Sächsischer Landtag
4. Wahlperiode

DRUCKSACHE 4/1474

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

12. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 2005

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 12. September 2005 Ausgegeben am: 12. September 2005

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

Logisch ist zu unterscheiden zwischen biologischem und grammatischem Geschlecht (sexus und genus). Es wäre ein Verlust, diese Unterscheidung aufzugeben; sie erleichtert das Verständnis von Texten und hilft, sich auf das Wesentliche zu konzentrieren. Frauen bitte ich, sich auch von scheinbar männlichen, in Wahrheit nur generellen Bezeichnungen gemeint zu wissen: Bauherr, Lehrer, Beamter, Betroffener etc. (Übrigens gibt es auch den umgekehrten Fall: Der [männliche] Entbindungspfleger ist eine Hebamme i. S. v. § 53 Abs. 1 Nr. 3 StPO.)

Herausgeber: Der Sächsische Datenschutzbeauftragte
Andreas Schurig
Bernhard-von-Lindenau-Platz 1 Postfach 12 07 05
01067 Dresden 01008 Dresden
Telefon: 0351/4935401
Fax : 0351/4935490

Besucheranschrift: Devrientstraße 1
01067 Dresden

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

Inhaltsverzeichnis

Abkürzungsverzeichnis

Vorschriften

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der *amtlichen, in Ausnahmefällen auch nichtamtlichen Abkürzung, ersatzweise der amtlichen Kurzbezeichnung* aufgeführt.

Die genaue Fundstelle und Angabe der letzten Änderung sind bei bekannteren Bundesgesetzen (die in den gängigen Gesetzessammlungen leicht zu finden sind) weggelassen worden.

AO	Abgabenordnung Fassung vom 1. Oktober 2002 (BGBl. I S. 3866)
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz) in der Fassung vom 14. Januar 2003 (BGBl. I. S. 66)
BerRehaG	Gesetz über den Ausgleich beruflicher Benachteiligungen für Opfer politischer Verfolgung im Beitrittsgebiet (Berufliches Rehabilitierungsgesetz) vom 23. Juni 1994 (BGBl. I S. 1311, 1314), in der Neufassung vom 1. Juli 1997 (BGBl. I S. 1625)
BewachV	Verordnung über das Bewachungsgewerbe vom 7. Dezember 1995, (BGBl I 1995 S. 1602)
BGB	Bürgerliches Gesetzbuch in der Fassung vom 2. Januar 2002 (BGBl. I S. 42, ber. S. 2909)
BNotO	Bundesnotarordnung; zuletzt geändert am 21. Dezember 2004 (BGBl. I S. 3599)
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 23. März 1994 (BGBl. I S. 646, ber. S. 2975); zuletzt geändert durch Art. 7 des Gesetzes vom 23. Dezember 2002 (BGBl. I S. 4621)
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565); zuletzt geändert durch Art. 2 des Gesetzes vom 16. Juni 1998 (BGBl. I S. 1300)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz) in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, ber. 1985 S. 195);

	zuletzt geändert durch Art. 6 des Gesetzes vom 31. August 1998 (BGBl. I S. 2600)
Dienstleistungs-Statistikgesetz	Gesetz zur Einführung einer Dienstleistungsstatistik und zur Änderung statistischer Rechtsvorschriften vom 19. Dezember 2000 (Erstverkündung) (BGBl I 2000, S. 1765)
DVO SächsBO	Durchführungsverordnung zur Sächsischen Bauordnung vom 2. September 2004 (GVBl. S. 427)
EALG	Gesetz über die Entschädigung nach dem Gesetz zur Regelung offener Vermögensfragen und über staatliche Ausgleichsleistungen für Enteignungen auf besatzungsrechtlicher oder besatzungshoheitlicher Grundlage (Entschädigungs- und Ausgleichsleistungsgesetz) vom 27. September 1994 (BGBl. I S. 2624)
EG-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (ABl. EG L 281 vom 23. November 1995, S. 31)
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit; zuletzt geändert am 22. Dezember 2004 (BGBl. I. S. 3675)
FlErwV	Flächenerwerbsverordnung in BGBl. I S. 2624, 2628; dazu in Sachsen: Verordnung über den Erwerb land- und forstwirtschaftlicher Flächen, das Verfahren sowie den Beirat nach dem Ausgleichsleistungsgesetz (GVBl. vom 30. Juni 2000)
GefHundG	Gesetz zum Schutze der Bevölkerung vor gefährlichen Hunden vom 24. August 2000 (GVBl. S. 358)
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz) vom 23. Mai 1949; zuletzt geändert durch Änderungsgesetz vom 26. Juli 2002
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz) vom 14. November 2003 (BGBl. I S. 2190)
HeimG	Heimgesetz vom 7. August 1974, neu gefasst durch Bekanntmachung vom 5. November 2001 (BGBl I S. 2970); zuletzt geändert durch Art. 12 G vom 21. März 2005 (BGBl I S. 818)

Hk-UIG	Handkommentar zum Umweltinformationsgesetz (2. Auflage, Göttingen 2002, Schomerus/Schrader/Wegener)
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz) vom 20. Juli 2000 (BGBl. I S. 1045); zuletzt geändert durch Art. 12 G vom 24. Dezember 2003 (BGBl. I S. 2954)
KJHG	Kinder- und Jugendhilfegesetz; SGB VIII; BGBl. I. S. 3546; zuletzt geändert am 30. Juli 2004 (BGBl. I. 2014)
KraftStG	Kraftfahrzeugsteuergesetz; neu gefasst durch Bekanntmachung vom 26. September 2002 (BGBl. I 381)
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturheberrechtsgesetz); zuletzt geändert am 16. Februar 2001 (BGBl. I. S. 266)
LBStUG	Gesetz über die Rechtsstellung des Sächsischen Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Landesbeauftragtengesetz) vom 30. Juni 1992 (GVBl. S. 293)
LWO	Verordnung des Sächsischen Staatsministeriums des Innern über die Durchführung der Wahlen zum Sächsischen Landtag (Landeswahlordnung) vom 15. September 2003 (GVBl. S. 543)
ÖPNVG	Gesetz über den öffentlichen Personennachverkehr im Freistaat Sachsen vom 14. Dezember 1995; zuletzt geändert am 28. Mai 2004 (GVBl. S. 196)
OWiG	Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz); zuletzt geändert am 22. August 2002 (BGBl. I S. 3387)
PassG	Passgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Art. 7 § 7 Betreuungsgesetz vom 12. September 1990 (BGBl. I S. 2002) und Art. 2 Änderungsgesetz vom 30. Juli 1996 (BGBl. I S. 1182)
PAuswG	Gesetz über Personalausweise in der Fassung der Bekanntmachung vom 21. April 1986 (BGBl. I S. 548), geändert durch Art. 1 Änderungsgesetz vom 30. Juli 1996 (BGBl. I S. 1182)
PStG	Personenstandsgesetz; zuletzt geändert am 21. August 2002 (BGBl. S. 3322)

PStV	Verordnung zur Ausführung des Personenstandsgesetzes (Personenstandsverordnung) in der Fassung der Bekanntmachung vom 25. Februar 1977, geändert durch Art. 1 der 13. ÄndVO vom 24. März 1994 (BGBl. I S. 621); zuletzt geändert am 29. August 2000 (GVBl. S. 410)
PostG	Postgesetz vom 22. Dezember 1997; zuletzt geändert am 25. November 2003 (BGBl. I. S. 2304)
RHG	Gesetz über den Rechnungshof des Freistaates Sachsen vom 11. Dezember 1991 (GVBl. S. 409); geändert durch 1. RHÄndG vom 11. Dezember 1995 (GVBl. S. 385)
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren vom 1. Januar 1977; zuletzt geändert am 30. Juni 1998 (SächsJMBl. S. 93)
RSAV	Risikostruktur-Ausgleichsverordnung vom 3. Januar 1994 (BGBl. I S. 55)
SächsAG G 10	Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Freistaat Sachsen vom 16. Oktober 1992 (GVBl. S. 464)
SächsAGSGB	Sächsisches Gesetz zur Ausführung des Sozialgesetzbuches vom 6. Juni 2002 (GVBl. S. 168)
SächsArchivG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449), geändert durch Art. 1 des Gesetzes zur Änderung verschiedener Vorschriften des Sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398); zuletzt geändert am 5. Mai 2004 (GVBl. S. 148)
SächsBeurtVO	Verordnung der Sächsischen Staatsregierung über die dienstliche Beurteilung der Beamten vom 21. April 1998 (GVBl. S. 169)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 370, berichtigt durch Bekanntmachung vom 16. Dezember 1999 (GVBl. 2000 S. 7)
SächsBRKG	Sächsische Gesetz über den Brandschutz, Rettungsdienst und Katastrophenschutz vom 24. Juni 2004 (GVBl. S. 245, ber. S. 647)
SächsDO	Dienstordnung für die Behörden des Freistaates Sachsen (DienstO), Sächsische Dienstordnung; zuletzt geändert am 18. Mai 2005
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); zuletzt Neufassung vom 25. August 2003 (GVBl. S. 330) *(a. F. = alte Fassung; n. F. = neue Fassung)*
SächsGemO	Gemeindeordnung für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 345); zuletzt geändert durch Art. 1 des Gesetzes vom 14. Februar 2002 (GVBl. S. 86)
SächsHG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 11. Juni 1999 (GVBl. S. 294); zuletzt geändert durch Art. 26 des Gesetzes vom 28. Juni 2001 (GVBl. S. 426)
SäHO	Vorläufige Haushaltsordnung des Freistaates Sachsen vom 19. Dezember 1990 (GVBl. S. 213); zuletzt geändert durch Art. 4 des Gesetzes vom 19. Oktober 1998 (GVBl. S. 505)
SächsKAG	Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502), geändert durch Art. 57 des 2. Gesetzes zur Eurobedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426; zuletzt geändert am 26. August 2004 (GVBl. S. 418)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675), geändert durch Art. 4 des Gesetzes zur Änderung verschiedener Vorschriften des sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398); zuletzt geändert am 24. Juni 2004 (GVBl. S. 245)
SächsKitaG	Gesetz zur Förderung von Kindern in Tageseinrichtungen im Freistaat Sachsen (Gesetz über Kindertageseinrichtungen) vom 27. November 2001 (GVBl. S. 705); geändert durch Art. 10 HH-Begleitgesetz 2003 und 2004 vom 11. Dezember 2002 (GVBl. S. 312); zuletzt geändert am 10. April 2003 (GVBl. S. 94)
SächsKomZG	Sächsisches Gesetz über die kommunale Zusammenarbeit vom 19. August 1993 (GVBl. S. 815, berichtigt GVBl. 1993 S. 1103); zuletzt geändert durch Art. 7 des Gesetzes zur Änderung verschiedener Vorschriften des Sächsischen Landesrechts vom 25 Juni 1999 (GVBl. S. 398)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577); zuletzt geändert durch Art. 10 des 2. Gesetzes zur Eurobedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)
SächsMG	Sächsisches Meldegesetz in der Fassung der Bekanntmachung vom 11. April 1997 (GVBl. S. 377); geändert durch Art. 4 des Gesetzes

	zum 4. Staatsvertrag rundfunkrechtlicher Staatsverträge vom 16. März 2000 (GVBl. S. 89)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (GVBl. S. 466)
SächsRettDG	Gesetz über Rettungsdienst, Notfallrettung und Krankentransport für den Freistaat Sachsen vom 7. Januar 1993 (GVBl. S. 9); geändert durch Art. 11 des Sächsischen Aufbaubeschleunigungsgesetzes vom 4. Juli 1994 (GVBl. S. 1261)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453); geändert durch Art. 2 des Gesetzes von 12. Februar 1999 (GVBl. S. 49) und durch Art. 36 des 2. Gesetzes zur Eurobedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)
SächsVerf	Verfassung des Freistaates Sachsen v. 27. Mai 1992 (GVBl. S. 243)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (GVBl. S. 459)
SächsVwOrgG	Sächsisches Verwaltungsorganisationsgesetz v. 25. November 2003 (GVBl. S. 148)
SächsVwVfG	Vorläufiges Verwaltungsverfahrensgesetz für den Freistaat Sachsen vom 21. Januar 1993 (GVBl. S. 74)
SächsVwVG	Sächsisches Verwaltungsvollstreckungsgesetz vom 17. Juli 1992 (GVBl. S. 327); zuletzt geändert durch Gesetz vom 19. Oktober 1998 (GVBl. S. 505)
SächsKomZG	Sächsisches Gesetz über kommunale Zusammenarbeit vom 19. August 1993; zuletzt geändert am 5. Mai 2004 (GVBl. S. 148)
SächsWahlG	Gesetz über die Wahlen zum Sächsischen Landtag vom 5. August 1993 (GVBl. S. 723); zuletzt geändert durch Art. 1 des Gesetzes zur Änderung des Sächsischen Wahlgesetzes und des Abgeordnetengesetzes vom 12. Januar 1995 (GVBl. S. 1)
SächsWG	Sächsisches Wassergesetz vom 18. Oktober 2004 (GVBl. S. 482)
SäHO	Sächsische Haushaltsordnung vom 10. April 2001 (GVBl. S. 333)

SchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213); zuletzt geändert durch Gesetz vom 29. Juni 1998 (GVBl. S. 271)
SchulGesPflVO	Schulgesetzpflegeverordnung vom 10. Januar 2005 (GVBl. S. 15)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015); zuletzt geändert durch Art. 2 des Gesetzes vom 21. August 2002 (BGBl. I S. 2950)
SGB IV	Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), zuletzt geändert durch Gesetz vom 10. Dezember 2002 (BGBl. I S. 3443)
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477); zuletzt geändert durch Art. 1 des Gesetzes v. 23. Dezember 2002 (BGBl. I S. 4637)
SGB VIII	Sozialgesetzbuch (SGB) Achtes Buch (VIII) - Kinder- und Jugendhilfe - in der Fassung der Bekanntmachung vom 8. Dezember 1998 (BGBl. I S. 3546); zuletzt geändert durch Art. 10 Nr. 9 des Gesetzes vom 20. Juni 2002 (BGBl. I S. 1946)
SGB X	Sozialgesetzbuch (SGB) Zehntes Buch (X) - Sozialverwaltungsverfahren und Sozialdatenschutz - in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130); zuletzt geändert durch Art. 5 des Gesetzes vom 23. Dezember 2002 (BGBl. I S. 4621)
SGB XI	Sozialgesetzbuch (SGB) Elftes Buch (XI) - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014); zuletzt geändert durch Gesetz vom 14. Dezember 2001 (BGBl. I S. 3728)
SGB XII	Sozialgesetzbuch (SGB) Zwölftes Buch (XII) - Sozialhilfe - (Artikel 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022)
SHG	Sächsisches Hochschulgesetz vom 11. Juni 1999; zuletzt geändert am 5. Mai 2004 (GVBl. S. 148)
StGB	Strafgesetzbuch vom 13. November 1998; zuletzt geändert am 24. März 2005 (BGBl. I S. 969)
StPO	Strafprozessordnung vom 7. April 1987; zuletzt geändert am 22. März 2005 (BGBl. I S. 837)

StrRehaG	Gesetz über die Rehabilitierung und Entschädigung von Opfern rechtsstaatswidriger Strafverfolgungsmaßnahmen im Beitrittsgebiet (Strafrechtliches Rehabilitierungsgesetz) vom 29. Oktober 1992 (BGBl. I S. 1814); geändert durch Gesetz zur Änderung des Strafrechtlichen Rehabilitierungsgesetzes, des Verwaltungsrechtlichen Rehabilitierungsgesetzes und des Beruflichen Rehabilitierungsgesetzes vom 15. Dezember 1995 (BGBl. I S. 1782)
StVG	Straßenverkehrsgesetz in der Fassung vom 5. März 2003 (BGBl. I. S. 310)
StVG	Straßenverkehrsgesetz vom 5. März 2003 (BGBl. I S. 919); zuletzt geändert am 24. August 2004 (BGBl. I S. 2198 ber. 2300)
StVO	Straßenverkehrs-Ordnung vom 16. November 1970 (BGBl. I S. 1565, 1971 I S. 38); geändert durch Artikel 1 der Verordnung vom 7. August 1997 (BGBl. I S. 2028)
UIG	Umweltinformationsgesetz v. 22. Dezember 2004 (BGBl. I S. 3704)
UKG	Gesetz über das Universitätsklinikum Leipzig an der Universität Leipzig und das Universitätsklinikum Carl-Gustav-Carus Dresden an der TU Dresden (Universitätsklinikagesetz) vom 6. Mai 1999; rechtsbereinigt vom 3. Mai 2003
Verpflichtungsgesetz	Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 2. März 1974 (BGBl. I S. 469, 545; III 453-17); zuletzt geändert durch Änderungsgesetz v. 15. August 1974 (BGBl. I S. 1942)
VersammlG	Gesetz über Versammlungen und Aufzüge (Versammlungsgesetz) in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1790); geändert durch Art. 3 des Gesetzes zur Änderung des Strafgesetzbuches usw. v. 9. Juni 1989 (BGBl. I S. 1059)
VwGO	Verwaltungsgerichtsordnung vom 19. März 1991; zuletzt geändert am 22. März 2005 (BGBl. I S. 837)
VwRehaG	Gesetz über die Aufhebung rechtsstaatswidriger Verwaltungsentscheidungen im Beitrittsgebiet und die daran anknüpfenden Folgeansprüche vom 23. Juni 1994 (BGBl. I S. 1311); neu gefasst durch Bekanntmachung vom 1. Juli 1997 (BGBl. I S. 1620); zuletzt geändert durch Art. 2 G vom 22. Dezember 2003 (BGBl. S. 2834)
VwVfG	Verwaltungsverfahrensgesetz vom 23. Januar 2003

WEG	Gesetz über das Wohnungseigentum und das Dauerwohnrecht vom 15. März 1951 (BGBl. I S. 1951); zuletzt geändert durch Art. 4 Abs. 36 G vom 5. Mai 2004 (BGBl. I S. 718)
WoGG	Wohngeldgesetz vom 14. Dezember 1970 (BGBl. I S 1637); neu gefasst durch Bekanntmachung vom 7. Juli 2005 (BGBl. I S. 2029)
WStatG	Gesetz über die allgemeine und die repräsentative Wahlstatistik bei der Wahl zum Deutschen Bundestag und bei der Wahl der Abgeordneten des Europäischen Parlaments aus der BRD (Wahlstatistikgesetz) vom 21. Mai 1999 (BGBl. I S. 1023)
ZPO	Zivilprozessordnung vom 12. September 1950; zuletzt geändert am 22. März 2005 (BGBl. I S. 837)

Sonstiges

AVS	Akademie für öffentliche Verwaltung des Freistaates Sachsen
BayVGH	Bayerischer Verwaltungsgerichtshof
BfD	Bundesbeauftragter für den Datenschutz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BMGS	Bundesministerium für Gesundheit und Soziale Sicherung
BMI	Bundesministerium des Innern
BMWA	Bundesministerium für Wirtschaft und Arbeit
BND	Bundesnachrichtendienst
BR-DS	Bundesrats-Drucksache
BSG	Bundessozialgericht

BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts
DöV	Die öffentliche Verwaltung
DVBl.	Deutsches Verwaltungsblatt
DVO	Durchführungsverordnung
EG	Europäische Gemeinschaft
EU	Europäische Union
e. V.	Eingetragener Verein
FEVS	Fürsorgerechtliche Entscheidungen der Verwaltungs- und Sozialgerichte
GmbH	Gesellschaft mit beschränkter Haftung
HStR	Handbuch des Staatsrecht der Bundesrepublik Deutschland
INPOL	Polizeiliches Informationssystem des Bundes und der Länder
LfD	Landesbeauftragte(r) für den Datenschutz
LfF	Landesamt für Finanzen des Freistaates Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LG	Landgericht
LKA	Landeskriminalamt Sachsen
LT-DS	Landtags-Drucksache

MAD	Militärischer Abschirmdienst
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MfS	Ministerium für Staatssicherheit der ehemaligen DDR
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen
SächsABl.	Sächsisches Amtsblatt
SächsDO	Sächsische Dienstordnung
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsMBl. SMF	Ministerialblatt des Sächsischen Staatsministeriums der Finanzen
SächsOVG	Sächsisches Oberverwaltungsgericht
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SBZ	Sowjetische Besatzungszone
SIS	Schengener Informationssystem
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
SML	Sächsisches Staatsministerium für Landwirtschaft und Forsten
SMS	Sächsisches Staatsministerium für Soziales
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft

SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SRH	Sächsischer Rechnungshof
SSG	Sächsischer Städte- und Gemeindetag
VG	Verwaltungsgericht
VwRR	Verwaltungsrechtsreport
ZBR	Zeitschrift für Beamtenrecht

Verweise im Text auf Ausführungen in früheren Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten sind durch Angabe der Nummer des jeweiligen Tätigkeitsberichtes sowie der jeweiligen Abschnitt-Nr. - getrennt durch einen Schrägstrich - gekennzeichnet (z. B. 4/5.1.2.6).

1 Datenschutz im Freistaat Sachsen

1.1 Neue Herausforderungen

Der Berichtszeitraum für den Tätigkeitsbericht umfasst seit der Novellierung des Sächsischen Datenschutzgesetzes vom 25. August 2003 zwei Jahre. Damit fallen die ersten neun Monate noch in die Amtszeit meines Vorgängers, für mich ein willkommener Anlass, um noch einmal auf sein Wirken als Sächsischer Datenschutzbeauftragter einzugehen.

Noch vor seiner Wahl zum Datenschutzbeauftragten hat Herr Dr. Giesen von Anfang an als Leiter des bei der Sächsischen Staatskanzlei angesiedelten Aufbaustabes die Geschicke des Datenschutzes in Sachsen mitgestaltet. Die Verabschiedung des Sächsischen Datenschutzgesetzes und die Schaffung der Kontrollbehörde 1991 waren der Auftakt für eine wirkungsvolle zwölfjährige Tätigkeit. Von der inhaltlichen Breite und Tiefe legen die elf Tätigkeitsberichte beredtes Zeugnis ab. Von der Wucht und Durchsetzungskraft könnte sicher mancher sächsischer Amtsträger noch heute lebhaft berichten. Seine Mitarbeiter haben mit ihm manche Höhen und Tiefen durchgestanden und sind von ihm und mit ihm geprägt worden. Als sein langjähriger Stellvertreter und Nachfolger danke ich ihm für die gemeinsam erlebte Zeit, für manchen freundschaftlichen Rat und für ein solides Fundament, das in diesen zwölf Jahren gelegt worden ist. Auch möchte ich an dieser Stelle dem Präsidenten des Sächsischen Landtages und der Verwaltung danken. Sie haben in mitunter auch schwierigen Zeiten stets den Datenschutzbeauftragten unterstützt und sichern seine tägliche Arbeit.

Notwendig ist es allerdings auch, immer wieder daran zu erinnern, warum dieses Fundament geschaffen worden ist. Die Verabschiedung des Sächsischen Datenschutzgesetzes und noch mehr die Aufnahme des Grundrechtes auf Datenschutz in die Sächsische Verfassung 1992 war nicht einfach die bloße Antizipation aus der „alten“ Bundesrepublik übernommener demokratischer Grundregeln, sondern entsprang eigenem erlebten Bedürfnis. Die Menschen im Osten Deutschlands hatten - unterbrochen von einer kurzen Zeit der schnell erstickten Hoffnung nach 1945 - zwei Diktaturen erlitten, denen bei aller Unvergleichlichkeit gemeinsam ist, dass in ihrem System die Achtung der Privatsphäre des Einzelnen und seine Selbstbestimmung keinen Platz hatte. Die Demonstranten des Herbstes 1989 haben frühzeitig und mit Klarheit auf ihren Transparenten gefordert, was ihnen dringend und was an der Zeit war. „Freiheit - Selbstbestimmung - Menschenrechte“ lautet eines der ersten Bänder aus dem Oktober. Mittlerweile sind 16 Jahre vergangen. Ich habe manchmal den Eindruck, die Gesellschaft hat sich an den erreichten Zustand gewöhnt. Das, was damals als bedrängend empfunden worden ist, ist heute zwar lästig, aber nicht entscheidend („Ich habe nichts

zu verbergen“). Waren damals die Sinne und das Empfinden für die Wichtigkeit einer solchen Forderung geschärft, so wird sie heute abgetan („Datenschutz ist Täterschutz“) oder man resigniert („man kann ja sowieso nichts machen“). Demokratie ist ein mühsames Geschäft. Ihre Grundlagen müssen stetig neu bedacht, formuliert und auch erkämpft werden. Sie sind allerdings nicht beliebig. Es gibt einen festen Wertekanon, in dem die Freiheit des Einzelnen an vorderer unaufgebbarer Stelle steht. Jedes demokratisch verfasste Staatswesen, das sich den derzeit immer wieder thematisierten Gefahren stellen will, sei es bei den inneren und äußeren Bedrohungen der Sicherheit, sei es bei der mangelnden Abgabenbereitschaft und dem unterstellten Leistungsmissbrauch seiner Bürger, tut gut daran, sich seines demokratischen und freiheitlichen Grundkonsenses zu erinnern. „Sooft eine bestimmte Freiheit in Frage gestellt ist, ist die Freiheit in Frage gestellt“ lautete ein anderes Transparent in Leipzig im Herbst 1989. Ich würde es begrüßen, wenn Amtsträger bei aller notwendigen Erfüllung der ihnen zugewiesenen Aufgaben diesen Grundkonsens im Auge haben. Ich werde sie daran erinnern.

Innerhalb der reichlich 13 Jahre währenden Existenz des sächsischen Datenschutzes hat es neben der fortwährenden Notwendigkeit, den Grundrechtsschutz der Bürger zu sichern, gravierende Veränderungen der Rahmenbedingungen gegeben, die in der letzten Zeit deutlich erkennbar geworden sind.

Der Technisierungsgrad der Verwaltungen ist in einem solchen Maße gestiegen, dass nicht mehr von der „elektronischen Schreibmaschine“ gesprochen werden kann. Mittlerweile sind Verwaltungsverfahren untrennbar mit ihrer technischen Umsetzung verbunden, ja sogar von der eingesetzten Technik bestimmt. Die Entscheidung über die mit dem Verfahren verbundene Systemstruktur determiniert das Projekt und bestimmt dessen Potentiale. Toll Collect und Gesundheitskarte sind klare Beispiele. Dies führt dazu, dass nicht allein der vorgesehene rechtliche Rahmen zu betrachten ist, sondern auch die - bisher noch nicht vorgesehenen - technischen Möglichkeiten, die solch ein Verfahren in sich birgt. Die Erfahrung zeigt, dass bei entsprechender Gelegenheit der juristische Rahmen sehr schnell erweitert wird, wenn es die Technik nur hergibt.

Neue Projekte reichen in der Regel über den Rahmen des Freistaates hinaus. Die Technisierung macht eine mindestens bundesweite - teilweise sogar europäische - Koordinierung und die Schaffung gemeinsamer verbindlicher Standards und Schnittstellen notwendig. Dies geschieht fast ausschließlich in den dem parlamentarischen Raum weit vorgelagerten Arbeitsgruppen und Kommissionen.

