrift der Schülerin / des Schülers] [ab dem 14. Lebensjahr ist auch die Unterschrift des Schülers vonnöten]

Stichwortverzeichnis