Die wesentlichen Entscheidungen sind im Prinzip gefallen, wenn die entsprechenden Gesetze behandelt werden. Sie lassen sich nur noch unter großem Aufwand revidieren, falls sich im System angelegte Mängel zeigen. Hinzu kommt, dass in solchen Fällen

eine Vielzahl von beteiligten Partnern gemeinsam diese Fehlentwicklungen revidieren müssten, was in der Regel an der Schwerfälligkeit des dann notwendigen Koordinierungsprozesses scheitert.

Darüber hinaus ist zu beobachten, dass die klassischen Grenzen zwischen privatem und öffentlichem Bereich verschwimmen. So sind private Stellen wie Ärzte oder Apotheker bei der Gesundheitskarte von Anfang an einbezogen. Wenn sich dies vom Ansatz des zu gestaltenden Sachverhaltes her ergibt, ist es notwendig und aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden. Bedenklicher ist es, wenn für öffentliche Zwecke auf private Datenbestände zurückgegriffen wird (Kontenabfrage, Verbindungsdatenabfrage bei Telekommunikationsunternehmen). Durch diese Zweck ändernde Nutzung versucht der Staat, sich Datenbestände der Privatwirtschaft zu erschließen, ohne sich den strengen für den öffentlichen Bereich geltenden Erhebungsmaßstäben zu unterwerfen. Das Grundrecht auf informationelle Selbstbestimmung ist ein Abwehrrecht gegenüber der öffentlichen Gewalt. Der Bürger gibt im Privatverhältnis unter ganz anderen Bedingungen personenbezogene Daten preis. Der Zugriff auf solche Datenbestände ist eine Aushöhlung des Grundrechtsschutzes.

Setzen datenschutzrechtliche Kontrollmaßnahmen erst kurz vor der Inbetriebnahme eines Systems ein, ist es meist zu spät. Durch die EG-Datenschutzrichtlinie ist das Instrument der Vorabkontrolle (in der Regel durch den behördlichen Datenschutzbeauftragten) in das deutsche Datenschutzrecht aufgenommen worden. Wird dies so praktiziert, dass erst kurz vor Inbetriebnahme eines Verfahrens die Kontrolle erfolgt, ist es wirkungslos. Bereits bei der Planungs- und Konzeptionsphase sind datenschutzrechtliche Fragen zu berücksichtigen, denn die Entscheidungen über sie haben in der Regel gravierende Auswirkungen auf technische Systemarchitekturen und organisatorische Abläufe. Dieses Instrument bezieht sich jedoch nur auf Verfahren in einer funktionalen bzw. organisatorischen Stelle; bei der Beteiligung mehrerer Stellen ist notwendigerweise die Kontrollbehörde gefragt.

Zusätzlich wäre durch die frühzeitige Einbindung auch die Unterstützung der parlamentarischen Kontrolle gewährleistet, die den meisten Datenschutzbeauftragten ebenfalls obliegt.

Zu der Notwendigkeit, die Aufsicht über den Privatbereich und den öffentlichen Bereich zu vereinigen, habe ich mich bereits öffentlich bei meiner Amtsübernahme geäußert. Die Entwicklung bestätigt mich. Neuere Verfahren sind ohne Public-private-partnership, ohne das Zusammenwirken öffentlicher und privater Stellen nicht mehr denkbar. Eine Zersplitterung der Aufsicht führt hier auch zu einer unvollständigen Einschätzung und Gestaltung übergreifender datenschutzrechtlicher Notwendigkeiten.

Auch auf die Tätigkeit der Datenschutzbehörden hat diese oben geschilderte Entwicklung Auswirkungen. Arbeitsteilung und Unterstützung bis hin zu koordiniertem Zusammenwirken sind notwendig. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tut dies seit Jahren in ihren Arbeitskreisen mit Erfolg. In letzter Zeit verstärkt sich diese Zusammenarbeit. Entsteht im Bund ein Vorhaben, das durch die Länder ausgeführt wird, so übernimmt der Bundesbeauftragte in Abstimmung mit den Landesbeauftragten die rechtliche Begleitung. Die anschließende abgestimmte Kontrolle in den Ländern führen die dortigen Datenschutzbeauftragten durch. Die Ergebnisse werden im betreffenden Arbeitskreis ausgetauscht und führen zu Änderungsvorschlägen, die der Bundesbeauftragte einbringt. Anders lässt sich eine adäquate datenschutzrechtliche Begleitung nicht mehr sichern.

Aus dem anfänglich lockeren Zusammentreffen „Datenschutzkonferenz“ ist ein notwendiges effizientes Arbeitsinstrument geworden, dessen halbjährliches öffentlichkeitswirksames Treffen nur die Spitze des Eisbergs ist. Eine ähnliche Entwicklung auf europäischer Ebene zeichnet sich ab. Mittlerweile gibt es sogar schon über diesen Rahmen hinaus internationale Kontakte unter den Datenschutzbeauftragten.

Datenverarbeitung - und damit auch Datenschutz - ist mittlerweile längst eine globale Angelegenheit.

1.2 Das neue Sächsische Datenschutzgesetz vom 25. August 2003

Am 9. September 2003, ein halbes Jahr nach Beginn meines Berichtszeitraums, ist das neu gefasste Sächsische Datenschutzgesetz nach einem fast 1½-jährigen parlamentarischen Gesetzgebungsverfahren in Kraft getreten. Zugleich ist das Vorgängergesetz vom 11. Dezember 1991 außer Kraft getreten. Mit der Neufassung (GVBl. 2003, S. 330) ist das Gesetz an die Vorgaben der EG-Datenschutzrichtlinie vom 24. Oktober 1995 angepasst und in einigen weiteren Punkten geändert worden. Die Grundstruktur des Gesetzes und seine Grundaussagen (z. B. die Definition des personenbezogenen Datums) blieben jedoch unverändert. Auch meine Rechtsstellung als unabhängiger Wahrer des Grundrechts auf Datenschutz, die in Artikel 57 der Verfassung des Freistaates Sachsen garantiert wird, ist schließlich im Wesentlichen erhalten geblieben.

Diesem Ergebnis war ein langes und hartes Ringen zwischen der Staatsregierung und dem Landtag, insbesondere um die Rechtsstellung und Kontrollbefugnisse meines Amtes, §§ 25 ff. SächsDSG, vorangegangen. Die Mehrheitsfraktion des Landtages hat dieses Ringen schließlich einer vernünftigen und akzeptablen Lösung zugeführt. Sie hat damit zugleich eine Auseinandersetzung vor dem Verfassungsgerichtshof des Freistaates Sachsen vermieden. Ohne die Hilfe engagierter und weitsichtiger Abgeordneter

und ihrer Mitarbeiter, denen ich für dieses Ergebnis meinen herzlichen Dank sage, wäre es andernfalls um den Datenschutz in Sachsen heute schlecht bestellt.

Der beim Sächsischen Landtag am 28. März 2002 eingegangene Regierungsentwurf einer Neufassung des Sächsischen Datenschutzgesetzes (LT-DS 3/6181) enthielt verfassungswidrige Regelungen. Er ging auf einen Mitte 2000 erarbeiteten und am 20. Dezember 2000 durch das Kabinett beschlossenen Referentenentwurf zurück. Er war von dem Versuch durchzogen, die als unbotmäßig empfundene Amtsausübung meines Vorgängers Thomas Giesen für die Zukunft zu konterkarieren. Dazu waren im Gesetzentwurf scharfe Beschränkungen seiner Rechtsstellung vorgesehen worden. Im März 2001 sah sich deshalb die 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder veranlasst, zu dem Gesetzgebungsvorhaben wie folgt Stellung zu nehmen - ein bisher einmaliger Vorgang: „Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Lande Sachsen, durch gesetzgeberische Maßnahmen dieses Recht (das Grundrecht auf informationelle Selbstbestimmung, Anm. d. V.) zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.“ Mit einer Mitteilung vom 12. März 2002 wandte sich mein Amtsvorgänger an die Presse und kündigte eine Klage vor dem Verfassungsgerichtshof für den Freistaat Sachsen für den Fall an, dass der Sächsische Landtag den erörterten Regierungsentwurf als Gesetz beschließen sollte.

Der eingebrachte Regierungsentwurf sah vor, die Staatsministerien, die Polizei und die Personalverwaltungen weitgehend von externer datenschutzrechtlicher Kontrolle auszunehmen. Zu diesem Zweck sollte der „Kernbereich exekutiver Eigenverantwortung“ der Staatsregierung, die gesamte polizeiliche Datenverarbeitung zum Zwecke der Strafverfolgung sowie die Personalaktenführung aller Dienststellen nicht mehr durch mich oder meine Mitarbeiter kontrolliert werden dürfen. Mit anderen Worten: Dort, wo das Grundrecht auf informationelle Selbstbestimmung nach Art. 33 SächsVerf besonders gefährdet ist, sollte die externe Kontrolle durch ein unabhängiges Amt so gut wie ausgeschlossen werden. Der Sächsische Datenschutzbeauftragte sollte nur mehr als „Hilfsorgan des Sächsischen Landtages“ verstanden werden. Der Anwendungsbereich des Datenschutzgesetzes sollte eingeschränkt, die Auskunftserteilung an Betroffene erschwert, der bei Datenschutzverstößen zu leistende Schadensersatz beschränkt werden. Die Anrufung des Sächsischen Datenschutzbeauftragten, ein Jedermannsrecht - auch für alle öffentlichen Bediensteten im Freistaat Sachsen - sollte nicht weiter reichen dürfen als meine dann stark reduzierte Zuständigkeit. Der Datenschutzbeauftragte sollte sich nur noch nach vorheriger Konsultation mit der betroffenen öffentlichen Stelle an die Öffentlichkeit wenden dürfen. Dass der Bundesgerichtshof in seinem Urteil zu den Verratsvorwürfen gegen meinen Vorgänger vom 9. Dezember 2002 (5 StR 76/02)

bereits festgestellt hatte, dass die Information der Öffentlichkeit über Gesetzesverstöße selbst ein wichtiges öffentliches Interesse darstellt, schien das federführende Innenministerium bei der Einbringung in den Landtag nicht zu beeindrucken.

Dies alles wäre mit der Verfassung des Freistaates Sachsen und der EG-Datenschutzrichtlinie nicht zu vereinbaren gewesen. Nach beiden Rechtsnormen darf es keine datenschutzkontrollfreien Räume in der öffentlichen Verwaltung des Freistaates Sachsen geben. Artikel 57 SächsVerf hat mir sowohl die Wahrung des Rechts auf Datenschutz nach Art. 33 SächsVerf als auch die „Unterstützung des Sächsischen Landtages bei der Ausübung seiner parlamentarischen Kontrolle“ als Aufgabe zugewiesen. Die erste Aufgabe erfülle ich in richtergleicher Unabhängigkeit für alle Menschen im Freistaat Sachsen. Sie steht in der Praxis im Vordergrund. Ohne sie wäre eine funktionierende und der EG-Datenschutzrichtlinie entsprechende Datenschutzkontrolle nicht möglich.

Die sich aus der EG-Datenschutzrichtlinie ergebenden Änderungen waren im Gesetzentwurf der Staatsregierung lustlos und auf dem jeweils niedrigstmöglichen Niveau umgesetzt. So war z. B. meine vorherige Anhörung nur zu Entwürfen *amtlich bekannt zu machender* Verwaltungsvorschriften vorgesehen, obwohl in der EG-Datenschutzrichtlinie eine solche Beschränkung nicht vorgesehen ist. Auch dieser Fehler wurde später korrigiert.

Der Einbringung des Regierungsentwurfs in den Landtag folgte ein langwieriges parlamentarisches Beratungsverfahren. Der Innenausschuss des Sächsischen Landtages befasste sich am 2. Mai 2002 erstmals mit dem Entwurf. Im August 2002 legte die Flutkatastrophe das Landtagsgebäude und mit ihm jede weitere Gesetzgebung für die folgenden Monate lahm. Am 19. September 2002 fand eine Öffentliche Anhörung des Regierungsentwurfs im Sächsischen Landtag mit Sachverständigen aus ganz Deutschland statt. Die darauf folgende Überarbeitung des Regierungsentwurfs in den mitberatenden Ausschüssen für Haushalt- und Finanzen und für Verfassung und Recht sowie im federführenden Innenausschuss nahm weitere zehn Monate in Anspruch. Sie fand schließlich ihren Niederschlag in einem umfangreichen Änderungsantrag der Mehrheitsfraktion des Sächsischen Landtages vom 3. Juli 2003.

Mit diesem Änderungsantrag wurden unter anderem die Beschränkungen meiner Kontrollbefugnisse zurückgenommen und der Anwendungsbereich des Datenschutzgesetzes auf bestimmte juristische Personen und sonstige Vereinigungen des privaten Rechts ausgeweitet. Der Ausschluss u. a. des Kernbereichs exekutiver Eigenverantwortung, der Strafverfolgungsvorgänge sowie der Akten im Gesundheits- und Personalwesen von meiner Kontrollbefugnis waren vom Tisch. Viele weitere Verbesserungen bezogen sich auf Details oder unproblematische Regelungen. Eine eventuelle

Normenkontrollklage vor dem Verfassungsgerichtshof in Leipzig hatte sich damit erledigt.

In einer Übergangsregelung wurde sichergestellt, dass die Anpassung automatisierter Verarbeitungsverfahren an die neuen Regelungen binnen drei Jahren nach In-Kraft-Treten dieses Gesetzes, also bis zum 9. September 2006, zu erfolgen hat. Mit dieser verwaltungsfreundlichen Regelung kann ich leben.

Am 8. Juli 2003 empfahl der Innenausschuss dem Plenum des Landtages ohne Gegenstimmen bei nur sechs Enthaltungen die Annahme des Gesetzentwurfs der Staatsregierung in der Fassung des Änderungsantrages (LT-DS 3/8769). Die Zweite und Dritte Lesung des so geänderten Gesetzentwurfes fanden im Plenum am 10. Juli 2003 statt; die Ausfertigung des Gesetzes durch den Präsidenten des Sächsischen Landtages geschah am 25. August 2003. Seit dem 9. September 2003 ist es in Kraft.

Natürlich hatte das Gesetz auch organisatorische Auswirkungen. Der Datenschutzbeauftragte hat in Zukunft zwei zusätzliche Register zu führen. Er hat zum einen sämtliche behördlichen Datenschutzbeauftragten zu erfassen, zum anderen für die Stellen, die keinen eigenen behördlichen Datenschutzbeauftragten haben, das Verzeichnis automatisierter Erarbeitungsverfahren nach § 10 SächsDSG zu führen.

Ich habe darüber hinaus bei den Stellen, die keinen eigenen Datenschutzbeauftragten besitzen, die Vorabkontrolle nach § 10 Abs. 5 SächsDSG für sämtliche Abrufverfahren, für automatisierte Verfahren, in denen besonders sensible Daten verarbeitet werden, sowie für automatisierte Verfahren, in denen Beschäftigtendaten verarbeitet werden, durchzuführen. Nach Abs. 5 Satz 2 SächsDSG ist die Stellungnahme innerhalb eines Monats abzugeben. Es ist dabei nicht mit einem einfachen Abheften und Durchnicken getan. Ich bin durch diese Neuregelung de facto der behördliche Datenschutzbeauftragte der Stellen, die sich keinen eigenen bestellen.

Ich habe diesen Mehraufwand durch eine organisatorische Änderung und eine minimale Stellenmehrung abgefangen. Um die oben genannten Aufgaben zu bewältigen, ist eine Geschäftsstelle des Sächsischen Datenschutzbeauftragten gebildet worden, die zusätzlich auch die bisherigen geschäftsstellenartigen Aufgaben des Sekretariates übernommen hat. Der damit verbundene personelle Mehraufwand hält sich in sehr moderaten Grenzen. Der Landtag hat ihn mit der Verabschiedung des Doppelhaushaltes 2005 bestätigt. Die Landtagsverwaltung hat zügig für die personelle und räumliche Umsetzung gesorgt.

Eine vorläufige Bewertung der Neufassung des Sächsischen Datenschutzgesetzes fällt nach dem Ablauf von anderthalb Jahren nicht in allen Teilen leicht. Zwar hat sich das

Gesetz, soweit es den bewährten datenschutzrechtlichen Bestand an die Vorgaben der EG-Datenschutzrichtlinie angepasst hat, im Wesentlichen bisher weiter bewährt. Probleme treten jedoch insbesondere bei der Bestimmung von öffentlichen Stellen auf, die privatrechtlich organisiert sind. Da die Koalition sich darauf verständigt hat, zu prüfen, ob dem Sächsischen Datenschutzbeauftragten auch die Kontrolle über den Privatbereich übertragen wird, und die bisherigen Äußerungen seitens der Staatsregierung in dieser Hinsicht positiv sind, bietet es sich an, im Rahmen eines solchen Gesetzgebungsvorhabens auch diese Probleme anzupacken. Der Sächsische Staatsminister des Innern hat dazu seine Bereitschaft erklärt.

1.3 Datenschutzbeauftragte nach § 11 SächsDSG

1. Allgemeines zur Bestellung bzw. zum Verzicht auf eine Bestellung eines behördlichen Datenschutzbeauftragten

Das neue Sächsische Datenschutzgesetz enthält in § 11 erstmals eine Bestimmung in der die Bestellung und die Aufgaben und Befugnisse interner Datenschutzbeauftragter beschrieben sind. Die Bestellung eines Datenschutzbeauftragten ist mir mitzuteilen. Erstaunlicherweise habe ich bisher - insbesondere aus dem kommunalen Bereich - nur wenige Mitteilungen erhalten. Hierfür sind aus meiner Sicht drei Gründe möglich:

- Die entsprechenden Regelungen im Sächsischen Datenschutzgesetz sind nicht bekannt bzw. es wurde nur die "Kann-Regelung", nicht aber die Konsequenzen einer Nichtbestellung in die Überlegungen einbezogen. Im letzteren Fall bin ich jeweils vor der Einführung automatisierten Verfahren im Rahmen der Vorabkontrolle zu beteiligen (§ 10 Abs. 5 SächsDSG) bzw. ist mir das Verfahrensverzeichnis zur Kenntnis zu bringen (§ 10 Abs. 3 Satz 1 SächsDSG).

- Die Regelungen sind bekannt, die Bestellung eines behördlichen Datenschutzbeauftragten wird aber als so wenig nützlich oder hinderlich betrachtet, dass man die Nachteile bzw. Konsequenzen einer Nichtbestellung in Kauf nimmt.

- Es ist bereits vor Inkrafttreten der Regelung nach dem neuen Sächsischen Datenschutzgesetz ein behördlicher Datenschutzbeauftragter bestellt worden.

Ich rechne damit, dass die Stellen, auf die die erstgenannten Gründe zutreffen, in den nächsten Monaten weniger werden, weil die Vorzüge einer gewissen Selbstkontrolle erkannt werden. Hilfestellungen habe ich vielen öffentlichen Stellen zwischenzeitlich gegeben und umfassende Hinweise bereits frühzeitig veröffentlicht. Meine Bekanntmachung zu § 10, zum Verzeichnis automatisierter Verarbeitungsverfahren ist in diesem

Tätigkeitsbericht unter 16.1.1 und auf meiner Internetpräsenz unter www.datenschutz.sachsen.de zu finden.

Sofern davon ausgegangen wird, dass die Bestellung behördlicher Datenschutzbeauftragter nicht nutzbringend ist, werden die datenschutzrechtlichen und datensicherheitstechnischen Fragestellungen häufig verkannt. Der Bedarf einer behördlichen datenschutzrechtlichen Beratung wird ab einer gewissen Größe der Dienststelle regelmäßig vorausgesetzt werden können.

Nicht wenige Behörden, die schon seit vielen Jahren über einen Datenschutzbeauftragten verfügen, haben meiner Einschätzung nach nicht realisiert, dass nach § 11 Abs. 1 Satz 6 der Neufassung des Sächsischen Datenschutzgesetzes der Sächsische Datenschutzbeauftragte über die Bestellung eines (behördlichen) Datenschutzbeauftragten zu unterrichten ist. Ich empfehle, auch Bestellungen vor der Neufassung des Gesetzes aus Gründen der Rechtssicherheit zu bekräftigen und die Personalakte - sofern es sich um einen Beschäftigten der Stelle handelt - zu ergänzen.

Über die Bestellungen hat meine Behörde ein Register zu führen. Mir sind Name und Tag der Bestellung mitzuteilen. Das entsprechende Meldeformular ist meiner Bekanntmachung als Anhang beigefügt. An dieser Stelle möchte ich auf meine Bekanntmachung zu § 11 zur Bestellung behördlicher Datenschutzbeauftragter mit Meldeformular vom 11. März 2004, Neufassung vom 12. September 2005, zu finden unter 16.1.2 und im Internet unter www.datenschutz.sachsen.de, hinweisen.

Bestellte behördliche Datenschutzbeauftragte bedürfen zur Einsicht in Personalakten und anderer einem besonderen Verschwiegenheitsschutz unterliegenden Unterlagen, insbesondere bei Amts- oder Berufsgeheimnissen, wie z. B. bei der ärztlichen Schweigepflicht, der Einwilligung der Betroffenen. Der bestellte Datenschutzbeauftragte hat immer, ebenso wie der Landesbeauftragte, den Grundsatz der Erforderlichkeit zu beachten.

*2. Bestellung des behördlichen Datenschutzbeauftragten gemäß § 11 SächsDSG im Zusammenhang mit Verzeichnis und Vorabkontrolle automatisierter Verarbeitungsverfahren gemäß § 10 Sä*chsDSG

Mit dem Inkrafttreten der gesetzlichen Neuerung der Bestellung eines Datenschutzbeauftragten nach § 11 SächsDSG wurde auch den Vorgaben der Art. 18 bis 20 der EG-Datenschutzrichtlinie vom 24. Oktober 1995 entsprochen:

Daten verarbeitende Stellen sind nunmehr verpflichtet, automatisierte Verarbeitungsverfahren vor dem erstmaligen Einsatz oder wesentlichen Änderung dem Sächsischen

Datenschutzbeauftragten (§ 10 Abs. 3 SächsDSG) zu melden. Bei der Verarbeitung besonders "sensibler" Daten sind durch den Datenschutzbeauftragten Vorabkontrollen (§ 10 Abs. 5 SächsDSG) vorzunehmen. An dieser Stelle möchte ich auf meine Bekanntmachung zur Vorabkontrolle vom 12. September 2005, zu finden unter 16.1.3 sowie im Internet unter www.datenschutz.sachsen.de, hinweisen. Ist kein Datenschutzbeauftragter bestellt worden, hat meine Behörde über die gemeldeten Verfahren ein Register zu führen (§ 10 Abs. 1 i. V. m. § 31 SächsDSG).

Der Gesetzgeber hat darauf verzichtet, *alle* Behörden zu verpflichten, einen behördlichen Datenschutzbeauftragten zu bestellen. Dies hätte nämlich bedeutet, dass auch kleine öffentliche Stellen (z. B. Bezirksschornsteinfegermeister und Notare) dieser Pflicht unterworfen wären.

Etliche öffentliche Stellen im Lande haben nach dem Inkrafttreten der Neufassung des Sächsischen Datenschutzgesetzes behördliche Datenschutzbeauftragte gemäß § 11 SächsDSG bestellt. Große Organisationseinheiten haben Beschäftigte aus Bereichen mit „verwandten“ Aufgabenbereichen zu Datenschutzbeauftragten bestellt. (z. B. Sachbearbeitung datenschutzrechtlicher Einzelfragen, zentrale Bearbeitung von Auskunftsersuchen, Behördenselbstschutz, allgemeine Sicherheitsfragen). Nicht selten handelt es sich bei der Tätigkeit des Datenschutzbeauftragten um eine neben einer Hauptaufgabe übertragene Funktion. Es empfiehlt sich, in diesen Fällen eine Festlegung in Bezug auf die Arbeits-Anteile vorzunehmen.

3. Interessenkollisionen bei der Bestellung des Datenschutzbeauftragten

Bei der Bestellung eines Datenschutzbeauftragten nach § 11 SächsDSG sind Interessenkollisionen vorstellbar.

Eine sächsische Behörde teilte mir z. B. mit, dass die Bestellung eines Abteilungsleiters (gleichzeitige Tätigkeit als stellvertretender Behördenleiter) wegen der trennenden Bereichsaufteilung für sie kein datenschutzrechtliches Problem darstelle. Der Auffassung, dass es wegen einer arbeitsteiligen Bereichsstruktur nicht zu Interessenkollisionen bei der Tätigkeit als behördlicher Datenschutzbeauftragter kommt, konnte ich nicht beitreten. Bereits aufgrund der Tätigkeit als Abwesenheitsvertreter sah ich ein erhebliches Konfliktpotential.

Auch durch das besondere dienstliche Näheverhältnis zum Behördenleiter können Interessenkonflikte entstehen, wenn Bedienstete bei der Erfüllung ihrer Aufgaben als behördlicher Datenschutzbeauftragter dem Leiter der Behörde unmittelbar unterstellt und weisungsfrei sein sollen (§ 11 Abs. 2 Satz 2 SächsDSG). Weisungsfrei bedeutet, dass die Behördenleitung nicht vorschreiben darf, wie er seinen Aufgaben nachzugehen

hat und welche Konsequenzen er aus seinen Erkenntnissen ziehen muss. Vielmehr entscheidet er selbst über den Zeitpunkt und die Art und Weise seines Tätigwerdens. Die Weisungsfreiheit ist jedoch strikt an die Funktion Aufgabenerfüllung als Datenschutzbeauftragter gebunden. Nimmt der Datenschutzbeauftragte neben seiner Funktion noch weitere Aufgaben wahr, können sich Spannungsverhältnisse zur eigentlichen Hauptaufgabe ergeben. Dem Datenschutzbeauftragten kommt gegenüber der Behörde, gegebenenfalls auch gegenüber Mitarbeitern und Betroffenen eine koordinierende und beratende - aber bis zu einem gewissen Grad auch eine intern kontrollierende - Funktion zu. Daher sollten Interessenkollisionen zwischen der Tätigkeit als Datenschutzbeauftragter und den sonstigen Aufgaben von weitgehend ausgeschlossen werden. Es gilt das Prinzip, dass der zu Kontrollierende nicht selbst der Kontrolleur sein darf.

Der zu bestellende Datenschutzbeauftragte muss nicht zwingend ein Jurist sein, diese Aufgabe kann auch z. B. ein Mitarbeiter Rechnungswesen, Rechnungsprüfung, Controlling oder Organisation übernehmen - jeder Mitarbeiter, welcher für die Erfüllung seiner Aufgaben die erforderliche Fachkunde und Zuverlässigkeit besitzt. Darüber hinaus erfordert die Tätigkeit als Datenschutzbeauftragter auch ein hohes Maß an Konflikt- und Kooperationsfähigkeit sowie Durchsetzungsvermögen. Dies erscheint mir besonders wichtig, wenn es darum geht, den datenschutzrechtlichen Erfordernissen Geltung zu verschaffen und im Sinne der Einhaltung des Datenschutzes angemessene Lösungen bei oft widerstreitenden Interessenlagen herbeizuführen.

1.4 Mitwirkungspflichten I

Obwohl bei meinen Kontrollen die überprüften Stellen fast immer anstandslos ihren Pflichten nachkommen, gibt es doch vereinzelt Amtsträger, die sich in ihrem Tun und Handeln vom Datenschutzbeauftragten nachhaltig gestört fühlen und sich widerspenstig zeigen. Das dämpft nicht etwa meinen Aufklärungseifer, sondern verstärkt ihn vielmehr.

Im vorliegenden Fall wollten meine Mitarbeiter aufgrund einer Petition ohne Vorankündigung - sonst wäre der Erfolg möglicherweise gefährdet gewesen - eine Kontrolle durchführen.

Nachdem sie sich bei dem zuständigen Amtsleiter der Kommune gemeldet hatten, zeigte sich dieser unwillig. Obwohl ihm - einem Volljuristen - auf seine Frage nach der Rechtsgrundlage der Kontrolle der Gesetzestext zum Lesen übergeben worden war, bezweifelte er nach der Lektüre der einschlägigen Paragraphen seine Zuständigkeit und leitete zudem daraus her, dass kein Anspruch auf mündliche Auskunft und umfängliche Akteneinsicht bestehe. Er äußerte sich hinsichtlich der Kontrolle folgendermaßen: Eine Kooperation erfolge später, „jedenfalls nur schriftlich“, zu einem Zeitpunkt, den er fest-

lege. Hier und heute gebe er keine Auskunft. Meine Kontrolle sei unverhältnismäßig, nicht zumutbar. Das Auftreten zu dritt sei unverhältnismäßig, stelle ein „Überfallkommando“ dar und sei als „Einschüchterungsversuch“ zu werten. Meine Entscheidung sei insoweit „ermessensfehlerhaft“ und ich sollte eine Begründung dafür liefern, dass ich unangemeldet erscheine. Im Übrigen sei es formell fehlerhaft, dass ich nicht über den Oberbürgermeister einen Termin gemacht habe. Er sei nicht zuständig für unser Kontrollbegehren, es gebe von ihm keine „Zuarbeit“.

In der Sache erhielten meine Mitarbeiter an diesem Tag keine Auskunft und wurde vielmehr der Räume verwiesen.

Es steht im „Ermessen“ des Sächsischen Datenschutzbeauftragten, das „ob“, „wann“ und „wie“ seiner Kontrollen selbst zu bestimmen. In § 28 Abs. 2 SächsDSG ist vorgesehen, dass ich mich vor der Kontrolle beim Leiter der betroffenen Stelle melde und ihn vom Beginn der Kontrolle informiere. Diese neu ins Sächsische Datenschutzgesetz aufgenommene Vorschrift verpflichtet aber nicht zur „Vorankündigung“ von Kontrollen. Eine Information unmittelbar vor Beginn der Kontrolle ist ausreichend (vergleiche auch die Regierungsbegründung).

Der Behördenleiter des Ordnungsamtes war der zuständige in § 28 Abs. 2 SächsDSG benannte Leiter der betroffenen Stelle. Das Sächsische Datenschutzgesetz geht hier vom funktionalen Stellenbegriff aus.

Gleichwohl braucht der Behördenleiter, der ja vielmals nicht in allen Details der Sachen Kenntnis haben kann und muss, meine Fragen nicht selbst beantworten. Es genügt, wenn er mir Zutritt zu allen Räumen und Unterlagen verschafft sowie einen auskunftsfähigen, das heißt sachlich informierten Bediensteten seiner Behörde zur Verfügung stellt. § 28 Abs. 1 SächsDSG normiert unmissverständlich, dass alle öffentlichen Stellen dazu verpflichtet sind, den Sächsischen Datenschutzbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen.

Nach dieser ersten misslungenen Kontrolle und nachdem ich mit der Verwaltungsspitze Rücksprache gehalten hatte, suchten meine Mitarbeiter die Behörde am nächsten Tag erneut auf. Der Leiter wollte wiederum keine Auskünfte zur Sache tätigen. Er nahm meine Fragen schriftlich auf und wollte sie zu gegebener Zeit (die er bestimme) schriftlich beantworten. Zudem verwies er meine Mitarbeiter an den Datenschutzkoordinator der Stadt.

Bemerkenswert war, dass er, obwohl er einen Tag Zeit hatte, sich immer noch nicht über meine Kontrollbefugnisse und seine Mitwirkungspflicht ausreichend informiert hatte. Den Ablauf der Kontrollen bestimmt selbstverständlich der Sächsische Daten-

schutzbeauftragte. Dazu gehört auch, wann und wie sich die Behörde äußert. In begründeten Fällen, wenn etwa eine umfangreiche Recherche erforderlich ist, die sich auch nach meiner Einschätzung nicht ad hoc bewerkstelligen lässt, kann eine Beantwortung von Fragen auf einen späteren Zeitpunkt oder gar in die Schriftform verschoben werden.

Um die Kontrolle an diesem Tag endlich erfolgreich durchführen zu können, war eine nochmalige Rücksprache mit einem dem Behördenleiter weisungsbefugten Beigeordneten der Stadt erforderlich. Nach mehreren Telefonaten erhielt der Behördenleiter die Weisung, uns sofort alle Auskünfte zu geben und Einsicht in alle Unterlagen zu gewähren. In der Sache konnte nun endlich mit der eigentlichen Kontrolle begonnen werden.

Ich habe letztendlich von einer Beanstandung abgesehen, da die Rathausspitze willens war, mich zu unterstützen. Ansonsten bin ich gewillt, mit allen mir zur Verfügung stehenden Mitteln meinen Kontrollanspruch in solchen Fällen durchzusetzen.

1.5 Mitwirkungspflichten II

Im Rahmen der datenschutzrechtlichen Überprüfung einer Eingabe bat ich eine Notarin um einige Angaben zu einem ihrer Verfahren, an dem der Petent beteiligt war. In ihrem Antwortschreiben berief sich die Notarin auf § 18 BNotO und erklärte, erst dann Auskunft zu geben, wenn sämtliche Beteiligte sie von ihrer Verschwiegenheitspflicht befreit hätten. Des Weiteren verwies sie auf den Vorrang bereichsspezifischen (Bundes-)Berufsrechts vor allgemeinen (landesrechtlichen) Vorschriften.

Notare sind gemäß § 1 BNotO unabhängige Träger eines öffentlichen Amtes, die für die Beurkundung von Rechtsvorgängen und andere Aufgaben auf dem Gebiet der vorsorgenden Rechtspflege in den Ländern bestellt werden. Die Notare des Freistaates Sachsen sind öffentliche Stellen des Freistaates Sachsen im Sinne von § 2 Abs. 1 SächsDSG; sie unterstehen gemäß § 92 Nr. 3 BNotO der Aufsicht des SMJus.

Das Sächsische Datenschutzgesetz findet auf die Verarbeitung personenbezogener Daten in sächsischen Notariaten Anwendung.

Dagegen spricht nicht, dass spezialgesetzliche Vorschriften in der Bundesnotarordnung und dem Beurkundungsgesetz datenschutzrechtliche Bezüge aufweisen. Soweit diese Spezialvorschriften die Verarbeitung personenbezogener Daten regeln, gehen sie dem Sächsischen Datenschutzgesetz vor, dessen Regelungen insoweit subsidiär sind (§ 2 Abs. 4 SächsDSG).

Es ist jedoch zu berücksichtigen, dass einzelne - in verschiedenen Spezialgesetzen zu findende - Vorschriften zum Schutz personenbezogener Daten das allgemeine Datenschutzrecht nicht insgesamt, sondern eben nur insoweit verdrängen, wie sie den Schutz personenbezogener Daten regeln (§ 2 Abs. 4 SächsDSG). Ein hierfür typischer Fall ist die gesetzlich normierte Datenschutzkontrolle: Die datenschutzrechtliche Kontrolle der sächsischen Notariate (als öffentliche Stellen des Freistaates Sachsen) obliegt dem Sächsischen Datenschutzbeauftragten (§ 27 Abs. 1 SächsDSG). Die Kontrollbefugnis des Sächsischen Datenschutzbeauftragten korrespondiert mit der Pflicht der öffentlichen Stellen, den Sächsischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ausdrücklich beschränkt sich die Zuständigkeit des Sächsischen Datenschutzbeauftragten nicht auf die Kontrolle der Einhaltung des Sächsischen Datenschutzgesetzes; gemäß § 27 Abs. 1 SächsDSG kontrolliert er auch die Einhaltung anderer Vorschriften über den Datenschutz. Wenden öffentliche Stellen des Freistaates Sachsen in Ausübung ihrer gesetzlich übertragenen Tätigkeit Bundesrecht an und enthält das angewandte Recht Regelungen zum Schutz personenbezogener Daten, kontrolliert der Sächsische Datenschutzbeauftragte die Einhaltung bundesrechtlicher Vorschriften über den Datenschutz. Andernfalls entstünden nicht hinnehmbare kontrollfreie Räume. Der Sächsische Datenschutzbeauftragte kontrolliert beispielsweise die Verarbeitung personenbezogener Daten in den Ausländerbehörden, die den Vorschriften des (bundeseinheitlichen) Ausländergesetzes unterliegt, ebenso wie die Einhaltung (bundeseinheitlicher) datenschutzrechtlicher Vorschriften in der Strafprozessordnung durch sächsische Staatsanwaltschaften.

Der Sächsische Datenschutzbeauftragte ist auch zur Kontrolle der Einhaltung der Datenschutzvorschrift des § 18 BNotO befugt; der Notar ist insoweit verpflichtet, Fragen zu beantworten und dem Sächsischen Datenschutzbeauftragten - auch und gerade vorgangsbezogene - Auskünfte zu erteilen. Die Kontrolle der Einhaltung des § 18 BNotO darf nicht mit dem Hinweis auf eben diese Vorschrift verhindert werden.

Dass auch die Datenverarbeitung, die besonderen Berufs- oder Amtsgeheimnissen unterliegt, durch den Sächsischen Datenschutzbeauftragten kontrolliert wird, normiert § 27 Abs. 1 Satz 2 SächsDSG. Im Zuständigkeitsbereich des Bundesbeauftragten für den Datenschutz erstreckt sich dessen Kontrolle gemäß § 24 Abs. 2 Nr. 2 BDSG auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Gemäß § 24 Abs. 6 BDSG gilt § 24 Abs. 2 BDSG entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind. Zwar verdrängen gemäß § 1 Abs. 2 Nr. 2 BDSG die Landesdatenschutzgesetze in ihrem Anwendungsbereich das Bundesdatenschutzgesetz - insofern ist die Übertragung der Kontrollbefugnis im Sächsischen Datenschutz-

gesetz maßgeblich -, § 24 Abs. 2 und 6 BDSG zeigen aber, dass auch der Bundesgesetzgeber die Notwendigkeit sah, Daten, die besonderen Berufs- oder Amtsgeheimnissen unterliegen, zum Zweck einer effektiven datenschutzrechtlichen Kontrolle der kontrollierenden Stelle zugänglich zu machen.

Die Argumentation, landesgesetzliche Regelungen - hier die des Sächsischen Datenschutzgesetzes - könnten bundesrechtliche Vorschriften nicht verdrängen, geht hier fehl, da es vorliegend gar nicht um die Rangordnung von Gesetzen geht, die denselben Regelungsinhalt haben. Der Grundsatz „Bundesrecht bricht Landesrecht“ (Art. 31 GG) kommt mangels tatbestandlicher Voraussetzungen hier nicht zur Anwendung.

Die Vorschrift des § 18 BNotO steht vorliegend nicht in Konkurrenz mit den die Kontrollbefugnisse des Sächsischen Datenschutzbeauftragten regelnden Vorschriften des Sächsischen Datenschutzgesetzes. Der Notar als öffentliche Stelle des Freistaates Sachsen ist gemäß § 28 Abs. 1 SächsDSG verpflichtet, den Sächsischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und Auskunft zu Fragen zu geben. Auf dieser gesetzlichen Grundlage sind für Kontrollzwecke des Datenschutzbeauftragten gegebenenfalls eben auch personenbezogene Daten aus einem konkreten Vorgang zu offenbaren, der Anwendungsbereich von § 18 BNotO ist insoweit nicht eröffnet. Es ist sinnwidrig, dem zur Kontrolle der Einhaltung der Verschwiegenheitspflicht Befugten eine erbetene Auskunft unter Hinweis auf eben diese Verschwiegenheitspflicht zu verweigern.

Mit diesen datenschutzrechtlichen Kontrollbefugnissen ist auch keine Absenkung des vom Notar gemäß § 18 BNotO geforderten hohen Schutzniveaus verbunden. Gemäß § 25 Abs. 6 SächsDSG sind der Sächsische Datenschutzbeauftragte und seine Mitarbeiter verpflichtet, über die ihnen bei ihrer amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit gegenüber jedermann zu wahren. Eine datenschutzrechtliche Aufsichtsbehörde, deren Kontrolltätigkeit den Schutz personenbezogener Daten gegenüber dem (spezialgesetzlich geregelten) Schutzniveau bei der kontrollierten Stelle vermindert, führte die Grundsätze des Datenschutzes ad absurdum, § 25 Abs. 6, 7 SächsDSG treffen hier die entsprechenden Vorkehrungen. Die Verschwiegenheitspflicht des Sächsischen Datenschutzbeauftragten entspricht in ihrer Qualität der Verschwiegenheitspflicht des Notars.

Nachdem auch das SMJus als oberste Aufsichtsbehörde für die sächsischen Notare davon ausgeht, dass die Verschwiegenheitspflicht des Notars nach § 18 BNotO die Kontrollbefugnisse des Sächsischen Datenschutzbeauftragten nicht einschränkt und die Notarin diese Einschätzung zur Kenntnis genommen hatte, erteilte sie schließlich die erbetenen Auskünfte.

1.6 Hinweise Bediensteter öffentlicher Stellen an den Sächsischen Datenschutzbeauftragten

Immer wieder werde ich von Mitarbeitern im öffentlichen Dienst und von Amtsträgern auf datenschutzrechtlich zu hinterfragende oder sogar offenkundige Datenschutzverstöße aufmerksam gemacht. Ich gehe diesen natürlich nach.

In einem Fall hatte ich die Frage zu beantworten, ob eine bestimmte Verarbeitung personenbezogener Daten in einer nichtöffentlichen Ausschusssitzung eines Stadtrates datenschutzgerecht erfolgte. Ein Datenschutzverstoß konnte letztendlich nicht festgestellt werden. Die Stadtverwaltung ging jedoch aufgrund meines Tätigwerdens davon aus, dass ein Stadtrat bzw. Ausschussmitglied mir gegenüber Sitzungsgeheimnisse preisgegeben habe und der Oberbürgermeister der Stadt wandte sich im Nachgang folgendermaßen an mich: „Um prüfen zu können, ob seitens der Teilnehmenden eine Ordnungswidrigkeit bzgl. ihrer Verpflichtung zur Verschwiegenheit vorliegt, bitten wir Sie hiermit ..., uns den Namen der Person zu nennen, von der Sie den Hinweis erhalten haben ...“ Da es sich um Hinweise aus einer nichtöffentlichen Sitzung handele, sehe sich die Stadt „gehalten, einer möglichen Verletzung der Verschwiegenheitspflicht nachzugehen und eine Prüfung des Sachverhalts vorzunehmen“. Dies sei nur möglich, wenn ihr „die Auskunftsperson“ im Wege der Amtshilfe benannt werde.

Zu der Frage, ob sich ein Gemeinderat, der sich mit einer datenschutzrechtlichen Fragestellung an mich wendet, damit gegen § 37 Abs. 2 SächsGemO und damit gegen die Verschwiegenheitspflicht der Gemeinderäte verstoßen haben könnte, habe ich nachstehende Auffassung vertreten.

Verschwiegenheitspflichten können nicht zur Geheimhaltung rechtsfehlerhafter oder sogar grob rechtsverletzender Vorgänge genutzt werden.[1] Wenn sich mithin ein Gemeinderat als Träger der Verschwiegenheit aber aus Datenschutzgründen nicht ohne weiteres an die Öffentlichkeit zu wenden berechtigt ist - entsprechende Verstöße habe ich im Übrigen schon häufiger moniert -, so darf ihm jedenfalls die Hinwendung zu den Ordnung und Kontrolle der Verwaltung gewährleistenden Aufsichtsbehörden und Institutionen nicht verwehrt sein. Vorliegend war daher schlicht die Frage zu klären, ob sich Gemeinderäte auch in Bezug auf (datenschutz-)rechtlich zu klärende Sachverhalte aus nichtöffentlicher Sitzung selbständig an den Sächsischen Datenschutzbeauftragten wenden dürfen. Ich habe dies bejaht.

Ich teilte der Stadt daher Folgendes mit: „Gegenüber Fach- und Rechtsaufsichtsbehörden gilt die Verschwiegenheitspflicht innerhalb deren Informationsrecht nicht. Dies

[1] Vgl. BVerfG Beschl. vom 28. April 1970 - 1 BvR 690/65 („Pätsch-Fall“ = BVerfGE 28, 191).

gilt auch für Datenschutzaufsichtsbehörden, wie den Sächsischen Datenschutzbeauftragten. Es liegt vorliegend gegenüber dem Sächsischen Datenschutzbeauftragten weder eine Verschwiegenheitspflicht vor, noch ist eine Aussagegenehmigung erforderlich. Nach § 27 Abs. 1 SächsDSG erstreckt sich die Kontrolle des Sächsischen Datenschutzbeauftragten auch auf die Behandlung personenbezogener Daten bei Verarbeitungsvorgängen, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Um solche Vorgänge handelt es sich bei nicht-öffentlichen Stadtratssitzungen, bei denen personenbezogene Daten verarbeitet werden. Der Sächsische Datenschutzbeauftragte und seine Mitarbeiter sind nach § 25 Abs. 6 SächsDSG verpflichtet, über die ihnen bei ihrer amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit gegenüber jedermann zu wahren. Ich habe klargestellt, dass mir gegenüber die Verschwiegenheit wegen der datenschutzrechtlichen Fragestellung nicht zu wahren gewesen ist und habe das Ersuchen des Oberbürgermeisters um Namensnennung zurückgewiesen.

Im Übrigen gilt Folgendes: Nicht im Sinne von § 24 Abs. 1 SächsDSG Betroffene, die Mitarbeiter der Verwaltung sind, haben sich zwar an den Dienstweg zu halten.[2] Diese Pflicht ist aber von der Pflicht zur Verschwiegenheit zu trennen. Der „Dienstweg“ stellt eine interne Verwaltungsregelung dar, um das Funktionieren der Verwaltung zu gewährleisten und ein geordnetes Wirken nach außen sicherzustellen. Amtsträger, die sich mit datenschutzrelevanten Hinweisen an mich wenden, tun dies jedoch nicht selten als Amtsträger „in persona“ und agieren ggf. außerhalb des Dienstwegs. Dies zu bewerten ist allerdings nicht meine Aufgabe. Schon gar nicht sehe ich es als meine Verpflichtung an, mir datenschutzrelevante Hinweise gebende Bedienstete gegenüber deren Dienststelle zu offenbaren. Für kommunale Mandatsträger (wie im geschilderten Fall) gilt der „Dienstweg“ im Unterschied zu Beschäftigten der Gemeindeverwaltung ohnehin nur eingeschränkt.

1.7 Öffentliche Stellen nach dem neuen Sächsischen Datenschutzgesetz

Zu § 2 Abs. 1 bis 3 SächsDSG in seiner neuen Fassung gab es einige Anfragen und Streitpunkte, mit denen ich mich auseinanderzusetzen hatte. Ich vertrete nachstehende Rechtsauffassung.

1. Eigenbetriebe

Eigenbetriebe sächsischer Gebietskörperschaften (z. B. Gemeinden, Landkreise, Freistaat) sind öffentliche Stellen im Sinne von § 2 Abs. 1 SächsDSG. Sie sind Teil der jeweiligen Gebietskörperschaft, ohne eine eigene Rechtspersönlichkeit zu haben. Mir ist

[2] So auch Ancôt, Sächsisches Datenschutzgesetz, Kommentar, 2. Auflage 2004, § 24 Rdnr. 4.

gleichwohl die Frage gestellt worden, ob nicht Krankenhäuser, die als kommunale Eigenbetriebe organisiert sind, öffentlich-rechtliche Unternehmen im Sinne von § 2 Abs. 3 SächsDSG seien und sich die Verarbeitung personenbezogener Daten daher in diesen Einrichtungen nach Bundesdatenschutzgesetz richte. Die Eigenbetriebe würden am Wettbewerb teilnehmen. Nach dem Wortlaut des § 2 Abs. 3 SächsDSG sind öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, nur solche mit „eigener Rechtspersönlichkeit“. „Eigene Rechtspersönlichkeit“ bedeutet, dass es sich um eine eigene juristische Person (hier: des öffentlichen Rechts) handeln muss. Daraus folgt die Rechtsfähigkeit. Krankenhäuser der Gemeinden oder des Landkreises, die Eigenbetriebe sind, sind aber nur Teil der juristischen Person „Gebietskörperschaft“, der Gemeinde oder des Landkreises. Ein Eigenbetrieb ist nicht rechtsfähig, d. h. er ist nicht selbständiger Träger von Rechten und Pflichten, sondern diese sind immer abgeleitet von der Gebietskörperschaft. Haushalterische Trennungen und Freiheiten, die Einsetzung von Verwaltungsräten, sind finanztechnische bzw. eigenorganisatorische Maßnahmen, die an der rechtlichen Einordnung nichts ändern. Eigenbetriebe fallen aufgrund des funktionalen Stellenbegriffs unter § 2 Abs. 1 SächsDSG (§ 2 Abs. 2 SächsDSG gilt nur für juristische Personen des Privatrechts), d. h. ein Krankenhaus, das als Eigenbetrieb geführt wird, ist eine öffentliche Stelle im Sinne des § 2 Abs. 1 SächsDSG. Der Sächsische Datenschutzbeauftragte ist zuständige Datenschutzaufsichtsbehörde, § 27 Abs. 1 SächsDSG. Für Eigenbetriebe anderer Art gilt Entsprechendes.

2. Juristische Personen des Privatrechts

Es ist mir gegenüber die Auffassung vertreten worden, dass es sich bei Verkehrs- und Krankenhausbetrieben, die als juristische Personen des Privatrechts (zumeist GmbHs) organisiert sind und deren Eigentümer oder Gesellschafter mehrheitlich öffentliche Stellen im Sinne von § 2 Abs. 1 SächsDSG sind (z. B. Gemeinde(n), Landkreis(e)), nicht um öffentliche Stellen nach § 2 Abs. 2 SächsDSG handele. Die Verarbeitung personenbezogener Daten richte sich nach § 2 Abs. 3 SächsDSG bzw. dem BDSG. Auch diese rechtliche Einschätzung ist nach meiner Überzeugung nicht zutreffend. Das Bundesdatenschutzgesetz ist subsidiär und nur dann anzuwenden, wenn der Datenschutz nicht bereits durch landesgesetzliche Bestimmungen geregelt wird (vgl. § 2 Abs. 4 BDSG).

Sofern ein Betrieb als juristische Person des Privatrechts von öffentlichen Stellen im Sinne von § 2 Abs. 1 SächsDSG, z. B. der Gemeinde, dem Landkreis oder von mehreren öffentlichen sächsischen Stellen mehrheitlich beherrscht, aber auch durch sich im Eigentum der öffentlichen Stellen befindende weitere juristische Personen des Privatrechts, also mittelbar (vgl. § 2 Abs. 2 Satz 2 SächsDSG) mehrheitlich beherrscht wird (§ 2 Abs. 2 Satz 1 SächsDSG: „… absolute Mehrheit der Anteile oder absolute

Mehrheit der Stimmen …“), richtet sich die Verarbeitung personenbezogener Daten nach sächsischem Recht. Mit dem Betreiben eines Verkehrsunternehmens, eines Krankenhauses oder eines Versorgungsunternehmens in privater Rechtsform durch eine Kommune werden nämlich auch öffentliche Aufgaben der Verwaltung im Sinne von § 2 Abs. 2 SächsDSG wahrgenommen. Z. T. ergibt sich das auch bereits aus Spezialgesetzen, so aus § 3 Abs. 1 ÖPNVG. Ferner gilt für die Kommunen allgemein Folgendes: Die Gemeinden erfüllen nach § 2 Abs. 1 SächsGemO in ihrem Gebiet im Rahmen ihrer Leistungsfähigkeit alle öffentlichen Aufgaben in eigener Verantwortung und schaffen die für das Wohl ihrer Einwohner erforderlichen öffentlichen Einrichtungen. Die Landkreise erfüllen nach § 2 Abs. 1 SächsLKrO alle überörtlichen die Leistungsfähigkeit der einzelnen kreisangehörigen Gemeinde übersteigenden Verwaltungsaufgaben. Dazu zählen auch für das soziale Wohl der Einwohner erforderliche öffentliche Einrichtungen. Zu diesen zählen z. B. Krankenhäuser. Die Gesundheitsversorgung, die Energie- und Wasserversorgung und das Betreiben einer Nahverkehrsinfrastruktur sind insofern öffentliche Aufgabe der Verwaltung. Damit im Einklang stehen die Bestimmungen des § 96 Abs. 1 SächsGemO bzw. § 63 SächsLKrO i. V. m. § 96 Abs. 1 SächsGemO. Hiernach darf die Gemeinde bzw. der Landkreis nur Privatunternehmen zur öffentlichen Aufgabenerfüllung betreiben, so dass die Wahrnehmung von Aufgaben der öffentlichen Verwaltung im Sinne von § 2 Abs. 2 SächsDSG als erfüllt angesehen werden muss, denn andernfalls wäre das Betreiben der jeweiligen Unternehmen in privater Rechtsform durch Gemeinden und Landkreise kommunalrechtlich nicht zulässig gewesen. Kommunalwirtschaft bzw. die staatliche Unternehmenswirtschaft sind Teil des Verwaltungsrechts und daher auch nach dem Sächsischen Datenschutzgesetz entsprechend einzuordnen. Die Bindung an die Aufgaben des Verwaltungsträgers gilt grundsätzlich auch bei juristischen Personen des Privatrechts, die keine Unternehmen sind und von denen nur wenige Fälle bekannt sind.

Zu dem Begriff der „Aufgabe der öffentlichen Verwaltung“ in § 2 Abs. 2 SächsDSG: Für diesen Begriff kann folgende Charakterisierung herangezogen werden: „Unter öffentlichen Aufgaben versteht man ... solche, deren Erfüllung im öffentlichen Interesse liegt, die aber auch von Privaten in gleicher Weise wie vom Staat wahrgenommen werden können.“ (Ossenbühl, Staatshaftungsrecht, 5. Auflage 1998, S. 24) Alles, was die öffentliche Verwaltung befugtermaßen und im öffentlichen Interesse tut, ist eine „Aufgabe“ der öffentlichen Verwaltung. Die Tatsache, dass eine öffentlich rechtliche Körperschaft sich zur Erfüllung ihrer Aufgabe in ein privatrechtliches Gewand kleidet, ändert am Charakter der öffentlichen Aufgabe nichts. Davon gehen die kommunalrechtlichen Bestimmungen und das Sächsische Datenschutzgesetz aus. Der Begriff ist damit zugegebenermaßen weitgehend konturenlos. Maßgebend sind nach § 2 Abs. 2 SächsDSG damit nämlich regelmäßig nur die Anteile der öffentlichen Stelle(n) an der

juristischen Person des Privatrechts. Insbesondere bei den Gemeinden sind die Aufgaben des örtlichen Wirkungskreises nur durch Zuweisungen von Aufgaben an andere Verwaltungsträger begrenzt. Die gemeindlichen Aufgaben sind nicht als Katalog gesetzlich beschreiben. Wegen der Weite des Aufgabenkreises, den die Gemeinden in Anspruch nehmen, dienen insofern auch alle privatrechtlich organisierten kommunalen Unternehmen der Erfüllung der öffentlichen Aufgaben, gleichgültig, ob es sich um Verkehrsunternehmen, um Strom- und Wasserversorgungs- oder Wohnungsbetriebe handelt. Zu beachten ist lediglich, dass das Sächsische Datenschutzgesetz auf juristische Personen und sonstige Vereinigungen des öffentlichen Rechts, an denen zwar juristische Personen des öffentlichen Rechts mehrheitsbeteiligt sind, die aber offensichtlich keinen Gemeinwohlbezug aufweisen (reine Finanzbeteiligungen), keine Anwendung findet.

3. Privatrechtlich organisierte Krankenhäuser

Mir gegenüber ist von einem Verein aus dem Bereich des Gesundheitswesens beharrlich die rechtsirrige Meinung entgegengehalten worden, es handele sich bei privatrechtlich organisierten Krankenhäusern, die mehrheitlich von öffentlichen Stellen beherrscht werden, um Stellen im Sinne von § 2 Abs. 3 SächsDSG. Auch juristische Personen des Privatrechts fielen unter § 2 Abs. 3 SächsDSG. Bei der rechtlichen Einordnung der Stellen ist der gesetzliche Wortlaut maßgebend. Auslegungsspielräume, wonach entgegen dem Wortlaut auch privatrechtlich organisierte Unternehmen unter die Vorschrift fallen könnten, sind nicht gegeben, da auch nach Sinn und Zweck des § 2 Abs. 3 juristische Personen des Privatrechts gerade nicht erfasst werden sollten, wie zudem die beispielhafte Aufzählung der juristischen Personen des öffentlichen Rechts in der Vorschrift selbst verdeutlicht. Da der Wortlaut nicht „öffentliche Stellen“ oder „öffentliche Unternehmen“ lautet, sondern öffentlich-rechtliche Unternehmen mit eigener Rechtspersönlichkeit, können Stellen nicht gleichzeitig § 2 Abs. 2 und § 2 Abs. 3 SächsDSG unterfallen. Ich bin daher auch dieser Einzelmeinung entgegengetreten.

4. Universitätsklinika

Mir ist die Frage gestellt worden, ob nicht auch die Universitätsklinika als Anstalten des öffentlichen Rechts von § 2 Abs. 3 SächsDSG erfasst werden. Die Universitätsklinika sind zunächst wie Eigenbetriebe auch Stellen im Sinne von § 2 Abs. 1 SächsDSG. Sie sind sonstige der Aufsicht des Freistaates Sachsen unterstehende juristische Personen des öffentlichen Rechts (vgl. den Wortlaut von § 2 Abs. 1 SächsDSG). Sie stehen nach § 3 Abs. 2 UKG unter Aufsicht des Freistaates (Rechtsaufsicht des SMWK). Die Universitätsklinika sind jedoch keine öffentlichen-rechtlichen Unternehmen mit eigener Rechtspersönlichkeit, die am Wettbewerb teilnehmen und damit keine öffentlichen Stellen nach § 2 Abs. 1 SächsDSG, die gleichzeitig § 2 Abs. 3 SächsDSG unterfallen.

Es fehlt am Tatbestandsmerkmal des Wettbewerbsunternehmens. Zwar werden in den Universitätsklinika Behandlungen wie in anderen Krankenhäusern auch durchgeführt, wodurch eine gewisse Konkurrenzsituation entsteht. Wettbewerb und Gewinn sind jedoch nicht beherrschender Zweck. Die Universitätsklinika erfüllen in erster Linie Aufgaben und Funktionen, die von anderen Krankenhäusern nicht wahrgenommen werden. Nach dem Universitätsklinika-Gesetz ist die Tätigkeit der Krankenhäuser mit Forschung und Lehre verbunden. In § 1 Abs. 4 UKG wird festgelegt: “Das Universitätsklinikum verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne der Abgabenordnung …“ § 2 Abs. 1 bestimmt u. a.: „… Es gewährleistet in enger Zusammenarbeit mit der Universität und ihrer Medizinischen Fakultät die Verbindung der Krankenversorgung mit Forschung und Lehre. Es wahrt die der Universität eingeräumte Freiheit in Forschung und Lehre und stellt sicher, dass die Mitglieder der Universität die durch Artikel 5 Abs. 3 Satz 1 des Grundgesetzes und Artikel 21 der Verfassung des Freistaates Sachsen verbürgten Grundrechte und die Freiheiten nach § 5 Abs. 2 bis 5 des Gesetzes über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz - SHG) vom 4. August 1993 (GVBl. S. 691), zuletzt geändert durch Gesetz vom 19. August 1998 (GVBl. S. 459), wahrnehmen können …“ Maßgebend für die Einordnung der Universitätsklinika ist, dass die Tätigkeit der Universitätsklinika insgesamt durch die Forschung und Lehre geprägt wird und nicht durch ein Wettbewerbsverhalten. Demgegenüber verfolgen z. B. die Sparkassen als öffentlich-rechtliche, in § 2 Abs. 3 SächsDSG erwähnte Unternehmen und Kreditinstitute keine gemeinnützigen Zwecke. Vielmehr ist deren Zweck gerade die Teilnahme am Wettbewerb (vgl. § 2 Abs. 1 des Gesetzes über die öffentlich-rechtlichen Kreditinstitute im Freistaat Sachsen und die Sachsen-Finanzgruppe).

1.8 Sonstige Fälle

Es gibt Fälle, in denen ich mit Rücksicht auf Petenten oder Bedienstete bzw. schwebende Verfahren hier nur mit größter Zurückhaltung berichten kann.

So habe ich in einem Fall dem Datenschutzbeauftragten eines Sozialleistungsträgers den Rücken stärken müssen, als er nach der pflichtgemäßen Feststellung unter Datenschutzgesichtspunkten unzulänglicher Leistungen eines Auftragsdatenverarbeiters offenbar hat erleben müssen, dass sein oberster Vorgesetzter aus Rücksicht auf eine Person des öffentlichen Lebens, deren Sohn in dem betreffenden auftragsdatenverarbeitenden Unternehmen verantwortlich tätig war, Anstalten machte, zu verhindern, dass die nötigen Schritte gegen den Auftragsdatenverarbeiter eingeleitet wurden.

In einem anderen Fall hat der Freistaat Sachsen durch das Handeln juristisch gut vorgebildeter Bediensteter die Ausbildung des Petenten vorzeitig beendet und in diesem Zu-

sammenhang, insbesondere auch als Mittel zur Absicherung dieser Maßnahme, schwere Datenschutzrechtsverstöße begangen, die ich in langwieriger und mühsamer Kleinarbeit in ihren Einzelheiten habe aufklären können. Hier besteht die Hoffnung, dass die hauptsächliche, ja eigentliche Beeinträchtigung des Petenten, eben diejenige in beruflicher Hinsicht, für die Zukunft doch wohl beseitigt werden kann. Dieser letztere rechtsstaatliche Gewinn hat gegenüber demjenigen rein datenschutzrechtlicher Natur im Vordergrund zu stehen.

2 Parlament

In diesem Jahr nicht belegt.

3 Europäische Union / Europäische Gemeinschaft

In diesem Jahr nicht belegt.

4 Medien

In diesem Jahr nicht belegt.

5 Inneres

5.1 Personalwesen

5.1.1 Verarbeitung von Beschäftigtendaten im Zusammenhang mit vorgesehenen Änderungskündigungen - Sozialauswahl

Im März 2005 erhielt ich Kenntnis von der Verarbeitung personenbezogener Daten durch die Regionalschulämter als Personal verwaltende Stellen der Lehrkräfte an Mittelschulen und Gymnasien. Auf Anordnung des zuständigen Staatsministeriums führten Mitarbeiter der Ämter mit den angestellten Lehrkräften der Mittelschulen und der Gymnasien Personalgespräche und erhoben hierbei tiefgehend Beschäftigtendaten. Hintergrund der Maßnahme waren nach Aussage des Staatsministeriums Überlegungen, dass die Personal verwaltenden Regionalschulämter wegen der Haushaltslage und der zukünftig niedrigeren Schülerzahlen Änderungskündigungen aussprechen sollten. Die Stundenzahlen sämtlicher Lehrer sollten hierbei reduziert werden, um Beendigungskündigungen für einen Teil der Lehrkräfte zu vermeiden. Die Personalgespräche sollten dazu dienen, so das Ministerium, die Datengrundlage in Bezug auf eine mögliche Sozialauswahl zu schaffen. Mehrere Betroffene wandten sich an mich und baten um Klärung datenschutzrechtlicher Fragestellungen, § 24 SächsDSG.

Bei einer Kontrolle im März stellte ich Folgendes fest: Referenten der für die Schularten zuständigen Abteilungen der Regionalschulämter erhoben anhand frei geführter Gespräche mit den Lehrkräften personenbezogene Daten der Betroffenen. Welche Daten erhoben werden sollten, hatte das Ministerium den Regionalschulämtern in einer Handreichung mitgeteilt. Bei den Personalgesprächen wurde auf einen schriftlichen Fragebogen verzichtet, so dass den Mitarbeitern nichts schriftlich vorlag. Es wurden Daten erhoben, die bereits in der Lehrerpersonaldatenbank oder in der Personalakte vorhanden waren, zum anderen aber auch weitergehende Daten, die zum Teil als sensibel einzustufen sind. Begründet wurde die Erhebung der Daten mit einem Aktualisierungsbedarf. Die weitergehende Verarbeitung von zusätzlichen Daten wurde mit der Notwendigkeit gerechtfertigt, den Betroffenen die Gelegenheit zu geben, für sie arbeitsrechtlich günstige Angaben den Personal verwaltenden Stellen mitzuteilen. Das Resultat dieser für die Lehrer nicht transparenten Verfahrensweise war, dass im Übermaß und uneinheitlich personenbezogene Daten über persönliche Verhältnisse der Mitarbeiter verarbeitet worden waren, so u. a. Unterhaltspflichten, die Arbeitslosigkeit des Ehegatten, Schuldenstände oder andere soziale Härtefälle. Eine Einsichtnahme in die Erhebungsblätter bestätigte, dass sensible personenbezogene Daten verarbeitet wurden.

Eine Verarbeitung personenbezogener Daten zur Personalplanung und -wirtschaft ist nach § 37 SächsDSG grundsätzlich zulässig. Hierfür werden auch konkrete und aktuelle

Daten der Beschäftigten benötigt. Auch ist dem Arbeitgeber hinsichtlich des Verfahrens eine gewisse Gestaltungsfreiheit zuzubilligen. Datenschutzrechtliche Grundsätze sind gleichwohl zu beachten. Um eine sachgerechte Entscheidung bei Teilkündigungen vornehmen zu können, kann es zwar notwendig sein, bereits im Vorfeld personenbezogene Daten der Beschäftigten zu erheben. Dem datenschutzrechtlichen Grundsatz der Erforderlichkeit ist aber insofern Rechnung zu tragen, als dass abgestuft vorzugehen ist. Der Kreis der Betroffenen ist durch den Arbeitgeber anhand eines zu erstellenden Kriterienkatalogs möglichst frühzeitig einzugrenzen. Nachdem für Teilkündigungen (objektive) Bedarfskriterien wie Unterrichtsfächer und Ausbildung verarbeitet und ausgewertet worden sind, können bei Bedarf in einem nächsten Schritt weitergehende persönliche Angaben von den tatsächlich von einer Sozialauswahl betroffenen Mitarbeitern Verwendung finden. Die gewählte Vorgehensweise entsprach dem nicht. Auch nach der Rechtsprechung des Bundesarbeitsgerichts erstreckt sich die Sozialauswahl innerhalb einer Verwaltung auf die Beschäftigten, die miteinander verglichen werden können. Eine Sozialauswahl darf erst stattfinden, wenn bekannt ist, welche Stellen aus betriebsbedingten Gründen wegfallen oder zu verringern sind. Da die Auswahl sich primär nach arbeitsplatzbezogenen Merkmalen richtet, muss zunächst die künftige Aufgabenverteilung bekannt sein, bevor die personelle Auswahl und damit einhergehend eine weitergehende Datenverarbeitung erfolgt. Wegen der bei den Schulleitungen ohnehin vorhandenen arbeitsplatzbezogenen Daten über die Lehrkräfte hätte bereits der für Änderungskündigungen und für eine Sozialauswahl in Frage kommende Kreis der Mitarbeiter dementsprechend eingegrenzt werden können. Personalgespräche zum Zweck der Erhebung der arbeitsplatzbezogenen Angaben wären jedenfalls nicht erforderlich gewesen.

Das vom Staatsministerium veranlasste Verfahren war auch nicht für die Betroffenen transparent. Über Inhalt, Umfang und Tiefe der zu erhebenden personenbezogenen Daten wurden die Betroffenen im Vorfeld bewusst im Unklaren gelassen. Es gab keine schriftliche Aufklärung der Mitarbeiter in Bezug auf den Zweck der Datenerhebung und den rechtlich relevanten Umfang der Daten. Wegen der fehlenden Konkretisierungen wurde damit bei ca. 17.000 betroffenen Lehrern auch die Verarbeitung ungeeigneter und nicht erforderlicher personenbezogener Daten in Kauf genommen. Bei einem einheitlichen Fragebogen, als Fragen-/Antwortenkatalog datenschutzgerecht ausgestaltet, hätten Erforderlichkeits- und Verhältnismäßigkeitsgesichtspunkte berücksichtigt werden, und sichergestellt werden können, dass nicht erforderliche Angaben, u. a. Verschuldungen, gesundheitliche Beeinträchtigungen und intimste Lebensumstände nicht mitgeteilt und als personenbezogene Angaben durch die Regionalschulämter verarbeitet werden.

Letztendlich wäre es erforderlich gewesen, dass die Mitarbeiter der Regionalschulämter, die die Erhebungen durchgeführt hatten, dem Personal verwaltenden Bereich angehören. Dies war so wohl nicht der Fall.

Über den Fortgang des Vorgangs werde ich berichten.

5.1.2 Mitarbeiterbefragungen

In der öffentlichen Verwaltung in Sachsen werden zunehmend Mitarbeiterbefragungen durchgeführt. Z. T. werden die Befragungen auch über das Internet vorgenommen, so z. B. durch die AVS, die auf diese Weise etwas über das Nutzungsverhalten, die Akzeptanz und die Erfahrungen von Nutzern der virtuellen Akademie (http://avsweb.sachsen.de), die verschiedenen Dienststellen angehören, zu erfahren sucht. Derartige Untersuchungen und Befragungen sind für die Mitarbeiter freiwillig.

Sofern es sich allerdings um Organisationsuntersuchungen handelt, bei denen Aufgaben und Aufwand der Verwaltung zur Personalplanung und zur Organisation hinterfragt werden sollen, ist die Verarbeitung personenbezogener Daten nach § 117 Abs. 4 SächsBG bzw. bei Angestellten und Mitarbeitern nach § 37 Abs. 1 Satz 1 SächsDSG zulässig. Die Beschäftigten haben aufgrund des Beamtenverhältnisses bzw. arbeitsvertraglich eine Mitwirkungspflicht. Sobald jedoch bei den Organisationsuntersuchungen der Kernbereich des Grundrechts auf informationelle Selbstbestimmung der Mitarbeiter betroffen ist, sind die Angaben der Mitarbeiter nur auf Einwilligungsgrundlage zu erheben. Regelmäßig ist dies dann der Fall, wenn subjektive Einschätzungen oder Werturteile abgefragt werden sollen. Besonders problematisch sind sensible Daten, z. B. Einschätzungen zum eigenen gesundheitlichen Befinden, während konkrete auf den Arbeitsplatz bezogene Einschätzungen zum körperlichen Wohlbefinden noch zulässig sein können. Nicht mehr abgefragt werden können bereits Angaben zur Einschätzung der Leistung von Kollegen und Vorgesetzten wie auch Angaben aus dem Familienbereich der Mitarbeiter. Sie sind zu tiefgehend. Derartige Abfragen können auch nicht unter dem Rückgriff auf die Einwilligung erfolgen, hat sich die Dienststelle doch am Erforderlichkeitsgrundsatz zu orientieren.

Was Mitarbeiterbefragungen im Übrigen angeht, sind diese freiwillig und auf Einwilligungsgrundlage durchführbar. Nach allgemeiner Erfahrung sollte schon aus Gründen der Validität der zu gewinnenden Daten ein anonymes Verfahren gewählt werden. Daher sollte auch bereits bei der Auswahl der zu erhebenden Daten darauf geachtet werden, dass zu viele statistische Angaben zu einer Identifizierbarkeit einzelner Mitarbeiter führen können. Regelmäßig sollte sich die Dienststelle auch eines Auftragnehmers bedienen, der die Auswertung vornimmt, sowie sichergestellt sein, dass

die Erhebungen direkt durch die auswertende Stelle erfolgen und die (Personal verwaltende) Dienststelle keinen Zugriff auf die Einzeldaten bekommt. Dies sollte den Mitarbeitern in geeigneter Weise bekannt gemacht werden, um die Validität der Daten zu erhöhen. Im Beispielsfall hatte sich die AVS in Meißen einer Universität als Auftragnehmer bedient. Die Auftragsdatenverarbeitung richtet sich nach § 7 SächsDSG und war auch in diesem Fall zulässig.

Bei einer Mitarbeiterbefragung kann wie folgt vorgegangen werden:

1. Die Beschäftigten sind in geeigneter Weise über die beabsichtigte Datenverarbeitung und ihren Zweck sowie die Empfänger vorgesehener Übermittlungen (Daten verarbeitende Stellen) und die Dauer der Datenspeicherung schriftlich aufzuklären. Wesentlich ist dabei auch der Hinweis auf die Anonymität der Datenerhebung.

2. Auch auf die Freiwilligkeit ist ausdrücklich und schriftlich hinzuweisen. Unter Mitteilung der Folgenlosigkeit einer Nichtbeteiligung sind die Beschäftigten darauf hinzuweisen, dass die Einwilligung verweigert werden kann und dass ein Widerruf für die Zukunft aufgrund des anonymen Verfahrens nicht möglich ist.

3. Von der Schriftform der Einwilligung nach § 4 Abs. 4 SächsDSG ist aus Gründen der Anonymitätswahrung der Beschäftigten abzusehen.

4. Fragebogen sind an einem geeigneten Ort in den Dienststellen zu platzieren, wo sie von den Beschäftigten hinreichend unbeobachtet in Besitz genommen werden können (Anonymität und Freiwilligkeit). Bei der Rückgabe der ausgefüllten Bögen ist ebenso auf die Anonymität zu achten. Sollen die Fragebögen bei den Stellen gesammelt werden, empfiehlt sich im Verfahren eine Urne für die Rückgabe der ausgefüllten Bögen aufzustellen. Der Personalrat sollte auch beim Übersendungsvorgang an die auswertende Stelle beteiligt sein.

Voraussetzungen der Zulässigkeit der Mitarbeiterbefragung allgemein sind u. a., dass

- die Befragung anonym erfolgt und die Anonymität nach menschlichem Ermessen tatsächlich gesichert ist,
- die technischen und organisatorischen Maßnahmen zur Datensicherheit sowie die Vorgaben zum Datenschutz befolgt werden (vgl. § 9 SächsDSG),
- die Teilnahme an der Befragung freiwillig ist (insbesondere wegen des anonymen Verfahrens seitens der Vorgesetzten oder durch Dritte nicht auf die Mitarbeiter beeinflussend eingewirkt werden kann),
- an keiner Stelle ein Name angegeben wird und der Fragebogen auch keine Absenderangaben enthält,

- die Rückgabe in verschlossenem Umschlag direkt an den Auswertenden erfolgt,
- die Datenerhebung auf die Angaben im Fragebogen beschränkt bleibt,
- die abgegebenen Antworten bzw. Daten bei der Auswertung nicht individualisiert werden können, die Auswertung durch Bildung hinreichend großer Vergleichsgruppen durchgeführt wird, so dass Rückschlüsse auf einzelne Mitarbeiter ausgeschlossen sind,
- die Auswertung streng vertraulich und allein durch die auswertende Stelle erfolgt,
- nach erfolgter Auswertung die Fragebögen vom Auswertenden vernichtet bzw. alle Datensätze gelöscht werden und
- die Darstellung der Auswertungsergebnisse Rückschlüsse auf einzelne Mitarbeiter nicht zulässt.

Sofern die vorstehenden Grundsätze eingehalten sind, dürften die datenschutzrechtlichen Belange gewahrt sein.

5.1.3 Grenzen der personenbezogenen Verarbeitung bei Leistungsprämien und Leistungsstufen

Die *Leistungsstufenverordnung* (LStVO) und die *Leistungsprämienverordnung* (LPVO) sehen Leistungselemente für Beamte vor. Darüber hinaus können auch den Angestellten und Arbeitern des Freistaates Leistungsprämien gewährt werden (*Verwaltungsvorschrift des Sächsischen Staatsministeriums der Finanzen zur Gewährung für Prämien für besondere Leistungen an Arbeitnehmer* (VwV Leistungsprämien).

Die Frage, ob und ggf. unter welchen Voraussetzungen die Empfänger von Leistungsstufen, -prämien und -zulagen dienststellenintern mit Namensbezug bekannt gegeben werden dürfen, stellte sich mir, nachdem ich mitgeteilt bekam, dass bei sächsischen Stellen die Empfänger von Leistungsprämien in Personalversammlungen bzw. im Intranet bekannt gemacht wurden. Der Gedanke, dass alle Mitarbeiter die Möglichkeit haben sollen, im Sinne einer Transparenz Kenntnis von Personalaktendaten zu nehmen, ist jedoch nicht systemgerecht. Dies widerspricht dem gesetzlich verankerten Prinzip der Vertraulichkeit des Personalakts. Prämien und Zulagen dienen eben in erster Linie einer persönlichen Anerkennung der individuellen Leistung eines Beamten bzw. Angestellten. Es besteht zudem ein enger Bezug zu den Beurteilungen und Leistungseinschätzungen des Mitarbeiters. Auch diese Informationen werden gerade vertraulich verwahrt. Eine Veröffentlichung in Dienststellen ist daher unzulässig.

Entscheidungen über Leistungsprämien und Leistungsstufen in Bezug auf konkrete Mitarbeiter sind als Teil des Personalakts zu qualifizieren, da die Unterlagen, die den Beamten betreffen, mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Unterlagen, die sich auf die Gewährung von Leistungsprämien

bzw. Leistungsstufen beziehen, sind somit von Gesetzes wegen vertraulich zu behandeln, § 117 Abs. 1 SächsBG. Der Empfänger von Leistungsprämien und Leistungsstufen und der Inhalt einer derartigen Entscheidung sind daher grundsätzlich nicht einem Adressatenkreis außerhalb der mit der Personalverwaltung befassten Mitarbeiter zu offenbaren (vgl. §§ 117 Abs. 3, 121 SächsBG). Sächsische Dienststellen, die eine dienststelleninterne Bekanntgabe anstreben, um die Transparenz des Verfahrens zu gewährleisten bzw. die Motivation der Beschäftigten zu steigern, haben dies zu berücksichtigen. Die Verarbeitung von Personalakten ist abschließend in den §§ 117 ff. SächsBG geregelt, eine Offenbarung für die Durchführung nach der LStVO und der LPVO ist nicht vorgesehen. Im Einklang mit dem Sächsischen Beamtengesetz bestimmen die Verordnungen, dass Entscheidungen *dem betreffenden Beamten gegenüber* schriftlich mitzuteilen sind (§ 5 Abs. 2 LPVO, § 7 Abs. 2 LStVO).

Sofern dennoch eine namentliche Veröffentlichung der Empfänger und der Beträge bzw. der Adressaten von Leistungsstufen in Hausmitteilungen oder im hauseigenen Intranet stattfinden soll, so ist mir die Frage gestellt worden, ob dies auf Grundlage einer vorherigen Einwilligung geschehen kann. Wäre eine Einwilligung zulässig, richtete sich das Einwilligungsverfahren nach § 4 Abs. 3 bis 5 SächsDSG. Eine wirkliche Freiwilligkeit der Einwilligung im Beamtenverhältnis bzw. im Abhängigkeitsverhältnis bei Angestellten und Arbeitern kann aber nur eingeschränkt gewährleistet werden. Ich vertrete daher den Standpunkt, dass ausgehend von der Gesetzeslage eine Veröffentlichung auch auf Einwilligungsbasis nicht erfolgen darf. Die Zulässigkeit von namensbezogenen Veröffentlichungen ist abschließend in den personaldatenschutzrechtlichen Vorschriften über die Veröffentlichung von „Personalaktendaten“ geregelt. Das Sächsische Beamtengesetz, die Verordnungen und die verwaltungsinternen Bestimmungen zur Personalaktenführung sind für Beamte abschließend und sehen für Leistungselemente jedenfalls keine Bekanntmachung, auch nicht auf Einwilligungsgrundlage, vor. Sofern in Bezug auf Angestellte und Arbeiter auf keine, auf die Vorschriften für Beamte geltende Bestimmungen, verwiesen wird, würde § 37 SächsDSG gelten. Selbst bei Anwendung des § 37 SächsDSG fehlt es an der Erforderlichkeit der Bekanntmachung. Nur die Einwilligung und Zweckmäßigkeitsgesichtspunkte reichen dagegen nicht aus. Auch § 37 Abs. 2 SächsDSG steht unter dem Vorbehalt, dass die Bekanntmachung für die Personal verwaltende Stelle erforderlich ist. An der Erforderlichkeit mangelt es jedoch. Unabhängig von dem grundlegenden und entgegenstehenden Prinzip der Vertraulichkeit des Personalakts, das auch bei Angestellten einzuhalten ist, ist zu berücksichtigen, dass die Veröffentlichung einer anonymisierten Übersicht über die Gewährung von Leistungsprämien und Leistungsstufen immer ausreichen wird, um eine Transparenz und eine entsprechende Motivation weiterer Mitarbeiter zu erreichen. Hinzu kommt, dass auch die Personalvertretung im

Rahmen ihrer Beteiligungsmöglichkeiten die Befugnis hat, die Vergabe in einem erforderlichen Maß zu kontrollieren.

5.1.4 Aktenführung eingegangener Schriftsätze des Sächsischen Datenschutzbeauftragten

Bei einer Kontrolle stellte ich fest, dass ein versendetes Schriftstück meiner Behörde in einer Personalakte geführt wurde. Das Schreiben betraf einen Vorgang, bei dem sich der betroffene Mitarbeiter wegen der Führung seiner Personalakte nach § 24 SächsDSG an mich gewandt hatte.

Zu dem Vorgang habe ich folgende Auffassung vertreten:
Nach § 24 SächsDSG haben Betroffene das Recht, sich an den Sächsischen Datenschutzbeauftragten zu wenden. Die Einschätzung, in seinem Grundrecht auf informationelle Selbstbestimmung selbst verletzt worden zu sein, genügt. Die Vorschrift bestimmt auch, dass niemand benachteiligt oder gemaßregelt werden darf, wenn er von diesem Recht Gebrauch macht. Das gesetzlich verbürgte Recht steht auch Bediensteten zu, die in ihrem Grundverhältnis und daher ebenso in dem Grundrecht betroffen sein können.

Der Vorgang ist daher in einer Sachakte zu führen, auch wenn er die Personalaktenführung bzw. die Personaldatenverarbeitung unmittelbar betrifft. Diese kann, wie dies z. T. bei anderen die Dienststelle betreffenden Beschwerdegegenständen geschieht, auch im Bereich der Personalverwaltung geführt werden, aber nicht in der förmlichen Personalakte selbst. In diese gehören keine datenschutzrechtlichen Sachvorgänge der beschriebenen Art. Die Personalakte hat eine besondere Bedeutung, was die Dokumentation des einzelnen Beamten- bzw. Arbeitsverhältnisses angeht. Nicht in die Personalakte aufzunehmen sind aber Vorgänge, die von den Rechten und Pflichten des konkreten Beamten getrennt werden können. So werden auch Remonstrationen des Beamten und gerichtliche Streitigkeiten aus dem Beschäftigungsverhältnis in Sachakten geführt. Da die Tatsache, dass sich ein Einzelner an den Sächsischen Datenschutzbeauftragten gewandt hat, zudem für diesen nach dem Gesetz nicht nachteilig sein darf, ist bereits datenschutzorganisatorisch dafür Sorge zu tragen, dass für den Beschwerdevorgang unzuständige Personen von der Anrufung, die nach allgemeiner Lebenserfahrung negativ gewertet werden kann, keine Kenntnis erhalten.

Die Führung des datenschutzrechtlichen Vorgangs in der Personalakte ist auch für die Personalverwaltung letztendlich so nicht erforderlich. Die Personal verwaltende Stelle hat lediglich die Personalakte betreffende Maßnahmen bzw. Empfehlungen des Sächsischen Datenschutzbeauftragten - sofern man diesen folgt - umzusetzen bzw. kann

ggf., sofern dies überhaupt personalaktenrelevant ist, den Abschluss des Sachvorgangs darstellende Schriftstücke in die Personalakte aufnehmen (z. B. im Fall einer arbeitsgerichtlichen Entscheidung). Zu berücksichtigen ist letztendlich auch, dass Personalakten auch an andere Dienststellen zeitweise übermittelt bzw. übernommen werden können, deren Kenntnisnahme vom Inhalt eines Beschwerdevorgangs ebenfalls nicht notwendig wäre.

Im vorliegenden Fall hat die Personal verwaltende Stelle mich bei meinem Anliegen unterstützt und der Vorgang wurde aus der Personalakte entfernt.

5.1.5 Verarbeitung von personenbezogenen Daten Beschäftigter privater Firmen - Outsourcing

Die Personalverwaltungen sächsischer öffentlicher Stellen sind nicht befugt, Personalaktendaten von Mitarbeitern externer Firmen zu verarbeiten. Bei einer Kontrolle in einer Personalverwaltung einer obersten Dienstbehörde stieß ich darauf, dass Beschäftigtendaten privater Wachdienste verarbeitet wurden. Die Wachdienste waren in Einrichtungen des Maßregelvollzugs eingesetzt. Vor der Beauftragung der Wachfirmen war die Bewachung durch Beschäftigte des Landes erfolgt. Die Personalverwaltung der öffentlichen Stelle forderte MfS-Erklärungen der Mitarbeiter der Wachdienste an und Auskünfte zu den Mitarbeitern aus dem Bundeszentralregister. In einem Fall wurde von dem privaten Wachdienst verlangt, eine vollständige Personalakte zur Einsicht zu übersenden.

Gerechtfertigt wurde die Verarbeitung seitens der obersten Dienstbehörde mit Sicherheitserfordernissen. Nach meiner Kontrolle wurden die die Beschäftigten der Privatfirmen betreffenden Unterlagen unverzüglich vernichtet bzw. an die zuständigen Personalverwaltungen zurückgesandt. Entsprechende Löschungsprotokolle wurden angefertigt. Die Personalverwaltung der Behörde unterstützte mich in meinen Bemühungen sehr.

Es fehlten in diesem Fall die Voraussetzungen für die Verarbeitung personenbezogener Daten in Bezug auf eine Mitarbeit der bei den Privatunternehmen Beschäftigten bei der Staatssicherheit oder vergleichbarer Organe der ehemaligen DDR. Auch die Übersendung der Personalakte hatte im konkreten Fall keine gesetzliche Stütze. Ich halte es zwar noch für zulässig, wenn sich der Freistaat durch seine Vertragspartner, die als Arbeitsgeber handeln, versichern lässt, dass Auskünfte aus den BZR-Registern zu den eingesetzten Mitarbeitern regelmäßig eingeholt und die Zuverlässigkeit durch den Auftragnehmer regelmäßig überprüft wird. Eine weitergehende personenbezogene Datenverarbeitung kann aber auch nicht durch vertragliche Regelungen dahingehend

konstruiert werden, dass z. B. das Wachunternehmen die BZR-Auskünfte oder andere personalaktenrelevante Unterlagen vorzulegen hat. Entscheidet sich der Staat für ein Outsourcing von Bereichen seiner Verwaltung, nimmt er damit datenschutzrechtlich auch die informationelle Trennung bei der Personaldatenverarbeitung der ausgelagerten Bereiche in Kauf.

5.1.6 Einsatz eines pensionierten Beamten als Ermittlungsführer bei disziplinarischen Vorermittlungen

Im Frühjahr 2004 erhielt ich Kenntnis von der Beauftragung eines pensionierten Beamten als Ermittlungsführer, um disziplinarische Vorermittlungen gegen den damaligen Landespolizeipräsidenten durchzuführen. Ich machte gegenüber dem SMI datenschutzrechtliche Bedenken geltend und kontrollierte den Vorgang.

Der pensionierte Beamte konnte nach dem Sächsischen Beamtengesetz beamtenrechtlich als Ruhestandsbeamter nicht wieder in Dienst gestellt werden. Er wurde auf Grundlage einer als „öffentlich-rechtlicher Vertrag“ bezeichneten Vereinbarung tätig. Diese sollte die disziplinarrechtliche Stellung des Ruhestandsbeamten als Vorermittlungsführer begründen. Zwischenzeitlich war der Ruhestandsbeamte als Vorermittlungsführer bereits intensiv tätig geworden.

Für eine Beleihung fehlten die gesetzlichen Grundlagen. Das Staatsministerium stützte sich auch auf den Vertrag, mit dem - so die Vorstellung der Dienstbehörde - ein „öffentliches (subordinations)rechtliches Auftragsverhältnis“ begründet werden sollte. Der Vorermittlungsführer wurde als „Verwaltungshelfer“ eingeordnet.

Um einen Bediensteten hätte es sich jedoch im Rahmen von Vorermittlungen nach § 24 Abs. 1 SächsDO wegen der Weisungsgebundenheit des Ermittlungsführers handeln müssen. Eine nach der Disziplinarordnung geforderte Weisungsgebundenheit konnte nach meiner Überzeugung nur in einem Dienst- bzw. zumindest Arbeitsverhältnis begründet und nicht auf andere vertragliche Weise erzeugt werden. Ein öffentlich-rechtliches Auftragsverhältnis gibt der beauftragenden Stelle nicht die Steuerungsmöglichkeiten in die Hand, über die ein Dienstvorgesetzter beamtenrechtlich und dienst-/arbeitsrechtlich verfügt. Auch der Wortlaut des § 3 SächsDO setzt voraus, dass nur ein sich im Amt befindender Bediensteter Vorermittlungen durchführt. Das SMI ging auch von der Weisungsgebundenheit des Vorermittlungsführers aus und zielte mit der Vereinbarung darauf ab, ein öffentlich-rechtliches Subordinationsverhältnis zu konstituieren. Dies wäre nach den gesetzlichen Bestimmungen aber gerade bei der Person des bestellten Pensionsbeamten nur in den gesetzlich vorgesehenen Fällen einer Reaktivierung möglich gewesen. Die disziplinarrechtlichen und beamtenrechtlichen Vor-

schriften betrachte ich insofern nämlich als abschließend. Auffangvorschriften, insbesondere § 7 SächsDSG - dies nebenbei - sind bei der Tätigkeit des Vorermittlungsführers nicht einschlägig gewesen. (Zur Problematik der Beauftragung externer Vorermittlungsführer am Beispiel des Bundesministers a. D. Hirsch: Battis/Kersten in ZBR 2001, S. 309 ff. m . w. N.)

Nach meiner Einschätzung wurde durch die Beauftragung eines gesetzlich nicht legitimierten Vorermittlungsführers gegen datenschutzrechtliche Grundsätze verstoßen, § 4 Abs. 1 SächsDSG.

Das SMI hielt an seiner gegensätzlichen Rechtsansicht fest und die Ermittlungen wurden durch den sich im Ruhestand befindenden Vorermittlungsführer letztendlich zum Abschluss gebracht.

Das SMI vertrat die Auffassung, dass auch natürliche, nicht in einem Dienst- oder Arbeitsverhältnis stehende Privatpersonen zu Vorermittlungsführern bestellt werden könnten. Im Ergebnis vertrat das Staatsministerium die Ansicht, dass es sich bei diesem Personenkreis um Verwaltungshelfer handele, die als außerordentliche Organwalter einer Behörde unselbständig tätig in die Erledigung hoheitlicher Aufgaben eingeschaltet werden könnten. (Nach h. M. bedarf es für die Bestellung von Verwaltungshelfern regelmäßig keiner besonderen gesetzlichen Ermächtigungsgrundlage.)

Eine Öffnung im Gesetzeswortlaut, die eine solche „Beauftragung“ zuließe, ist in der Sächsischen Disziplinarordnung nach meiner Überzeugung jedoch nicht vorhanden. Unabhängig davon - sofern man eine Verwaltungshelfertätigkeit bejaht - hätte sich aus meiner Sicht dann allerdings die Frage gestellt, ob es aus Verfassungsgründen nicht doch Ausnahmen von der Beauftragung von Verwaltungshelfern in bestimmten Bereichen der Verwaltung geben muss. Durch disziplinarische Vorermittlungen stehen hoheitliche Eingriffe in Rede. Es geht nämlich nicht alleine um Eingriffe in das Grundrecht auf informationelle Selbstbestimmung. Nach der Disziplinarordnung kann der betroffene Beamte daher auch einen Rechtsanwalt, einen Verteidiger beteiligen. In vergleichbaren wenigen Fällen der Inanspruchnahme von Verwaltungshelfern, die Eingriffe in das Grundrecht auf informationelle Selbstbestimmung vornehmen können sollen, da sie personenbezogene Daten mit einer gewissen Eingriffstiefe verarbeiten, hat sich in der Praxis die Ansicht durchgesetzt, dass hierfür doch eine gesetzliche Bestimmung benötigt wird. So wird z. B. bei dem Einsatz von Verwaltungshelfern zur Erhebung von Daten von Hundebesitzern mindestens eine Regelung in der entsprechenden Satzung für erforderlich gehalten. Das informationelle Selbstbestimmungsrecht enthält für das Verhältnis von Verwaltung und Verwaltungshelfer Informationsschranken. Zumindest in Bereichen wie der Personalverwaltung, die sich bereits selbst

informationell und gegenüber anderen Organisationseinheiten abzugrenzen hat, bzw. im strengen und formalisierten Disziplinarrecht, bei dem regelmäßig Dienstvergehen, manchmal Straftaten in Rede stehen, muss dies gelten. Eine Beteiligung externer Dritter und von Verwaltungshelfern ist bei einer im Disziplinarrecht zu erwartenden Intensität des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung ohne normenklare gesetzliche Grundlage unzulässig.

Von einer Beanstandung habe ich allein wegen einer noch nicht einheitlichen und gefestigten Meinungsbildung in der Rechtslehre abgesehen. Der Staatsregierung rate ich jedoch bereits aus Gründen der Rechtssicherheit dazu, zukünftig nur Vorermittlungsführer, die Bedienstete sind, zu bestellen.

Nachdem ich meinen Standpunkt verdeutlicht hatte, gehe ich davon aus, dass es zu keinen weiteren Beauftragungen externer Dritter außerhalb der Gesetze in dem Bereich der hoheitlichen Personalverwaltung kommen wird. Während des Berichtszeitraums gab es auch keine weiteren Vorgänge der beschriebenen Art. Ich bin zudem mit dem SMI dahingehend übereingekommen, eine gemeinsame Empfehlung zum Einsatz von Verwaltungshelfern und Auftragnehmern zu erarbeiten.

5.1.7 Beurteilungsverfahren

Mir ist der Entwurf einer neuen Sächsischen Beurteilungsverordnung zugeleitet worden. Der Staatsregierung gegenüber habe ich datenschutzrechtliche Empfehlungen abgegeben.

Der Entwurf sah u. a. vor, dass bestimmte Mitarbeitergruppen von der regelmäßigen Beurteilung ausgenommen werden. Er enthielt die Festlegung bei *Strafverfahren*, *Disziplinarverfahren* und bei *Ermittlungsverfahren* keine regelmäßige Beurteilung mehr durchzuführen. Derartige starre Festlegungen halte ich für unbillig. Es gilt grundsätzlich die Unschuldsvermutung zugunsten der zu beurteilenden Mitarbeiter. In Bereichen, wo Anzeigen berufsgedingt an der Tagesordnung sind, wie z. B. bei der Polizei kann die vorgesehene Vorschrift z. B. dazu führen, dass einige Beamte wegen gegen sie eingeleiteter *Ermittlungsverfahren* nicht mehr regelmäßig beurteilt werden, was sich für die Betroffenen negativ auswirken könnte. Ich hoffe, dass der Entwurf so nicht in Kraft treten wird.

Darüber hinaus habe ich einen Vorschlag zur Verarbeitung personenbezogener Daten durch die zu bildenden Beurteilungskommissionen unterbreitet. Zur Einhaltung eines einheitlichen Beurteilungsmaßstabes ist auch die Bildung von Beurteilungskommissionen, denen allerdings nur Bedienstete der jeweiligen personalverwaltenden Dienststelle angehören dürfen, geeignet. Die Beurteilungskommissionen dürfen auch nur

beratende Funktion haben und sind nicht berechtigt, die Entscheidungen der Beurteiler zu ändern oder zu ersetzen. Die Personalverwaltungen sollten unter Zugrundelegung der ihnen vorgelegten Beurteilungsentwürfe Übersichten für die Vergleichsgruppen, aus denen sich die beabsichtigte Notenverteilung innerhalb der Behörden und Organisationseinheiten ergeben, erstellen und die Beurteilungskommissionen anhand der Übersichten über die vorgesehenen Notenvergaben informieren. Die Beurteilungskommissionen dürfen Beurteilungen im Einzelfall nur und soweit dies aus Gründen der Herstellung eines einheitlichen Maßstabes unabdingbar erforderlich ist, beraten. Es gilt der Grundsatz der Datensparsamkeit. Sofern ein Verfahren unter Beachtung der vorstehenden Grundsätze normenklar gesetzlich geregelt ist, können auch Beurteilungsdaten im erforderlichen Maße behördenintern erörtert werden und dies ist dann auch im datenschutzrechtlichen Sinne für Zwecke der Personalverwaltung „erforderlich“. Dies stünde m. E. auch im Einklang mit § 124 Abs. 1 SächsBG.

Gegen die vorgesehene Einführung und Festsetzung von Platznummern habe ich keine Bedenken erhoben.

Zwischenzeitlich ist die Beurteilungsverordnung noch nicht erlassen worden. Bei den Entwürfen zu ausführenden Bestimmungen der Geschäftsbereiche und den Verwaltungsvorschriften werde ich weiter beraten.

5.1.8 Verstoß gegen die Verschwiegenheitspflicht durch einen Wahlbeamten durch Veröffentlichung von personenbezogenen Schriftstücken in den Medien

Wegen der öffentlichen Äußerungen eines Beigeordneten einer sächsischen Stadt auf einer von diesem selbst einberufenen Pressekonferenz im März 2004 habe ich die damit verbundene Übermittlung personenbezogener Daten an einen unbestimmten Empfängerkreis beanstandet.

Die Besonderheit bei dem Vorgang war, dass zum Zeitpunkt der Presseerklärung gegenüber dem Beigeordneten bereits durch den Oberbürgermeister eine Anordnung des Verbots der Führung der Dienstgeschäfte als Bürgermeister und Beigeordneter ergangen war. Eine Genehmigung, Auskünfte an die Medien zu erteilen, hatte der Beamte nicht erteilt bekommen und nach meinem Kenntnisstand auch nicht erbeten. Gleichwohl hatte der Bürgermeister und Beigeordnete auf einer Pressekonferenz zu einem Untersuchungsbericht einer politischen Partei, der geeignet war, ihn in der Öffentlichkeit wegen finanzieller und vertraglicher Einzelheiten politisch in Bedrängnis zu bringen, Stellung genommen. Die 20-seitige Stellungnahme zu dem Untersuchungsbericht war samt acht Anlagen sogar auf der Internetpräsenz einer Tages-

zeitung nachzulesen. Die öffentlich verbreitete Stellungnahme des Beigeordneten beinhaltete zahlreiche personenbezogene Daten, die nicht nur partei-interne Vorgänge, sondern auch das Handeln der Stadt und mit der Stadt wegen eines Stadionumbaus in geschäftliche Beziehung getretene natürliche und juristische Personen, mithin dienstliche Vorgänge betrafen.

Die Stadt teilte in ihrer Stellungnahme mit, dass der Beamte lediglich die Genehmigung erhalten habe, in dem gegen ihn laufenden Disziplinarverfahren seine berechtigten Interessen gegenüber der zuständigen Behörde, dem Regierungspräsidium, wahrzunehmen.

Ich habe den Vorgang als nicht unerheblichen Verstoß gegen datenschutzrechtliche Bestimmungen betrachtet, denn die Preisgabe personenbezogener Daten und der Bruch der Vertraulichkeit der Geschäftsbeziehungen zwischen einer Stadt und ihren Geschäftspartnern durch eigenmächtiges und unbefugtes Handeln einer Amtsperson ist geeignet, das Vertrauen der Öffentlichkeit in den Grundsatz des gesetzmäßigen Handelns von Verwaltungsorganen zu erschüttern. Unbeachtlich war in diesem Zusammenhang auch, dass der Untersuchungsbericht der Partei wie auch andere Angaben zu dem in Rede stehenden Gesamtvorgang bereits von anderer Seite zuvor veröffentlicht worden waren. Ausreichend für das Vorliegen eines Datenschutzverstoßes war schon die Tatsache, dass ein Amtsträger der Stadt unbefugt personenbezogene Daten - auch wenn diese gegebenenfalls bereits aus anderen Quellen bekannt gewesen waren - bestätigte, richtig stellte, ergänzte oder in neue Zusammenhänge stellte. Die Stadt unterliegt als öffentliche Stelle dem Anwendungsbereich des Sächsischen Datenschutzgesetzes und sie darf nur nach § 4 Abs. 1 SächsDSG personenbezogene Daten verarbeiten, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt. Die mit der Pressekonferenz des suspendierten Bürgermeisters und Beigeordneten öffentlich verbreitete Stellungnahme mit personenbezogenen Daten berührte insbesondere Privatpersonen, die im Zusammenhang mit sachlichen oder persönlichen Verhältnissen genannt wurden und deren Grundrecht auf informationelle Selbstbestimmung. Unter einem Gliederungsabschnitt der Stellungnahme wurden nämlich mit der Stadt beim Umbau eines Stadions in geschäftliche Beziehung getretene natürliche und juristische Personen genannt. Dabei erfolgten Angaben, die in jedem Fall bereits Veröffentlichtes teilweise übertrafen.

Die Anordnung des Verbots der Führung der Dienstgeschäfte als Bürgermeister und Beigeordneter enthielt keine Genehmigung, Auskünfte zum Sachvorgang an die Medien zu erteilen. Ausgangspunkt des Datenschutzverstoßes war der Verstoß gegen beamtenrechtliche Regelungen durch den Bürgermeisters und Beigeordneten. Gemäß § 78 Abs. 2 SächsBG darf der Beamte ohne Genehmigung weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Ein Verstoß gegen die Amtsver-

schwiegenheit liegt nur dann nicht vor, wenn der Dienstvorgesetzte die Genehmigung erteilt hat.

Ferner erteilt nach § 80 SächsBG der Oberbürgermeister oder ein von ihm Beauftragter Auskünfte an die Medien. Die Stadt hatte dies auch durch eine entsprechende Organisationsverfügung geregelt. Der Beigeordnete hatte im vorliegenden Fall weder für außergerichtliche Aussagen oder Erklärungen eine Genehmigung nach § 78 Abs. 2 SächsBG, noch war er nach § 80 SächsBG beauftragt.

Die mit der Pressekonferenz verbundene Übermittlung personenbezogener Daten durch den Bürgermeister und Beigeordneten war weder von Seiten der Stadt, vertreten durch den Oberbürgermeister, genehmigt, noch war sie beamtenrechtlich zulässig. Sie war daher seitens der öffentlichen Stelle auch nicht gewollt, nicht erforderlich und verstieß damit gegen § 16 Abs. 1 Nr. 1 SächsDSG.

Die aus der Verletzung seiner Dienstpflichten resultierende rechtswidrige Datenverarbeitung durch den Beigeordneten war auch der Stadt zuzurechnen (vgl. § 16 Abs. 2 SächsDSG). Ich habe der Stadt empfohlen, in künftigen Fällen der Anordnung des Verbots der Führung der Dienstgeschäften zugleich regelmäßig datenschutzorganisatorische Festlegungen zu den Rechten und Pflichten vom Dienst suspendierter Beamten während strafrechtlicher Ermittlungsverfahren und gegen ihn laufender disziplinarrechtlicher Verfahren zu treffen. Dabei sollte aus datenschutzrechtlicher Sicht auf die Genehmigungserfordernisse nach §§ 80, 78 Abs. 2 bzw. 79 Abs. 3 SächsBG und auf mögliche Ahndungen bei Verstößen hingewiesen werden.

5.1.9 Unbefugte Personaldatenverarbeitung und Personalaktenführung durch öffentliche Stellen

Öffentliche Stellen sind lediglich befugt, auf gesetzlicher Grundlage Daten zu verarbeiten, § 4 Abs. 1 SächsDSG. In Bezug auf Personalakten ergibt sich die Befugnis aus den beamtengesetzlichen Bestimmungen bzw. geschieht die Verarbeitung zulässigerweise auf arbeitsvertraglicher Grundlage. Dies gilt sowohl für staatliche als auch Stellen des kommunalen Bereichs. Auch Bezügeakten sind Teil der Personalakten. Leider stellte ich im letzten Berichtszeitraum bei meinen Kontrollen fest, dass nicht wenige öffentliche Stellen ohne gesetzliche Stütze Bezügeakten für externe Stellen, insbesondere eingetragene Vereine, die darüber hinaus finanziell unterstützt werden, führen. Außerhalb der beamtenrechtlichen Gesetze, arbeitsvertraglicher Bindungen bzw. anderen Gesetzen, wie dem Sächsischen Gesetz über kommunale Zusammenarbeit ist eine Personaldatenverarbeitung unzulässig. In einem Fall wurde ich bei einer Kommune sogar damit konfrontiert, dass die Führung der gesamten Personalakten für eine externe

Stelle erfolgte. Wegen der besonderen Vertraulichkeit, der die Personalakten unterliegen, sind derartige Verstöße gegen § 4 Abs. 1 SächsDSG auch regelmäßig als schwerwiegend einzustufen.

Zukünftig beabsichtige ich, regelmäßig solche Verstöße zu beanstanden und auch der für die - zumeist nicht öffentliche - Stelle zuständigen Datenschutzaufsichtsbehörde den Vorgang zuzuleiten. Ich bitte die sächsischen Kommunalverbände um Mitwirkung und sämtliche Personal verwaltenden Stellen um Beachtung, damit bereits im Vorfeld datenschutzgerecht verfahren wird.

5.1.10 Ausblick - Reform des öffentlichen Dienstrechts

Im Dienstrecht stehen entscheidende Veränderungen bevor. Die Länder und damit auch der Freistaat sollen im Beamtenrecht mehr Spielraum erhalten. Im Bereich des öffentlichen Dienstes gibt es schon länger Überlegungen, Leistungselemente im öffentlichen Dienst einzuführen. Nach Vorstellung des Bundesgesetzgebers soll das Bezahlungssystem im Hinblick auf individuelle Leistungen und Anforderungen angepasst werden können. Die Einführung von Leistungselementen wird notwendigerweise nicht nur ein Mehr an Aufwand für die Personalverwaltungen, sondern auch ein Mehr an Verarbeitung personenbezogener Daten bedeuten. Auch die Einführung digitaler Personalakten ist seit langem im Gespräch und soll ermöglicht werden, sehen doch die beamtenrechtlichen Regelungen bisher Papierform der Dokumente vor. Ohne die gesetzlichen beamtenrechtlichen Rahmenbedingungen zu verändern, können derartige Neuerungen auch in Sachsen nicht erfolgen. Die Einführung elektronischer Personalakten kann nur bei entsprechender datenschutzorganisatorischer Sicherheit, insbesondere bei Verfügbarkeit und gegebenen Möglichkeiten zur Authentifizierung mittels qualifizierter Signatur umgesetzt werden.

Ich werde die Entwicklung aufmerksam verfolgen und die sächsischen Behörden nach Bedarf beraten.

5.1.11 E-Mail-Adressen und Kontaktangaben des öffentlichen Dienstes

Ein Mitarbeiter einer Behörde wandte sich an mich mit der Frage, ob das personenbezogene Datum, bestehend aus Name und Vorname, das bei vielen Stellen des öffentlichen Dienstes zur Bildung der E-Mail-Adresse verwendet wird hierfür verarbeitet werden könne, da es u. a. auch eine mögliche Identifizierung der Person außerhalb der Behörde zulasse. Gegen eine Verarbeitung in der Weise bestehen meinerseits keine datenschutzrechtlichen Bedenken.

Grundsätzlich ist zur Bildung von E-Mail-Adressen Folgendes zu beachten:

Aus Vor- und Zunamen gebildete E-Mail-Adressen beinhalten personenbezogene Daten im Sinne des § 3 Abs. 1 SächsDSG. Nach § 37 Abs. 1 Satz 1 i. V. m. Abs. 2 Nr. 2 und Abs. 3 Nr. 3 SächsDSG ist die Verarbeitung von Daten von Beschäftigten jedoch erlaubt, wenn dies zur Durchführung des Dienst- und Arbeitsverhältnisses oder für organisatorische Maßnahmen erforderlich ist und dem keine schutzwürdigen Interessen des Betroffenen entgegenstehen. Schutzwürdige Interessen haben bei dem von mir geprüften Vorgang nicht entgegengestanden. Amtsträger genießen in Bezug auf ihre Namensangaben und Kontaktdaten (Amtsbezeichnung, dienstliche Rufnummer, Zimmernummer usw.) lediglich einen eingeschränkten Schutz. Die Mitarbeiterdaten dürfen aber auch nur im Rahmen des Erforderlichen verarbeitet werden, § 37 Abs. 1 Satz 1 SächsDSG.

Grundsätzlich ist im öffentlichen Dienst Sachsens der Vorname Bestandteil des Namens der Amtsträger und dient einer sicheren Identifizierung. Dies gilt auch für dienstliche Adressen. Das Datum Vorname ist insbesondere von Wichtigkeit, wenn gleiche Nachnamen mehrmals in einer Behörde bzw. in Behörden mit ähnlichen Aufgabengebieten vorkommen. Beschäftigte, die dienstlichen Außenkontakt haben, müssen aus diesem Grunde dulden, dass ihre E-Mail-Adressen bekannt gemacht werden. Eine mögliche Identifizierung ihrer Person außerhalb des öffentlichen Dienstes mag dann möglich sein; sie ist allerdings hinzunehmen, wenn sie Ansprechpartner von Bürgern sind. Unbestritten ist auch, dass die Feststellung der Identität des einzelnen Beschäftigten (hier: Vorname und Nachname) für den innerdienstlichen elektronischen Postverkehr und sofern erwünscht zwischen einzelnen Dienststellen unerlässlich ist.

Je nach dienstlicher Stellung, der Bedeutung des dienstlichen Außenkontaktes im Verhältnis zur Aufgabenerfüllung und nach Art der Bekanntmachung der E-Mail-Adressen auf Briefbögen, im Intranet oder im Internet ist zu differenzieren. Sofern die E-Mail-Adressen nur über Akten und bei der Korrespondenz verbreitet werden, ist der Eingriff in das Persönlichkeitsrecht des betroffenen Beschäftigten in jedem Fall lediglich geringfügig, wird von § 37 Abs. 1 SächsDSG gedeckt und hinzunehmen sein. Eine weitergehende Veröffentlichung im Intranet der Behörde oder in einem Intranet-Verbund wäre die nächste Stufe der Veröffentlichung. Z. B. verfügt der gesamte Bereich der Staatsministerien gemeinsam mit dem Sächsischen Landtag über einen Verzeichnisdienst im Intranet. Auch diese Art der Bekanntgabe ist grundsätzlich datenschutzrechtlich zulässig. Allerdings sollte der Verzeichnisdienst, was die Nutzer angeht, nicht über eine Erforderlichkeit hinaus zu sehr ausgeweitet werden, da mit einem zu weiten Nutzerkreis wiederum eine Missbrauchsgefahr steigt. Sofern E-Mail-Adressen im Internet oder über andere Medien für eine unbeschränkte Öffentlichkeit verbreitet werden, ist dies jedenfalls eingehender zu betrachten. Bei einer unbeschränkten Bekanntgabe von

E-Mail-Adressen ist zunächst auch im Sinne der Erforderlichkeit zu prüfen, ob nicht Funktionsangaben oder Bezeichnungen von Stellen und entsprechende nicht personenbeziehbare E-Mail-Adressen ausreichend wären. Meist ist dies bei Außenkontakten auch praktischer, denn in der Regel wechseln Behördenmitarbeiter öfter als die organisatorischen Zuständigkeiten der Behörde selbst. Geeignet können ggf. auch Dienstvereinbarungen zwischen den Dienststellen und Personalvertretungen sein, die die Belange der Beschäftigten und das Informationsinteresse ausgewogen berücksichtigen.

5.1.12 Die Zulässigkeit von Verwaltungsermittlungen

Im letzten Berichtszeitraum führte eine oberste Dienstbehörde im Bereich der Sächsischen Staatsregierung Verwaltungsermittlungen durch. Die Verwaltungsermittlungen wurden durch Bedienstete eines anderen Geschäftsbereichs durchgeführt.

Bei den Verwaltungsermittlungen habe ich die Staatsregierung beraten. Ich habe u. a. darauf hingewiesen, dass die aus dem Geschäftsbereich eines anderen Staatsministeriums kommenden, untersuchenden Bediensteten dienstrechtlich einzugliedern sind. Das verfassungsrechtlich verankerte Ressortprinzip ist zu beachten. In vergleichbaren Fällen empfehle ich daher, förmliche Abordnungen durchzuführen.

Verwaltungsermittlungen sind nach meiner Überzeugung und nach der herrschenden Meinung in der Rechtsliteratur grundsätzlich zulässig, aber nur dann, wenn sich die Ermittlungen gegen unbekannte Verantwortliche richten oder in ganz engen Grenzen als Vorprüfung dann, wenn aufzuklären ist, ob überhaupt Anlass besteht, Ermittlungen und damit ein Disziplinarverfahren einzuleiten. Grundsätzlich sind Verwaltungsermittlungen gegen einen bestimmten namentlich bekannten Beamten unzulässig. Auch in den Fällen, in denen Bedienstete erkennbar durch irrige Vorwürfe belastet sind, die sich leicht ausräumen lassen - so etwa bei Personenverwechslungen -, kann das formlose Verfahren noch geduldet werden, um vorschnelle und für den Bediensteten unbillige disziplinarische Ermittlungen zu vermeiden. Die Zulässigkeit von Verwaltungsermittlungen neben bzw. vor oder anstelle eines Disziplinarverfahrens oder gar eines strafrechtlichen Ermittlungsverfahrens halte ich nicht für zulässig. Zwar wird in der Rechtsliteratur z. T. die grundsätzliche Zulässigkeit bejaht, dann aber wird zumeist gleichzeitig verlangt, dass den Betroffenen adäquate Schutzrechte, wie sie in den gesetzlich geregelten Verfahren gewährt werden, wie rechtliches Gehör, Akteneinsichtsrecht und Aussageverweigerungsrechte zugestanden werden. Ich vertrete die Auffassung, dass neben disziplinarischen Verfahren und strafrechtlichen Ermittlungsverfahren, die formal gestaltet sind, zum selben Tatsachenkomplex keine parallelen formlosen Ermittlungen durchgeführt werden dürfen. Verwaltungsermittlungen dürfen nur in einer Phase durchgeführt werden, in der noch nicht von einem Anfangsverdacht gegen

eine bestimmte Person gesprochen werden kann. Ergibt sich ein Anfangsverdacht bzw. werden Tatsachen bekannt, die den Verdacht eines Dienstvergehens rechtfertigen, sind die Verwaltungsermittlungen zu diesem Bereich und dem konkreten Betroffenen unverzüglich abzubrechen. Die ermittelnden Bediensteten haben die zuständige Stelle mit ihren Feststellungen zu unterrichten. Die Verwaltungsermittlungen dürfen nicht parallel fortgeführt werden. Ordnungsgemäße und gesetzlich geregelte Ermittlungen müssen die Regel sein. Es gilt das Legalitätsprinzip. Bei dem Disziplinarverfahren vorgelagerten Ermittlungen ist auch zu verlangen, dass keine die Betroffenen belastenden Entscheidungen durch die untersuchenden Bediensteten getroffen werden. Die Schutzrechte der Betroffenen dürfen nicht verkürzt werden. Bei Ermittlungen, die sich auf betroffene Beschäftigte in Arbeitsverhältnissen beziehen, empfiehlt es sich, sich an den beamtenrechtlichen Verfahren zu orientieren und den Betroffenen frühzeitig zu beteiligen, insbesondere ihn anzuhören und ihm Akteneinsicht zu gewähren.

Sofern die gesetzlich nicht geregelten formlosen Verwaltungsermittlungen durchgeführt werden können sollen, ist formal zu fordern, dass die untersuchenden Bediensteten einen konkretisierten Auftrag erhalten, damit ihr Untersuchungsgegenstand klar abgrenzbar ist und keine personenbezogenen Daten über das erforderliche Maß hinaus verarbeitet werden. Die Verwaltungsermittlungsunterlagen sind zunächst in eine Sachakte aufzunehmen. Diese sind zumindest bis zum Abschluss der Ermittlungen aufzubewahren. Nach Abschluss der Verwaltungsermittlungen ist dann eine Entscheidung darüber zu treffen, ob gegen einzelne Bedienstete disziplinarische Ermittlungen durchgeführt werden sollen oder arbeitsrechtliche Schritte eingeleitet werden sollen. In einigen Fällen wird man auch auf die Regelungen des § 122 Abs. 1 SächsBG zurückzugreifen haben.

Die vorstehenden genannten Voraussetzungen für ein rechtmäßiges Verfahren waren aus meiner Sicht zunächst erfüllt gewesen. Auch konnte ich zunächst keine datenschutzrechtlichen Verstöße, was die Datenverarbeitung durch die ermittelnden Bediensteten angeht, feststellen. Während der Ermittlungen und nachdem die formlosen Ermittlungen mit einem Bericht abgeschlossen worden waren, wandten sich betroffene Bedienstete an mich. In diesem Zusammenhang ergaben sich verschiedene rechtliche Fragestellungen.

Es erging eine verwaltungsgerichtliche Entscheidung, in der festgestellt wurde, dass auf Grundlage der formlosen und gesetzlich nicht geregelten Verwaltungsermittlungen durchgeführte beamtenrechtliche (vorläufige) Maßnahmen nicht zulässig gewesen sind. Die gerichtliche Entscheidung, die sich nicht auf die datenschutzrechtliche Zulässigkeit der Verwaltungsermittlungen selbst bezog, zeigte, dass die formlos zusammengetragenen Informationen nur eingeschränkt weitergenutzt werden können.

Eine Beschwerde bezog sich auf eine zunächst nicht erteilte Auskunft aus den Verwaltungsermittlungsakten. Wie die oberste Dienstbehörde selbst, bin ich davon ausgegangen, dass es sich bei den angelegten Akten um Sachakten handelt. Zumindest ist bei Verwaltungsermittlungen den von der damit einhergehenden Verarbeitung personenbezogener Daten, Betroffenen Auskunft nach § 18 SächsDSG zu geben. Sofern Akten nicht zu einzelnen Personen angelegt werden, was bei den angelegten Akten der Fall war, besteht kein Anspruch auf Akteneinsicht, aber ein Anspruch auf eine bestmögliche Auskunft. Nachdem zunächst rechtsirrig seitens der verantwortlichen Behörde ein Personenbezug generell verneint worden war, ist der Betroffene dann mehrfach aufgefordert worden, sein „Informationsinteresse“ darzulegen und letztendlich über einen nicht unerheblichen Zeitraum nicht beschieden worden. Anträge auf Auskunft nach dem Sächsischen Datenschutzgesetz sind aber hinsichtlich des Zweckes nicht besonders zu begründen. Insbesondere eine rechtliche Begründung verlangt das Gesetz nicht. Das in § 18 Abs. 3 Satz 2 SächsDSG erwähnte „geltend zu machenden Informationsinteresse“ bedeutet lediglich, dass der Betroffene einen Antrag stellt, aus dem sich inhaltlich alles für die Auskunft gebende Stelle Erforderliche ergibt. Die Entscheidung über die Erteilung der Auskunft oder der Akteneinsichtnahme hat, insbesondere wenn die Akteneinsicht oder Auskunft nur teilweise gewährt wird oder verweigert wird, als rechtsmittelfähiger Bescheid zu ergehen (vgl. auch den Beitrag unter 5.14.2). Nachdem die Auskunft zunächst vollständig versagt worden war, wurde sie teilweise erteilt, danach umfassend. Z. T. waren die Auskünfte unvollständig.

Während der Verwaltungsermittlungen nahmen die untersuchenden Bediensteten eine Strafanzeige entgegen, die in keinem Zusammenhang zu dem Untersuchungsauftrag stand. Die Anzeige wurde von einem der untersuchenden Bediensteten der Staatsanwaltschaft überbracht. Kurz darauf erschienen in der Tagespresse Informationen aus der Anzeige, insbesondere die namentliche Nennung von Bediensteten in einem negativen Zusammenhang. Die mit den vorgenannten Vorgängen zusammenhängenden datenschutzrechtlichen Fragen und Verstöße habe ich nicht vollständig aufklären können.

Während der Verwaltungsermittlungen fanden Befragungen von Bediensteten zum Untersuchungsgegenstand statt. Die dazu angelegten Protokolle waren weitschweifig abgefasst und standen dennoch inhaltlich zu einem großen Teil erkennbar in keinem Zusammenhang zu dem Ermittlungsauftrag. Ich musste daraus schließen, dass die Befragungen bzw. die Dokumentation der Ermittlungen in einem nicht ausreichenden Maße gesteuert worden war. In einem Fall eines Betroffenen, bei dem letztendlich kein dienstrechtlicher Verstoß festgestellt werden konnte, wurde dieser auffällig gehäuft, fast einhundert Mal, erwähnt, was ihn in konkreten Zusammenhängen und im Gesamtkontext als Grundrechtsträger belastet. Ein Zusammenhang zwischen dem Betroffenen

und nach dem Ermittlungsauftrag zu untersuchenden oder auch anderen Unregelmäßigkeiten waren aber letztendlich nicht ersichtlich.

Ich habe der Behörde empfohlen, die Verwaltungsermittlungsakten schnellstmöglich zu vernichten.

5.2 Personalvertretung

In diesem Jahr nicht belegt.

5.3 Einwohnermeldewesen

5.3.1 Regelmäßige Datenübermittlungen an den MDR bzw. die GEZ nach § 30 a Sächsisches Meldegesetz

Nach § 30 a SächsMG darf die Meldebehörde, die Gemeinde, dem Mitteldeutschen bzw. der GEZ u. a. Vor- und Zunamen sowie Veränderungsdaten volljähriger Einwohner zur Erhebung von Rundfunkgebühren mitteilen. Die Vorschrift, die eine regelmäßige Datenübermittlung zulässt, beruht auf der Überlegung, dass der MDR eine öffentlich-rechtliche Anstalt ist und zur Herstellung einer Gebührenberechtigung auf die Mitteilung von Meldedaten angewiesen ist.

Es handelt sich bei § 30 a SächsMG um eine Datenübermittlungsbefugnis und keine Pflicht der Meldebehörden. Dennoch übermitteln fast alle Gemeinden die Daten ihrer Einwohner an den MDR bzw. die GEZ. Viele bei mir eingehende Anfragen und Beschwerden zeigen, dass den Bürgern die Datenübermittlungsvorschrift nicht bekannt ist.

Mit der Änderung des Rundfunkgebührenstaatsvertrags (durch den 8. Rundfunkänderungsstaatsvertrag) werden nunmehr die öffentlich-rechtlichen Anstalten befugt, personenbezogene Daten wie Privatunternehmen nach dem Bundesdatenschutzgesetz zu verarbeiten, indem § 28 BDSG für anwendbar erklärt wird. Ich habe diese staatsvertragliche Regelung gegenüber der Staatsregierung kritisiert.

Dass mit dem Vertrag öffentlich-rechtliche Anstalten datenschutzrechtlich Privatunternehmen gleichgestellt werden, betrachte ich als verfassungsrechtlich bedenklich.

Die Datenschutzbeauftragten des Bundes und der Länder haben auf einer ihrer letzten Datenschutzkonferenzen deutlich gemacht, dass eine parallele Nutzung von Daten aus den Melderegistern bei gleichzeitiger Beschaffung von Adressen im privaten Adresshandel unverhältnismäßig ist. U. a. bemerken sie: „Die vorgesehene Befugnis ist mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Während öffentlich-recht-

liche Institutionen personenbezogene Daten nur verarbeiten dürfen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, ist die Datenverarbeitung der im Wettbewerb stehenden Privatwirtschaft vom Prinzip der Vertragsfreiheit geprägt. Die öffentlich-rechtlichen Rundfunkanstalten stehen hinsichtlich des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern. Schließlich haben die Länder gegen das Votum der Datenschutzbeauftragten bereits vor Jahren regelmäßige Übermittlungen von Meldedaten an die Rundfunkanstalten zugelassen, weil dies für erforderlich gehalten wurde. Eine parallele Nutzung von Daten aus den Melderegistern bei gleichzeitiger Beschaffung von Adressen im privaten Adresshandel ist jedoch unverhältnismäßig."

Ich habe mich daher bei der anstehenden Änderung des Sächsischen Meldegesetzes dafür ausgesprochen, dass § 30 a SächsMG gestrichen wird.

Der Auftrag, für einen ordnungsgemäßen Rundfunkgebühreneinzug zu sorgen, kann nicht eine maximierte Verarbeitung personenbezogener Daten unter Heranziehung aller möglichen Gesetzesgrundlagen rechtfertigen.

Der Gesetzgeber ist gefragt, verhältnismäßige Bedingungen bzw. eine neue Grundlage zur Gebührenerhebung zu schaffen, bei einer Institution, bei der fraglich ist, ob sie über eine unabhängige Datenschutzkontrolle im Sinne der EG-Datenschutzrichtlinie verfügt.

5.3.2 Novellierung des Sächsischen Meldegesetzes und des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung

Die Novellierungen des Sächsischen Meldegesetzes und des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung stehen an. Entwürfe wurden mir zur Stellungnahme zugeleitet. Mit der Novellierung des Meldegesetzes sollen die Vorgaben des Melderechtsrahmengesetzes des Bundes in Landesrecht umgesetzt werden. Kernpunkte sind der landesinterne und länderübergreifende Datenaustausch zwischen den Behörden auf elektronischem Weg und die Möglichkeit für den Bürger, z. B. die einfache Melderegisterauskunft oder seine Anmeldung über das Internet vornehmen zu können. Die Vertraulichkeit und Unversehrtheit der im Melderegister gespeicherten Daten ist gerade bei der Nutzung der modernen Kommunikations- und Informationstechnologien durch geeignete Maßnahmen zur Sicherung von Datenschutz und Datensicherheit, die dem Stand der Technik entsprechen, zu gewährleisten.

Darüber hinaus soll ein so genanntes Kommunales Kernmelderegister zur Speicherung ausgewählter Meldedaten für den automatisierten Abruf bereitgehalten werden. Gegen eine derartige Speicherung eines Teils des Meldedatensatzes bei einer zentralen Stelle

habe ich keine grundsätzlichen Einwendungen erhoben. Hinsichtlich der Einrichtung des Kommunalen Kernmelderegisters räumt das Melderechtsrahmengesetz den Ländern die Möglichkeit ein (§ 2 Abs. 3 MRRG), in den Landesgesetzen zu regeln, dass über die Festlegungen des Melderechtsrahmengesetzes hinaus weitere Daten zur Erfüllung von Länderaufgaben für einen automatisierten Abruf gespeichert werden können. Durch meine Intervention und Hinweis auf die notwendig nachzuweisende Erforderlichkeit der zu speichernden Daten, ist im Gesetzentwurf bis auf die Speicherung des Vorliegens einer sprengstoffrechtlichen Erlaubnis auf eine weitere Datenspeicherung verzichtet worden.

Ein wesentlicher Kritikpunkt des Entwurfs zur Meldegesetznovelle ist meinerseits die unveränderte Befugnis der Meldebehörden, der GEZ bzw. dem MDR regelmäßig Meldedaten zu übermitteln (ausführlich hierzu 5.3.1). Ich sehe noch die Möglichkeit, ggf. auch im parlamentarischen Verfahren, dass die Vorschrift gestrichen wird.

Mehrfach habe ich mich in meinen Tätigkeitsberichten (vgl. 3/5.3.3.3, 6/5.3.8. und 11/5.3.1) kritisch zu Gruppenauskünften vor Wahlen, Auskünften zu Jubiläen oder für Adressbücher o. ä. geäußert. Wenn die Novellierung des Sächsischen Meldegesetzes diese nach dem Melderechtsrahmengesetz zulässige Auskunftserteilung in besonderen Fällen im Grunde beibehalten werden soll, halte ich es für erforderlich und habe vom SMI gefordert, die Hinweispflicht des Betroffenen durch eine Modifizierung der entsprechenden Formulare nach der Meldevordruckverordnung zu unterstützen und den Betroffenen auf den Vordrucken durch Ankreuzen in Bezug auf die *jeweils einzelnen und sämtliche gesetzlichen Fälle* (§ 30 Abs. 2, § 32 Abs. 4, § 33 Abs. 4 SächsMG) die Möglichkeit zu geben, zu widersprechen. Der Hinweis würde in der Verwaltungspraxis keinerlei Nachteile mit sich bringen. In der Praxis zeigt sich vielmehr, dass der Hinweispflicht in vielen Fällen gerade nicht nachgekommen wird. Gerade bei der Umsetzung des neuen Meldegesetzes und Ausführungsverordnungen werde ich die Behörden weiter beraten.

5.3.3 Nutzung von Meldedaten zu Werbezwecken für eine stadteigene Verkehrsgesellschaft

Im letzten Berichtszeitraum erreichte mich eine Beschwerde eines Bürgers der Landeshauptstadt, der ein Werbeschreiben der Dresdener Verkehrsbetriebe AG (DVB AG), bei der die Stadt Alleingesellschafterin ist, erhalten hatte, kurz nachdem er seinen Hauptwohnsitz bei der Meldebehörde in Dresden angemeldet hatte.

Nachdem ich die Stadtverwaltung um Stellungnahme gebeten hatte, stellte sich mir der Sachverhalt folgendermaßen dar: Die Stadt Dresden hatte im Zeitraum Dezember 2001

bis September 2004 auf Antrag der DVB AG in 20.458 Fällen Meldedatensätze für Werbeschreiben zur Verfügung gestellt. Nachdem zunächst eine Etikettierung und Kuvertierung durch die Meldebehörde selbst vorgenommen wurde, erfolgte letztendlich eine Übermittlung von Meldedaten an die DVB AG mit der Übersendung von Etikettenaufdrucken. Am Ende des Jahres 2004 ist diese Nutzung der Meldedaten für Werbezwecke eingestellt worden. Anlass hierfür war erst eine bei der Meldebehörde eingegangene Beschwerde eines Bürgers. Diese hatte dazu geführt, dass dem Datenschutzbeauftragten der Stadt Dresden der Vorgang mit der Bitte um Stellungnahme zugeleitet wurde. Dieser teilte dem verantwortlichen Geschäftsbereich der Stadt zutreffend mit, dass die weitergehende Nutzung der Meldedaten unzulässig gewesen sei. Daraufhin wurde die Praxis nicht mehr fortgesetzt.

Die Versendung der Werbeschreiben der DVB AG durch das Einwohnermeldeamt erfolgte unter Umgehung der strengen Zweckbindung der Meldedaten. Melderechtlich handelte es sich um eine Nutzung der Meldedaten für gesetzlich nicht vorgesehene Zwecke bzw. um eine unerlaubte regelmäßige Meldedatenübermittlung an Private. In Bezug auf die zunächst getroffene Entscheidung der Meldebehörde, die Werbeschreiben der DVB AG selbst zu kuvertieren und unter Nutzung des Melderegisters Etiketten herzustellen, die Kuverts zu etikettieren und die Werbeschreiben der DVB AG zu versenden, mangelte es an einer Rechtsgrundlage, wie § 4 Abs. 1 SächsDSG es verlangt. Es gehört schlichtweg nicht zu den Aufgaben einer Meldebehörde, Werbeaktionen zu betreiben. Die DVB AG ist auch ein Privatunternehmen und die Übermittlung von Meldedaten an Private regelt sich nach § 32 Abs. 3 SächsMG. Keine Rolle spielen die Eigentumsverhältnisse, dass die Stadt Alleingesellschafterin ist.

Aus den mir sich darstellenden Unterlagen ergab sich auch, dass der Meldebehörde frühzeitig bekannt gewesen sein muss, dass eine derartige Übermittlung an eine Privatfirma in Form einer Gruppenauskunft nicht mit einem nach dem Meldegesetz geforderten öffentlichen Interesse begründet werden konnte. Beabsichtigt war dennoch eine unbefristete und regelmäßige Datenübermittlung an die DVB AG, was dann mit den tatsächlich stattgefundenen Datenübermittlungen begonnen wurde, umzusetzen.

Obwohl die Verfahrensweise erkennbar nicht auf eine gesetzliche Grundlage gestützt werden konnte, versuchte die Stadt in ihren Stellungnahmen mir gegenüber ein öffentliches Interesse zu konstruieren. Der Vorgang stellte sich insbesondere wegen des Umfangs der Datenmengen und wegen seiner zeitlichen Dauer einen erheblichen Datenschutzverstoß dar.

Gegen das Anbieten von Informationsmaterial zum Nahverkehr durch eine Gemeinde als Serviceleistung für neue Einwohner durch die Mitarbeiter der Bürgerbüros oder der

Einwohnermeldeämter ist nichts einzuwenden, zu einer zweckwidrigen Nutzung von Meldedaten sind die Kommunen jedoch nicht befugt, auch nicht um ihre kommunalen Unternehmen zu unterstützen, so nützlich dies letztendlich auch für die Gemeindekassen und kommunale Unternehmen sein mag. Das Sächsische Datenschutzrecht geht vielmehr vom funktionalen Stellenbegriff aus. Die Verarbeitung personenbezogener Daten, die die Gemeinde durchführt und die ihrer Wirtschaftunternehmen, deren Eigentümerin sie ist, sind informationell zu trennen. Die Daten der Meldebehörde sind sogar zunächst informationell getrennt von denen der anderen Bereiche der Gemeindeverwaltung zu verarbeiten. Bereits jede Übermittlung der Meldebehörde an andere Bereiche der Gemeindeverwaltung stellt eine Übermittlung an andere öffentliche Stellen dar.

In Auswertung des Vorgangs wurde seitens der Stadtverwaltung die Festlegung getroffen, für neu eingehende Anträge auf Gruppenauskunft den Datenschutzbeauftragten der Stadt in die Prüfung einzubeziehen und seine schriftliche Stellungnahme nunmehr dem Vorgang beizufügen. Diese organisatorische Entscheidung ist positiv zu bewerten gewesen. Ich habe bei der Stadt zudem angeregt, auch die Herausgabe einer Dienstanweisung zur Auskunftserteilung nach §§ 29, 32, 33 SächsMG, die im Zweifelsfall eine unzulässige Auskunftserteilung vermeiden helfen könnte, zu prüfen.

5.4 Personenstandswesen

5.4.1 Verlesung von Berufsbezeichnungen bei Eheschließungen

Durch den Hinweis eines Betroffenen erfuhr ich von einer gängigen, aber nicht datenschutzgerechten Verwaltungsübung der Standesämter. Eine Gemeinde bestätigte mir auf Nachfrage die Verfahrensweise, wonach durch die Standesbeamten während der Trauung der im Heiratsbuch einzutragende Beruf oder die gegenwärtig ausgeübte Tätigkeit vor den Versammelten laut verlesen worden ist. Durch diese ungefragte Offenbarung seiner beruflichen Tätigkeit sah sich der Betroffene in seinem Grundrecht auf informationelle Selbstbestimmung beeinträchtigt. Auch wurde mir von der Gemeinde mitgeteilt, dass regelmäßig so verfahren wird. Die Vorgehensweise sei von der Fachaufsicht geprüft worden und gängige Praxis in allen Standesämtern der Umgebung.

Demgegenüber stellt sich die Rechtslage folgendermaßen dar: Nach dem Personenstandsgesetz sind in das Heiratsbuch neben der Erklärung der Eheschließenden und dem Ausspruch des Standesbeamten die Vor- und Familiennamen der Eheschließenden, ihr Beruf und Wohnort, Ort und Tag ihrer Geburt sowie - im Falle des Einverständnisses - ggf. die Zugehörigkeit zu einer Kirche, Religionsgesellschaft oder Weltanschauungsgemeinschaft einzutragen. Außerdem sind die Vor- und Familiennamen der bei der

Eheschließung anwesenden Zeugen, ihr Alter, Beruf und Wohnort einzutragen (§ 11 PStG). Nach der Personenstandsverordnung sollen Eintragungen, die im Heiratsbuch vorgenommen werden, 1. den Ort und Tag der Eintragung, 2. die Bezeichnung der Erschienenen, 3. den Vermerk des Standesbeamten, dass und wie er die Persönlichkeit der Erschienenen festgestellt hat und 4. *den Vermerk, dass die Eintragung den Erschienenen vorgelesen und von ihnen genehmigt worden ist* enthalten (§ 3 PStV).

Ich habe den Bürgermeister darauf aufmerksam gemacht, dass es hingegen rechtsirrig sei, aus § 3 PStV abzuleiten, dass die nach dem Personenstandsgesetz vorzunehmenden Eintragungen in das Heiratsbuch während der Trauung (§ 1312 BGB) vorzulesen seien.

Weder das Personenstandsgesetz noch die Personenstandsverordnung setzen die Bekanntgabe anderer Daten als den Namen der Eheschließenden und gegebenenfalls der Zeugen voraus. Die Bekanntgabe weiterer Daten entspricht daher einer - hier nicht zulässigen - Übermittlung personenbezogener Daten an nicht-öffentliche Stellen gemäß § 16 Abs. 1 SächsDSG. Ein solcher Datenverarbeitungsvorgang unterliegt dem Grundrecht auf informationelle Selbstbestimmung. Die Übermittlung mit einer Einwilligung der Betroffenen sehe ich insofern hingegen als zulässig an (vgl. § 4 Abs. 1 Nr. 2 SächsDSG).

Der Standesbeamte hat also vor der Trauung und im Zusammenhang mit seiner Prüfung der Voraussetzungen der Anmeldung der Eheschließung (§§ 5, 5 a, 6 PStG) zeitlich ausreichende Gelegenheit, die nach dem Personenstandsgesetz (§ 11 Abs. 1) von ihm vorzunehmenden Eintragungen den Eheschließenden und gegebenenfalls den Zeugen vorzulesen. Dabei hat er auch die Möglichkeit zu erfragen, ob bzw. inwieweit eingewilligt wird, weitergehende Daten auch bei der Trauung zu verlesen. Fehlt eine solche Einwilligung, wie im vorliegenden Fall, sind die Daten bei der Trauung nicht zu verlesen, sondern die Erschienenen lediglich namentlich zu benennen.

Von einer Beanstandung der Gemeinde habe ich bei dem konkreten Vorgang u. a. abgesehen, da der Bürgermeister meine Ausführungen unverzüglich zum Anlass nahm, die Verfahrensweise bei der Durchführung von Trauungen meinen Empfehlungen entsprechend anzupassen.

Wegen der Bedeutung des Falles in Bezug auf eine rechtseinheitliche, das informationelle Selbstbestimmungsrecht der Betroffenen beachtende Anwendung des § 11 Abs. 1 PStG i. V. m. § 3 PStV in Sachsen habe ich mich an das SMI gewandt. Das Staatsministerium unterstützte mich in meiner Rechtsauffassung und bat in einem Schreiben an die Aufsichtsbehörden, das nachrichtlich auch der Landesfachverband der

Standesbeamtinnen und Standesbeamten des Freistaates Sachsen erhielt, meine gegebenen Empfehlungen zu beachten.

Nach einem mehrjährigen Verfahren habe ich Anfang 2005 den Gesetzentwurf des BMI zur Reform des Personenstandsrechts zur Stellungnahme übersandt bekommen. Der dort u. a. vorgesehene Verzicht auf die Erfassung personenstandsfremder Daten wie das des Berufs in einem neu zu schaffenden Register schafft insofern Klarheit.

5.5 Kommunale Selbstverwaltung

5.5.1 Datenschutzgerechte Abrechnung von Schiedsstellengebühren

Der Friedensrichter der Schiedsstelle einer sächsischen Gemeinde wandte sich an mich und äußerte Zweifel an der datenschutzrechtlichen Zulässigkeit der ihm bekannten Abrechnungspraxis von Verfahrensgebühren seiner Schiedsstelle.

Die Gemeinde, die die Schiedsstelle eingerichtet hatte, verbuchte die von den Antragstellern einzuzahlenden Gebührenvorschüsse auf einem von ihr geführten Anderkonto. Mit der Buchung erlangt die Gemeinde aber nicht nur Kenntnis von der Tatsache, ob der Vorschuss gezahlt wurde. Das im Verwendungszweck der Überweisung angegebene Aktenzeichen lässt auch erkennen, um welche Verfahrensart vor der Schiedsstelle es sich handelt (Verfahren in bürgerlichen Streitigkeiten; Sühneverfahren; gemischtes Verfahren).

Ein vergleichbares Problem stellt sich in den Fällen der baren Leistung der Gebühren. Wie mir das SMJus mitteilte, seien die Friedensrichter gehalten, die Gelder aus ihren Schiedsstellenkassen in die Kasse der Gemeinde einzuzahlen, da in Sachsen das Prinzip der Einheitskasse bestehe. Von der Gemeindekasse sei dann eine Prüfung auf sachliche und rechnerische Richtigkeit vorzunehmen, die in der Regel vom örtlichen Rechnungsprüfungsamt verlangt werde und ohne Kenntnis der Daten des Einzahlers (Name und Verfahrensart) nicht möglich sei.

Die Gemeinden errichten Schiedsstellen und sind als Träger der Schiedsstellen außerhalb der Verfahren aufsichts- und weisungsbefugt. Die Aufsicht über die ordnungsgemäße Durchführung der Verfahren obliegt dem Vorstand des zuständigen Amtsgerichts. Im Rahmen der Verfahren und der damit verbundenen Verarbeitung personenbezogener Daten der Beteiligten agiert die - auch funktional eigenständige - Schiedsstelle unabhängig von der Gemeinde.

Die Verbuchung von Gebühren und Gebührenvorschüssen fällt in den Aufgabenbereich der Schiedsstellen. Erst wenn der Kostenschuldner die ihm mitgeteilte Kostenrechnung nicht begleicht, darf die Gemeinde tätig werden, indem sie die Kosten dann nach den

Vorschriften des Sächsischen Verwaltungsvollstreckungsgesetzes beitreibt. Im Rahmen dieser Aufgabenerfüllung erhält dann die Gemeinde Kenntnis von Daten des Kostenschuldners. Das ist für die Durchführung der Vollstreckung erforderlich und datenschutzrechtlich nicht zu beanstanden.

Die datenschutzrechtliche Bewertung kann auch im Fall der baren Leistung der Gebühren nicht anders ausfallen.

Die Gemeinde ist zwar Trägerin der Schiedsstelle, sie darf aber nicht auf die personenbezogenen Daten zugreifen, die die (insoweit gemeindeunabhängige) Schiedsstelle in einem Schiedsverfahren verarbeitet. Das Prinzip der Einheitskasse darf nicht dazu führen, dass Daten funktional getrennter Stellen auf diesem Weg der jeweils anderen Stelle zur Kenntnis gelangen.

Für eine Prüfung auf sachliche und rechnerische Richtigkeit benötigt die Gemeindekasse allenfalls einen Hinweis auf die Art des Verfahrens, die dem Aktenzeichen zu entnehmen ist. Der Name des verfahrensbeteiligten Einzahlers ist für eine Plausibilitätsprüfung irrelevant. Im Einzelfall kann eine Rückfrage (des Rechnungsprüfungsamtes) beim Friedensrichter erfolgen.

Dem örtlichen Rechnungsprüfungsamt dürfen zur Erfüllung seiner Aufgaben personenbezogene Daten übermittelt werden. Allerdings ist das Rechnungsprüfungsamt nicht befugt, den Friedensrichter anzuweisen, der Gemeindekasse Namen des Beteiligten und Verfahrensart mitzuteilen.

Das SMJus erwog, auf die Einrichtung eigener, vom Konto der jeweiligen Gemeindekassen unabhängiger Schiedsstellenkonten hinzuwirken und informierte mich über die Absicht des SMI, bei der anstehenden Überarbeitung der Gemeindekassenverordnung eine klarstellende Regelung für die Kassengeschäfte der Friedensrichter aufzunehmen. Nach Auskunft des SMJus wird es demnächst Gespräche mit dem Schiedsstellenverband führen, in denen auch die Problematik datenschutzgerechter Gebührenabrechnung thematisiert werden wird.

5.5.2 Beitreibung und Abtretung von Bußgeld- und Gebührenforderungen durch bzw. an Private

Schon seit einigen Jahren gibt es in sächsischen Gemeinden Überlegungen, Leistungsbescheide gegen Bürger, die auf eine Geldzahlung gerichtet sind, durch private Inkassounternehmen beitreiben zu lassen. Bereits in 6/5.5.6 und 7/5.5.9 habe ich meine grundsätzlichen Vorbehalte gegen die Übertragung von öffentlich-rechtlichen Forderungen auf Private, sei es im Wege der Inkassozession oder im Wege der Abtretung, geltend

gemacht. Die Eingabe eines Bürgers, dessen aus einer Verkehrsordnungswidrigkeit resultierendes Bußgeld im Auftrag des Landratsamtes als Verfolgungsbehörde durch ein privates Inkassounternehmen beigetrieben werden sollte, ist für mich Anlass, erneut zu dieser Problematik - hier speziell zur Beitreibung von Bußgeldern aus Verkehrsordnungswidrigkeiten - Stellung zu nehmen.

Das Ordnungswidrigkeitenverfahren ist als hoheitliches Verfahren gesetzlich ausgestaltet. Im Rahmen der Ermittlung, Verfolgung und Ahndung der Ordnungswidrigkeit wird die zuständige Verfolgungsbehörde hoheitlich tätig. Dies wird für den Betroffenen insbesondere dadurch deutlich, dass ihn nach Abschluss des Bußgeldverfahrens ein Bußgeldbescheid erreicht. Das maßgebende Gesetz über Ordnungswidrigkeiten regelt aber nicht nur das Verfahren bis zum Erlass eines Bescheides oder gerichtlichen Urteils, sondern trifft darüber hinaus auch Aussagen zur Vollstreckung der jeweiligen Entscheidung. So legt § 90 Abs. 1 OWiG fest, dass der Bußgeldbescheid, soweit er durch eine Verwaltungsbehörde eines Landes erlassen wurde, nach den Vorschriften des Verwaltungsvollstreckungsgesetzes des Landes vollstreckt wird. Zuständige Vollstreckungsbehörde ist gemäß § 92 OWiG, der insoweit die landesrechtliche Vorschrift des § 4 SächsVwVG verdrängt, die Verwaltungsbehörde, die den Bußgeldbescheid erlassen hat.

Das Sächsische Verwaltungsvollstreckungsgesetz regelt die Vollstreckung von Leistungsbescheiden - und Bußgeldbescheide sind auf die Zahlung bestimmter Geldbeträge gerichtete Leistungsbescheide - in den §§ 12 ff. Danach kann die Beitreibung der Forderung auf verschiedene Weise erfolgen. Nicht vorgesehen ist die Übertragung der Forderung auf Private, weder in Form der Inkassozession noch als Forderungsabtretung. Allein der Gerichtsvollzieher als außerhalb der Vollstreckungsbehörde stehende Person kann durch die Vollstreckungsbehörde - etwa im Fall der Beitreibung durch Vollstreckung in bewegliche Sachen nach § 14 Abs. 2 SächsVwVG - eingeschaltet werden. Das klar geregelte Verfahren enthält keine Öffnungsklauseln, die eine Abgabe der Vollstreckung an Private gestatten würden. Dadurch wird neben der Erfüllung des rechtsstaatlichen Gebots hinreichender Bestimmtheit und Klarheit in Grundrechte eingreifender Normen auch das Grundrecht auf informationelle Selbstbestimmung geschützt. Die im hoheitlich ausgestalteten Bußgeldverfahren durch die Verfolgungsbehörde erlangten personenbezogenen Daten des Betroffenen verbleiben bei der Verfolgungsbehörde, da das Gesetz letztere auch als Vollstreckungsbehörde bestimmt. Ausnahme ist allein die - allerdings auch gesetzlich geregelte - Betrauung des Gerichtsvollziehers mit einzelnen Tätigkeiten in der Vollstreckung. Zuständigkeits- und Verfahrensvorschriften wie § 92 OWiG und §§ 12 ff. SächsVwVG bestimmen, welche Stelle die im Verfahren erhobenen personenbezogenen Daten verarbeiten darf. Ist aber

gesetzlich klar geregelt, welche Aufgaben von welcher Stelle in welcher Art und Weise zu erfüllen sind, ist kein Raum für die Übertragung von Aufgaben oder einzelnen Tätigkeiten. Übertrüge die Verfolgungsbehörde die Vollstreckung eines Bußgeldbescheides auf ein privates Inkassounternehmen, würde sich die Vollstreckung entgegen der Vorschrift von § 90 Abs. 1 OWiG nicht mehr nach den Vorschriften des Sächsischen Verwaltungsvollstreckungsgesetzes richten, da letzteres auf öffentliche Stellen des Freistaates Sachsen, nicht aber auf Private Anwendung findet. Die Übertragung der Vollstreckung und mithin auch die Übermittlung der im Bußgeldverfahren erhobenen personenbezogenen Daten hätte keine gesetzliche Grundlage und wäre unzulässig.

Die Forderungsabtretung an einen Privaten im Wege des Factoring erachte ich erst recht als unzulässig. Dabei verkauft die Verwaltungsbehörde ihre Forderung an das Inkassounternehmen. Dieses vollstreckt allein im Eigeninteresse, nicht aber im Auftrag der Verwaltungsbehörde, die sich mit dem Verkauf ihrer Forderung ihrer Einflussmöglichkeiten begibt. Ob der Forderungskäufer die von ihm erworbene Forderung vollstreckt, bleibt ihm überlassen. Der private Zessionar ist nun auch nicht mehr für die Einhaltung des Sächsischen Datenschutzgesetzes und anderer für öffentliche Stellen geltende Vorschriften über den Datenschutz verantwortlich. Er unterliegt dann als nicht öffentliche Stelle den Bestimmungen des Bundesdatenschutzgesetzes.

Personenbezogene Daten des Betroffenen eines hoheitlichen Verfahrens, in dem anfangs - bei Verfolgung und Ahndung der Ordnungswidrigkeit - Datenschutzverpflichtungen öffentlicher Stellen greifen, dürfen im Endstadium des Verfahrens nicht durch die Abtretung der öffentlich-rechtlichen Forderung an einen Privaten für dessen eigene Geschäftszwecke „freigegeben“ werden. Grundrechtsschutz wird eben auch durch Verfahrensrecht gewährleistet.

5.5.3 Verschwiegenheitspflicht und Verpflichtung der Gemeinde- und Kreisräte auf das Datengeheimnis

Bereits mehrfach habe ich auf Verstöße von Gemeinde- und Kreisräten gegen die ihnen auferlegte Verschwiegenheitspflicht aufmerksam gemacht (vgl. 11/5.5.4). Auch in diesem Berichtszeitraum musste ich wieder einige Verstöße dieser Art feststellen. Für die von der Preisgabe ihrer personenbezogenen Daten Betroffenen ist das zum Teil mit erheblichen Beeinträchtigungen verbunden. In einem Fall, bei dem die Beteiligung von Stadträten nicht auszuschließen war, hatten gezielte Indiskretionen mit nachteiligem Inhalt in Bezug auf einen leitenden Mitarbeiter der Stadt an die Presse zur Folge, dass dessen berufliches Fortkommen verhindert, seine Existenz gefährdet, zumindest aber erschwert wurde. Einige Gemeinde- und Kreisräte scheinen schlichtweg nicht zu

begreifen, dass sie Teil eines Verwaltungsorgans sind, sie entsprechenden geregelten Verhaltenspflichten unterliegen und sich nicht auf übergesetzliche Sonderrechte berufen können.

Dabei sind Gemeinde- und Kreisräte nach § 19 Abs. 2 SächsGemO bzw. § 17 Abs. 2 SächsLKrO zur Verschwiegenheit über alle Angelegenheiten verpflichtet, deren Geheimhaltung gesetzlich vorgeschrieben, besonders angeordnet oder ihrer Natur nach erforderlich ist. Sie dürfen die Kenntnis von geheim zu haltenden Angelegenheiten nicht unbefugt verwerten. Das wirkt auch nach Beendigung der ehrenamtlichen Tätigkeit fort. § 37 Abs. 2 SächsGemO bzw. § 33 Abs. 2 SächsLKrO regelt darüber hinaus die Verschwiegenheitspflicht über alle in nicht öffentlicher Sitzung behandelten Angelegenheiten. Nach § 35 Abs. 1 SächsGemO (§ 31 Abs. 1 SächsLKrO) verpflichtet der Bürgermeister bzw. Landrat die Gemeinderäte bzw. Kreisräte in der ersten Sitzung öffentlich auf die gewissenhafte Erfüllung ihrer Pflichten. Ein Verstoß gegen die Verschwiegenheitspflicht gemäß § 19 Abs. 2 SächsGemO (§ 17 Abs. 2 SächsLKrO) kann durch den Gemeinderat/Kreistag nach § 19 Abs. 4 SächsGemO (§ 17 Abs. 4 SächsLKrO) mit bis zu 500 € geahndet werden.

Zusätzlich zu der Verpflichtung nach der Gemeinde- bzw. Landkreisordnung durch den Bürgermeister bzw. Landrat ist eine schriftliche Verpflichtung auf das Datengeheimnis nach § 6 SächsDSG vorzunehmen. So sind alle für *eine öffentliche Stelle tätigen Personen* auf das *Datengeheimnis zu verpflichten.* Nach der Gesetzeslage, die keine Ausnahmen vorsieht und wegen der fortgesetzten Verstöße durch Gemeinde- und Kreisräte ist diese zusätzliche Maßnahme auch nicht verzichtbar, zumal das Datengeheimnis und die Verschwiegenheitspflicht nicht deckungsgleich sind.

Meiner Forderung, die Bediensteten (Amtsträger) der Gemeinde- und Landkreisverwaltungen wie der Landesverwaltung auf das Datengeheimnis zu verpflichten, ist ohnehin - das zeigen mir meine vielen Gespräche und Kontrollen in den Kommunen - bereits weitgehend entsprochen worden. In den wohl meisten größeren Städten sind die Stadträte ebenfalls auf das Datengeheimnis verpflichtet worden. Dies ist übrigens umso bemerkenswerter, als dass sich im Jahr 2001 diesbezüglich ein Regierungspräsidium mit einem Erlass an die Landkreise und Kreisfreien Städte wandte und mitteilte, es sei nicht erforderlich, Mitglieder des Gemeinderates nach § 6 Abs. 2 SächsDSG auf das Datengeheimnis zu verpflichten. Gemeinderäte seien nicht - und man bezog sich damit auf den konkreten Wortlaut des alten Sächsischen Datenschutzgesetzes - „bei der Datenverarbeitung beschäftigt“. Die in § 35 Abs. 1 Satz 2 SächsGemO ausdrücklich vorgeschriebene allgemeine Verpflichtung auf die gewissenhafte Erfüllung ihrer Pflichten und die in § 37 Abs. 2 SächsGemO normierte Pflicht zur Verschwiegenheit von Angelegenheiten, die in nicht öffentlicher Sitzung behandelt worden sind, stellten

auch mit Blick auf datenschutzrechtliche Belange ausreichende bereichsspezifische Regelungen dar. Für Mitglieder des Kreistages gelte dies entsprechend. Abgesehen davon, dass die Auffassung des Regierungspräsidiums, Gemeindevertreter seien nicht „bei der Datenverarbeitung beschäftigt“, schon bereits nicht zutrifft, da die alte Vorschrift mit ihrem Wortlaut sich nicht lediglich auf formale Beschäftigungsverhältnisse bezog, ist mit der Novellierung des Sächsischen Datenschutzgesetzes im Jahr 2003 durch die redaktionelle Änderung in „Den für eine öffentliche Stelle tätigen Personen …“ (§ 6 Abs. 1 SächsDSG n. F.) eine Klarstellung erfolgt. Die Rechtslage sollte insofern eigentlich klar sein. Im Einklang mit dieser Rechtslage steht auch, dass Gemeinde- und Kreisräte als Amtsträger anzusehen sind. Sowohl die Literatur (u. a. Schönke/Schröder und Tröndle/Fischer (Kommentierungen zum Strafgesetzbuch), Gern: Kommunalrecht, Meyer, Das Recht der Ratsfraktionen, Wiesbaden 1994; Epp, Die Abgeordnetenbestechung, Frankfurt/M 1997, S. 103 ff., S. 384 ff.) als auch die Rechtsprechung (LG Krefeld, Beschl. vom 14. März 1994 - 21 Qs 22/94; BGH, Urt. vom 21. Dezember 1998 - III ZR 118/88) geht von der *Amtsträgereigenschaft* der Gemeinde- und Kreisräte gemäß § 11 Abs. 1 Nr. 2 c StGB aus. Danach ist Amtsträger, „wer nach deutschem Recht sonst dazu bestellt ist, bei einer Behörde oder bei einer sonstigen Stelle oder in deren Auftrag Aufgaben der öffentlichen Verwaltung unbeschadet der zur Aufgabenerfüllung gewählten Organisationsform wahrzunehmen“.

Die speziellen Regelungen zum Verschwiegenheitsgebot für Gemeinde- und Kreisräte in der Gemeinde- bzw. der Landkreisordnung besagen, dass diese die ihnen im Zusammenhang mit ihrer ehrenamtlichen Tätigkeit zur Kenntnis gelangten geheim zu haltenden Angelegenheiten nicht unbefugt *offenbaren* oder *verwerten* dürfen. Unter Verwerten ist allgemein „verwenden“, „anwenden“, „sich einer Sache bedienen“, „Nutzen“, „sich zunutze machen“ zu verstehen. Den Kommentaren zur Gemeinde- und Landkreisordnung ist gemeinsam, dass sie zum Ausgangspunkt der Verschwiegenheitspflicht über die geheim zu haltenden Angelegenheiten deren Kenntnis voraussetzen. Sie stellen darauf ab, dass alles zu unterlassen ist, was die Geheimhaltung gefährden könnte und darüber hinaus auf die unbefugte Verwertung dieser Kenntnisse. Als Beispiele werden u. a. „das sorglose Liegenlassen von Akten“, „Verschwiegenheit gegenüber Angehörigen und der Presse“, „Erwerb eines Grundstücks in Kenntnis der geplanten Bebaubarkeit“ genannt.

Demgegenüber ist es nach dem Datengeheimnis den für eine öffentliche Stelle tätigen Personen untersagt, personenbezogene Daten unbefugt zu *verarbeiten* (§ 6 Abs. 1 Satz 1 SächsDSG). Die auf das Datengeheimnis verpflichteten Personen (oder ehrenamtlich Tätigen) sind bei dienstlichem Zugang zu personenbezogenen Daten verpflichtet, diese nur im Rahmen der ihnen zugewiesenen Aufgabe zu verwenden. Das Datengeheimnis

untersagt das unbefugte Verarbeiten als „Erheben“, „Speichern“, „Verändern“, „Anonymisieren“, „Übermitteln“, „Nutzen“, „Sperren“ und „Löschen“ von personenbezogenen Daten insgesamt (§ 3 Abs. 2 SächsDSG). Unbefugt ist jeder Umgang mit personenbezogenen Daten zu einem anderen als dem zur jeweiligen Aufgabenerfüllung - bei den Gemeinde- bzw. Kreisräten sind die Aufgaben in § 28 SächsGemO bzw. § 24 SächsLKrO beschrieben - gehörenden Zweck. Dadurch, dass die Verpflichtung auf das Datengeheimnis das Erheben personenbezogener Daten als jedes zielgerichtete Beschaffen beim Betroffenen selbst oder durch zweckgerichtete Beobachtung oder unter Mitwirkung anderer einschließt, wird der Unterschied dieser datenschutzrechtlichen Vorschrift auch zum allgemeinen Amtsgeheimnis und den speziellen Berufs- oder Amtsgeheimnissen deutlich. Diese erfassen in der Regel nur die unbefugte Offenbarung an Dritte, also das Übermitteln. Das Datengeheimnis bewirkt, dass selbst Mitarbeiter beauftragter Unternehmen und Verwaltungshelfer, die eine weitaus weniger enge Bindung zur Gemeinde- bzw. Landkreisverwaltung haben (vgl. Ancôt, Sächsisches Datenschutzgesetz, Kommentar, 2. Aufl. 2004 § 6 Rdnr. 2) als Gemeinde- und Kreisräte (die Inhaber eines öffentlichen Amtes sind) zu verpflichten sind.

Dem eventuellen Einwand, das Sächsische Datenschutzgesetz sei nicht einschlägig, weil nach § 2 Abs. 4 SächsDSG das Gesetz nur anzuwenden ist, soweit nicht besondere Rechtsvorschriften des Freistaates Sachsen oder des Bundes den Schutz personenbezogener Daten regeln, ist Nachstehendes entgegenzuhalten. Zwar ist das Sächsische Datenschutzgesetz als Auffanggesetz zum Schutz personenbezogener Daten nachrangig gegenüber spezialgesetzlichen Regelungen. Es schließt aber die Lücke dann und ist als Rechtsgrundlage heranzuziehen, wenn spezialgesetzliche Regelungen wie z. B. die Sächsische Gemeinde- bzw. Landkreisordnung diesen Schutz nicht gewähren. Auch hat der Gesetzgeber die Sanktionsmöglichkeiten bezogen auf die Höhe der zu bemessenden Strafe bei einem Verstoß gegen das Datengeheimnis deutlich höher bemessen, als die Sanktionsmöglichkeit bei einem Verstoß gegen die in der Sächsischen Gemeinde- bzw. Landkreisordnung geregelte Verschwiegenheitspflicht. Ein Verstoß gegen das Datengeheimnis kann als Ordnungswidrigkeit mit einer Geldbuße bis zu 25.000 € (§ 38 Abs. 2 SächsDSG) und in besonderen Fällen als Straftat mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe (§ 39 SächsDSG) geahndet werden. Ein Verstoß gegen die in der Sächsischen Gemeinde- bzw. Landkreisordnung geregelte Verschwiegenheitspflicht dagegen beschränkt sich auf das Auferlegen eines Ordnungsgeldes in einer Höhe von bis zu 500 €.

Ich bin davon überzeugt, dass die zusätzlich zur Verschwiegenheitspflicht nach der Gemeinde- bzw. Landkreisordnung abzugebende Verpflichtung der Gemeinde- und Kreisräte auf das Datengeheimnis im Übrigen geeignet ist, das Vertrauen der Bürger in

ihre gewählten kommunalen Vertreter sowie die öffentliche Verwaltung insgesamt zu stärken.

5.5.4 Prangerwirkung durch die Veröffentlichung eines Zeitungsbeitrags mit personenbezogenen Angaben im Amtsblatt einer Gemeinde

Bereits mehrfach hatte ich in meinen Tätigkeitsberichten auf die Veröffentlichung personenbezogener Daten mit Prangerwirkung hingewiesen (11/5.5.2 und 11/5.6.1).

In der Ausgabe des Amtsblatts einer Stadt erfolgte im November 2003 der Nachdruck eines Zeitungsbeitrages einer großen überregional erscheinenden Tageszeitung, in dem personenbezogene Daten einer Person mit Vor- und Zunamen verarbeitet wurden. Mit Eingabe wendete sich der Petent an mich, nachdem der Artikel der Zeitung, in dem der Petent mit Vor- und Zunamen und Herkunftsort (er war nicht Einwohner der Gemeinde) identifizierbar bezeichnet worden war, im Amtsblatt der Stadt veröffentlicht wurde. Der Artikel enthielt mehrere Tatsachenbehauptungen in Bezug auf den Betroffenen. Es war u. a. auch die Rede von einem angeblich noch nicht abgeschlossenen Ermittlungsverfahren gegen den Betroffenen und von seiner bisherigen Rolle im Zusammenhang mit der Veröffentlichung von Musik mit rechtsextremen Texten. Der Wortlaut des abgedruckten Textes war mit dem in dem Beitrag einer überregionalen Zeitung identisch. Neben der Überschrift war ein Emblem eines eingetragenen Vereins abgedruckt worden und über der Überschrift befand sich ein Quellenhinweis. Unter dem eigentlichen Beitrag war ein Hinweis der Stadtverwaltung abgedruckt, dass der Betroffene sein „Tätigkeitsfeld“ in den letzten Jahren auch auf den Verwaltungsbereich der Stadt „ausgedehnt“ habe. Der Betroffene befand sich zum Zeitpunkt der Veröffentlichung im Amtsblatt seit Mitte des Jahres 2001 im Strafvollzug zur Verbüßung einer Haftstrafe, was in dem Zeitungsbeitrag selbst Erwähnung fand. Neben den vornehmlich gegen den Betroffenen gerichteten Aussagen im Zusammenhang mit Vorgängen der Justiz enthielt der Beitrag auch Andeutungen über die Rolle des LfV. Unter anderem enthielt der Zeitungsbeitrag die Angabe, dass es unklar sei, zu welchem Zeitpunkt der Betroffene mit dem Verfassungsschutz kooperiert habe und welche kriminelle Aktivitäten er unter den Augen oder gar mit stillschweigender Billigung seiner Verbindungsleute ausgeführt habe. Der Betroffene selbst schweige eisern über seine Kontakte zu dem Geheimdienst und auch der Verfassungsschutz zeige keine Neigung, die „dubiose Liaison mit dem kriminellen Spitzel“ aufzuklären.

Die Gemeinde vertrat in ihrer Stellungnahme mir gegenüber die Auffassung, dass eine Persönlichkeitsrechtverletzung des Betroffenen nicht vorliege. Das „Informationsrecht der Öffentlichkeit“ wiege schwerer als das Persönlichkeitsrecht. Zudem handele es sich bei dem Betroffenen um eine „stadtbekannte Person“, die durch „zahlreiche Funk- und

Fernsehberichte im Zusammenhang mit ihrem Tätigwerden in der rechten gewaltbereiten Szene und vermutlich auch für seine mittlerweile ebenfalls öffentlich gemachten Aktivitäten für den Verfassungsschutz“ bekannt sei. In der Sache selbst berief sich die Gemeinde für die Veröffentlichung auf Art. 28 Abs. 2 GG, die kommunale Selbstverwaltungsautonomie. So gehöre auch Gewalt- und Kriminalprävention zum Aufgabenbereich der Gemeinde.

Es ist meine gesetzliche Aufgabe, Verletzungen des Grundrechts auf informationelle Selbstbestimmung ohne Ansehen der betroffenen Person zu behandeln, sei der Betroffene Straftäter, sei er politisch missliebig oder sei er sonst Behörden unangenehm aufgefallen. Ausnahmslos jeder Grundrechtsträger hat einen Anspruch darauf, dass sächsische öffentliche Stellen ihn mit „Fairness“, d. h. ganz einfach rechtsstaatlich behandeln. Nach unserem Verfassungsverständnis muss niemand damit rechnen, dass Behörden ihn abseits gesetzlicher Grundlagen durch öffentliche Bekanntmachungen an den Pranger stellen.

Dass durch die Veröffentlichung im Amtsblatt der Gemeinde personenbezogene Daten im Sinne von § 3 Abs. 1 SächsDSG verarbeitet wurden, war evident. Es lag ein Verstoß gegen § 4 Abs. 1 SächsDSG vor. Die Veröffentlichung des Inhaltes des Zeitungsbeitrages durch die Stadt konnte auf keine gesetzliche Grundlage gestützt werden. Die Übermittlung war weder geeignet noch erforderlich zur Aufgabenerfüllung der Gemeinde. Die Veröffentlichung diente nämlich weder der Aufgabenbewältigung der Gemeindeverwaltung selbst, noch war sie von der Informationsbefugnis des § 11 Abs. 1 SächsGemO umfasst. Nach der Vorschrift des § 11 Abs. 1 SächsGemO sind Veröffentlichungen wegen § 2 SächsGemO lediglich im Rahmen des gemeindlichen Wirkungskreises zulässig. Veröffentlichungen im Amtsblatt haben sich an Art. 28 Abs. 2 GG, § 11 Abs. 1 i. V. m. § 2 SächsGemO zu orientieren. Sie finden ihre Grenze an den gemeindlichen Aufgaben und den Grundrechten Dritter. Die kommunalrechtliche Vorschrift besagt, dass die Gemeinde die Einwohner fortlaufend über die allgemein bedeutsamen Angelegenheiten ihres Wirkungskreises zu informieren hat. Die Angelegenheit zählte nicht dazu. Die Pflicht zur Unterrichtung der Öffentlichkeit in der Gemeinde bezieht sich lediglich auf originäre Aufgaben der Gemeinde und auf Aufgaben des übertragenen Wirkungskreises, mithin auf Weisungsaufgaben. Demgegenüber sind Ausführungen zum Lebensweg des Betroffenen, der nicht Einwohner ist, in einem Zeitungsartikel keine Angelegenheit der Gemeinde und es gehört auch regelmäßig nicht zu den Aufgaben einer Gemeinde über den Werdegang einzelner Straftäter bzw. über Vorgänge der Justiz zu berichten oder die Rolle des Landesamtes für Verfassungsschutz zu bewerten. Auch der Hinweis auf die angeblichen kriminal- bzw. gewaltpräventiven Aufgaben der Gemeinde lag, zumindest was den personenbezogenen Inhalt des Artikels

angeht, daneben. Veröffentlichungen mit einem allgemeineren und übergreifenden Bezug im Rahmen des gesetzlich Zulässigen vorzunehmen, ist das Privileg der nichtamtlichen Presse. Personenbezogene Informationen über Angelegenheiten außerhalb ihrer Zuständigkeit zu geben, ist für die Gemeinde nicht nur nicht erforderlich, sondern auch unzulässig.

Unerheblich war auch, ob die Gemeinde den Artikel selbst verfasst hatte. Im vorliegenden Fall stellt sich wegen des hinweisgebenden Nachsatzes der Gemeindeverwaltung zur angeblichen Ausweitung des „Tätigkeitsfelds“ des Betroffenen die Frage, ob die Gemeinde sich inhaltlich die in dem Zeitungsartikel gemachten Tatsachenbehauptungen und Meinungen zu Eigen machte. Der entsprechende Hinweis der Stadtverwaltung verstärkte jedenfalls den Eindruck und die Prangerwirkung, denn er drückte aus, dass die Gemeinde als öffentliche Stelle das Handeln und die Person des Betroffenen missbilligte. Die Gemeinde trug für den Nachdruck die alleinige Verantwortung, da ihr die Entscheidung oblag, ob der Beitrag veröffentlicht wurde oder nicht.

Im Ergebnis erfolgte die Veröffentlichung durch die Gemeinde ohne Rechtsgrundlage, da sowohl das Sächsische Datenschutzgesetz als auch andere Rechtsvorschriften die Datenverarbeitung nicht zuließen, und sie war damit rechtswidrig.

Die Namensnennung des Betroffenen im Amtsblatt war Ausdruck fehlender Einsicht in die Grenzen zulässigen Handelns öffentlicher Stellen. Bei der Namensnennung eines Betroffenen ist das Recht auf Anonymität als Ausfluss des allgemeinen Persönlichkeitsrechts stets zu beachten. Am Persönlichkeitsschutz orientiert, hat selbst die Presse bei der Abwägung, ob eine Namensnennung in einer Veröffentlichung erfolgen kann, auf die Bedeutung der Straftat und auf die Aktualität abzuheben. Eine Aktualität war bei einem Haftantritt im Jahre 2001 und einer relativ kurzen Haftzeit nicht erkennbar. Die Rechtsprechung erkennt eine Zulässigkeit der Nennung von Vor- und Zunamen in den nichtamtlichen Veröffentlichungen nur in Ausnahmefällen an. Das Resozialisierungsinteresse des Betroffenen ist nach Entscheidungen des Bundesverfassungsgerichts ein „genuin persönlichkeitsrelevantes Anliegen von hohem Rang“, das selbst dann zu beachten ist, wenn der Täter keine oder nur eine sehr kurze Freiheitsstrafe verbüßt hat (vgl. 1 BVR 755/98, Beschluss vom 25. November 1999). Zwar haben Straftäter nach der verfassungsgerichtlichen Rechtsprechung keinen Anspruch darauf, nach Verbüßung der Strafe mit ihrer Tat in jeglicher Weise „alleine gelassen“ zu werden und sie müssen eine gewisse Berichterstattung mit wahren Tatsachen dulden. Anders liegt der Fall aber dann, wenn eine identifizierende Berichterstattung erfolgt, hier sogar mit Namensnennung und Herkunftsort des Betroffenen. Hierdurch erleidet der Betroffene einen tiefgehenden Eingriff in sein Persönlichkeitsrecht.

Ich forderte die Gemeinde zur Stellungnahme auf und bat darum, zugängliche Exemplare der Amtsblattausgabe mit dem Zeitungsbeitrag zu sperren und des Weiteren organisatorische und personelle Maßnahmen zu veranlassen, dass sichergestellt ist, dass zukünftig durch Amtsblattveröffentlichungen nicht unzulässig in die Persönlichkeitsrechte Dritter eingegriffen wird. Die Gemeinde ist meinen Hinweisen und Empfehlungen gefolgt.

5.5.5 Datenabgleich durch Behörden nach dem Postgesetz

Mir ist die Frage gestellt worden, ob Gemeindebehörden - in einem Fall ging es um die Finanzkasse einer Großstadt in einem anderen Fall um das Einwohnermeldeamt einer Großstadt - gesetzlich befugt sind, ihre Anschriftendaten mit denen von Adressunternehmen abzugleichen. Konkret ging es um die von einem Postdienstunternehmen gespeicherten Umzugs- und Anschriftendaten. Nach § 40 PostG haben Unternehmen und Personen, die geschäftsmäßig Postdienste erbringen oder an der Erbringung solcher Dienste mitwirken, Behörden auf deren Verlangen die zustellfähige Anschrift eines am Postverkehr Beteiligten mitzuteilen, soweit dies für Zwecke behördlichen Postverkehrs erforderlich ist. Nach § 40 Satz 2 PostG gilt dies auch dann, wenn der Empfänger eine für die Übermittlung erforderliche Einwilligung nicht erteilt oder gegen die Übermittlung Widerspruch erhoben hat.

Bei meiner Beratung der Stellen habe ich deutlich gemacht, dass aufgrund der datenschutzrechtlichen Bestimmungen in Sachsen keine Bereinigung von Anschriftendateien bei dem Privatunternehmen erfolgen dürfe, da eine hierfür notwendige Übermittlung vom Sächsischen Datenschutzgesetz nicht gedeckt sei. Jedoch habe ich die auch nach dem Postgesetz zulässige Übermittlung an die Behörden bejaht. Einen weitergehenden Datenabgleich habe ich in der Weise noch für zulässig erachtet, dass die Abgleiche durch einen Datenverarbeitungsauftragnehmer der Stadt oder bei der Stadt selbst erfolgen, die die Umzugsdatenbank des Unternehmens nutzen. Voraussetzungen waren weiter die Einhaltung datenschutzorganisatorischer und Datensicherheitsmaßnahmen im Sinne von § 9 SächsDSG und die schon im Verfahren des Abgleichs unverzüglich vorzunehmende Löschung überschüssiger Daten aus dem Bestand der übermittelten Angaben.

Letztendlich war die Zweckbindung der Daten zu beachten. Die Daten durften nur zu Zwecken des Postverkehrs genutzt werden, damit z. B. beim Versand von Lohnsteuerkarten und ähnlichem Retoursendungen reduziert werden. Hingegen wäre z. B. ein Abgleich der Daten mit denen des Einwohnermeldeamtes, um festzustellen, welcher Bürger sich möglicherweise seiner Meldepflicht entzogen hat, um Ordnungswidrigkeitenverfahren nach dem Meldegesetz in Gang zu setzen, nicht zulässig gewesen.

Die diesbezüglich vorzunehmenden Vorkehrungen wurden von den Städten schon mit entsprechenden vertraglichen Regelungen mit dem Daten übermittelnden Unternehmen gesichert.

5.5.6 Personenbezogene Daten in Sitzungsvorlagen für den Gemeinderat

Ein betroffenes Gemeinderatsmitglied wandte sich mit der Frage an mich, ob die Gemeindeverwaltung berechtigt sei, dem Gemeinderat - wie geschehen - eine Aufstellung seines Grundeigentums zu unterbreiten. Ich antwortete wie folgt:

Die Übermittlung des aufgelisteten Grundstückseigentums an die Mitglieder des Stadtrats halte ich für unzulässig, soweit nicht besondere Gegebenheiten im Einzelfall vorliegen, die die privaten Angelegenheiten der ehrenamtlich tätigen Bürger in den Aufgabenbereich der Gemeinde rücken.

Zwar besteht gemäß § 28 Abs. 5 SächsGemO ein Fragerecht des einzelnen Ratsmitgliedes. Dabei haben sich die Fragen jedoch auf Angelegenheiten der Gemeinde zu beziehen. Die wirtschaftlichen Verhältnisse eines Ratsmitgliedes (wie sie durch dessen persönliches Eigentum zum Ausdruck kommen) zählen grundsätzlich nicht dazu. Allerdings steht außer Frage, dass Zusammenhänge entstehen können (bspw. Befangenheit, § 20 SächsGemO), die sich auf Angelegenheiten der Gemeinde auswirken, ja sogar mit diesen unauflösbar verknüpft sind.

Die gestellte Anfrage war mit nicht weiter substantiierten Befürchtungen des Fragestellers im Zusammenhang mit Nachteilen für die Gemeinde begründet und auf dieser Grundlage beantwortet worden. Es hätte daher auch ausgereicht, dass dem Gemeinderat - bei Anlass auch nach eventueller Rückfrage bei dem Betroffenen - mitgeteilt wird, dass die geäußerten Befürchtungen nicht begründet sind. Die Übermittlung der Grundeigentumsliste war jedenfalls nicht erforderlich (§ 11 Abs. 1 SächsDSG a. F., der § 12 Abs. 1 SächsDSG n. F. entspricht). Im vorliegenden Fall hätte die Übermittlung der einzelnen Grundstücksdaten an den Gemeinderat daher unterbleiben müssen. Sie war rechtswidrig.

5.5.7 Datenverarbeitung durch einen externen Berater der Landeshauptstadt

Im April 2003 wurde der Sächsische Datenschutzbeauftragte zum ersten Mal auf die Tätigkeit eines externen Beraters des Oberbürgermeisters der Stadt Dresden aufmerksam gemacht. Zu diesem Zeitpunkt war dieser Berater ohne einen schriftlichen Vertrag, ein alter Beratungsvertrag zum Ende des Jahres 2002 war ausgelaufen. Dennoch war der Privatmann weiterhin, angeblich unentgeltlich, im Rathaus tätig. Hierfür standen ihm ein geräumiges Büro und ein Vorzimmer samt einer städtischen Angestellten als

Sekretärin zur Verfügung. Dass es sich um einen externen Berater handelte, war der Raumbeschilderung nicht zu entnehmen. Er selbst nannte die Koordination größerer Investitionsvorhaben und die Vertretung des Oberbürgermeisters bei diesen Vorhaben als seine Aufgaben. Da die Funktion des Beraters wegen des Aufgabenbereichs nicht als Tätigkeit von untergeordneter Bedeutung zu betrachten war und er spätestens seit Beginn des Jahres 2003 ohne besondere Einschränkungen personenbezogene Informationen von städtischen Mitarbeitern sowie von anderen natürlichen Personen verarbeiten konnte, forderte der Sächsische Datenschutzbeauftragte die Stadt auf, die vertraglich ungeregelte Tätigkeit des Beraters aus datenschutzorganisatorischen Gründen zu beenden. Nachdem die Beendigung zwischenzeitlich sogar durch den Oberbürgermeister bestätigt worden war, erhielt der Sächsische Datenschutzbeauftragte Ende April 2003 davon Kenntnis, dass der Berater nunmehr einen befristeten Vertrag erhalten hatte und ihm die Aufgabe der Flutschadenbeseitigung bei der Stadt Dresden übertragen worden sei. Der Berater sei auf Grundlage eines bis Juni 2005 befristeten Auftragsverhältnisses tätig. Das eingerichtete Büro für Hochwasserschadensabwicklung des Oberbürgermeisters der Landeshauptstadt Dresden, dem der Berater vorstehen sollte, wurde mit zwei Sachbearbeitern und einer Bürokraft geführt. Der Berater sollte ausweislich seines Vertrags mit der Stadt Dresden „direkte Zuarbeit zum Oberbürgermeister“ leisten. Gegenüber dem Oberbürgermeister machte mein Vorgänger daraufhin erneut deutlich, dass eine Rechtsberatungstätigkeit des Beraters wegen dessen fehlender beruflicher Voraussetzungen nicht fortgesetzt werden könne. Darüber hinaus bestehe seit 1. Januar 2003 kein klares Vertragsverhältnis zwischen der Stadt Dresden und dem Berater. Dieser verfüge damit nicht über eine ordnungsgemäße Einbindung in die Hierarchie der Stadtverwaltung. Der Berater verarbeite dennoch personenbezogene Daten, er erhalte Vorzugsinformationen in Bezug auf Ausschreibungsverfahren, nehme Informationen über Mitarbeiter und deren Tätigkeit wahr, sammle Kenntnisse über die Verhältnisse Dritter, sowohl verwaltungsexterner Personen, als auch großer und kleiner Unternehmen (Geschäftsgeheimnisse).

Im Mai 2003 erhielt der Sächsische Datenschutzbeauftragte ein Schreiben des Oberbürgermeisters, dem Verpflichtungserklärungen des Beraters nach § 1 VerpflichtungsG und § 6 SächsDSG beigefügt waren und ein weiteres Schreiben, in dem mitgeteilt wurde, dass der Berater mit seinem neuen Vertrag eine Tätigkeit als „Projektkoordinator zum Gesamtprojektsteuerer und zum Freistaat Sachsen“ ausübe. Er kümmere sich um die Flutfolgen. Der Berater arbeite als „Projektkoordinator“. Eine solche Tätigkeit sei, so die Stadt unter Hinweis auf § 11 BDSG, § 7 SächsDSG (Auftragsdatenverarbeitung) und § 1 des Gesetzes über die förmliche Verpflichtung nichtbeamteter Personen, im Auftragsverhältnis zulässig.

Im Juni 2003 kontrollierten Mitarbeiter der Behörde des Sächsischen Datenschutzbeauftragten das Büro des Beraters und dessen Vorzimmerbereich stichprobenweise. Der Berater hatte u. a. Zugriff auf sieben Aktenbände, in denen personenbezogene Daten mit zum Teil sensiblen personalaktenrelevanten Inhalten gespeichert waren. In seinem Büro verwahrte er darüber hinaus mehrere Schriftstücke im Original oder in Kopie, die z. T. als vertraulich klassifiziert worden waren. Der Berater hatte u. a. Zugriff auf Geschäftsunterlagen des 1. FC Dynamo Dresden, Leistungsangebote von Anbietern, Haushalts-, Controlling- und Geschäftsunterlagen privater und städtischer Unternehmen, Bewerbungsunterlagen. Mit seinem von der Stadt zur Verfügung gestellten Personal Computer hatte der Berater Zugriff auf weitere vielfältige personenbezogene Daten, unter anderem auf von anderen Mitarbeitern erstellte Dateien, unter diesen auch Personalverwaltungsangelegenheiten sowie Dateien aus der Zeit des ehemaligen Oberbürgermeisters. Mithin handelte es sich auch um Unterlagen, die in starkem Maße geeignet waren, die Persönlichkeitsrechte Betroffener zu berühren. Zahlreiche Dateien und Akten standen damit auch nicht im Zusammenhang mit der vorgegebenen Tätigkeit des Beraters bei der Flutfolgenbewältigung. Auch die Vertragsunterlagen, die sich beim Oberbürgermeister persönlich unter Verschluss befanden, konnten die Mitarbeiter des Sächsischen Datenschutzbeauftragten einsehen. Andere Mitarbeiter und zuständige Dezernenten hatten auf diese Vertragsunterlagen keinen Zugriff und keine Kenntnis von deren Existenz und Inhalt. Eine Organisationsverfügung zur Einbindung, zur Aufgabe und zu den Befugnissen des Beraters existierte in der Stadtverwaltung nicht.

Der Vertrag sah eine vollständige örtliche und zeitliche Ungebundenheit des Auftragnehmers bei einem festgelegten Pauschalhonorar vor. Darüber hinaus enthielt er das Recht des Beraters, ein Dienstzimmer und einen Arbeitsplatz entgeltfrei zu nutzen. Mein Vorgänger wies darauf hin, dass die Vertragsleistungen des Beraters weder verständlich noch klar begrenzt seien und das Vertragsziel unklar bleibe, sowie dass der Berater wegen zwingender datenschutzrechtlicher Erfordernisse in der Verwaltung angestellt werden müsse oder als Auftragnehmer einzelne konkrete Aufgaben erledigen dürfe. Der Oberbürgermeister sagte eine diesbezügliche Prüfung zu. Als dem Sächsischen Datenschutzbeauftragten nach einem Gespräch im Oktober erneut ein datenschutzorganisatorisch unzureichender Vertragsentwurf übermittelt worden war und ihm, nachdem er erneut das Gespräch gesucht hatte, erstmals mitgeteilt wurde, dass der Berater eine „klassische“ Projektsteuerungstätigkeit für die Stadt Dresden nach Honorarordnung für Architekten und Ingenieure durchführe, obwohl bereits eine größere Firma für Projektsteuerungsleistungen beauftragt worden war, und erneut vortrug, dass es sich rechtlich um Auftragsdatenverarbeitung handele, beanstandete er die Stadt Dresden.

Es handelte sich das erste Mal um eine Beanstandung aus datenschutzorganisatorischen Gründen. Hierfür war ausschlaggebend, dass der Berater wie ein Verwaltungsangestellter in der Verwaltungsspitze der Stadt Dresden arbeitete, aber nicht in deren Hierarchie integriert war. Es wurde praktisch eine nicht abgegrenzte Vertreterposition des Oberbürgermeisters geschaffen, ein Nebenregime. Eine greifbare datenschutzrechtliche Verantwortlichkeit des Beraters in arbeitsrechtlicher oder dienstrechtlicher Weise war nicht ersichtlich.

Seit Beginn des Jahres 2003 hatte der Berater im Rahmen der Flutbewältigung und bei der Wahrnehmung anderer vielfältiger Aufgaben personenbezogene Daten verarbeitet. Die Datenverarbeitung im Zeitraum bis zum 21. April 2003 erfolgte ohne rechtliche und erkennbare vertragliche Grundlage und war schon deshalb ersichtlich rechtswidrig. Eine Rechtsvorschrift, die die Datenverarbeitung zulässt, bestand nicht. Die Datenverarbeitung war auch nicht erforderlich gewesen. Es handelte sich daher um einen Verstoß gegen §§ 4 Abs. 1, 15 Abs. 1 SächsDSG a. F.

Auch die Verarbeitung personenbezogener Daten durch den Berater ab April 2003, mit dem neuen Vertrag, war rechtswidrig gewesen. Grundrechtseingriffe - dazu gehört jede Verarbeitung personenbezogener Daten durch öffentliche Stellen - können nur durch eine öffentliche Stelle und nur auf gesetzlicher Grundlage erfolgen, § 4 Abs. 1 SächsDSG.

Auch die Überlegungen der Stadt in Bezug auf eine Auftragsdatenverarbeitung gingen fehl. Die Datenverarbeitung im Auftrag beschränkt sich auf Hilfstätigkeiten, also den (eben nicht selbständigen) Umgang mit personenbezogenen Informationen. Es handelte sich um eine Funktionsübertragung.

Selbstverständlich sind auch Beratungsverträge zulässig, hingegen kann dies nicht auf eine pauschale Funktionsübertragung hinauslaufen, die die umfassende Wirkung eines Anstellungsverhältnisses hat, ohne jedoch die Weisungs- und Kontrollmechanismen herzustellen, die bei einer Einordnung in die Verwaltungshierarchie gewährleistet sind und sein müssen. Das Datenschutzrecht begrenzt eine erlaubte Aufgabenübertragung auf einzelne, konkret begrenzte Leistungsgegenstände, auch bestimmter Abschnitte intern-vorbereitenden Verwaltungshandelns, so z. B. bei Sachverständigen oder Firmen, die Organisationsuntersuchungen durchführen. Nicht zulässig ist, dass die Verwaltung sich im Kerngeschäft, nämlich der Steuerung von Gesamtaufgaben „privatisiert“ und damit Verantwortlichkeiten und die Genese wesentlicher Entscheidungen aus der Verwaltungsverantwortung herauslöst. Das führt zum Entzug von Zuständigkeiten bei den dazu berufenen Funktionsträgern, zu Parallelverantwortlichkeiten und damit zu einer Gefährdung des ordnungsgemäßen Ablaufs der Datenverarbeitung. Diese Desorga-

nisation widerspricht dem Verfassungsgebot der Transparenz der Verarbeitungsvorgänge. Hier lag ein Verstoß gegen § 9 Abs. 2 Nr. 6 SächsDSG vor.

Weder hatte der Berater einen klar umrissenen und abgegrenzten Auftrag erhalten - der bloße Hinweis auf eine Projektsteuertätigkeit reichte nicht aus, die vertragliche Klarheit herbeizuführen-, noch war seine Datenverarbeitung auf ein eng umrissenes Feld beschränkt gewesen, noch war er in die Hierarchie der Stadt eingeordnet. Auch „Freie Mitarbeiter“ sind der öffentlichen Verwaltung fremd. Bei Auftragsverhältnissen ist aus datenschutzrechtlichen Gründen eine Konkretisierung des einzelnen Auftrags erforderlich. Die Aufgaben des externen Beraters waren wegen der Unklarheit im Vertrag nicht gegenüber den übrigen Mitarbeitern abgrenzbar. So blieb offen, wie weit die Befugnisse und Aufgaben des externen Beraters gingen. Die Bediensteten der Stadt wussten nicht, was sie dem Berater des Oberbürgermeisters mitteilen durften bzw. wo ihre amtliche Schweigepflicht dem Externen gegenüber begann oder endete.

Die Stadt Dresden wurde nach § 29 Abs. 1 SächsDSG aufgefordert, die Verarbeitung personenbezogener Daten durch den externen Berater unverzüglich vollständig einzustellen, sowie die Beanstandung dem Stadtrat vorzulegen. Dies geschah nicht. Die Kommunalaufsichtsbehörde wurde dem Gesetz entsprechend von der Beanstandung unterrichtet. Das zuständige Regierungspräsidium wirkte nicht anordnend ein, um der Tätigkeit des Beraters ein Ende zu bereiten. Die Zusammenarbeit der Stadt Dresden mit dem Berater wurde erst, nachdem dieser wegen eines Untreuevorwurfs verhaftet worden war und in Untersuchungshaft genommen wurde, beendet.

5.5.8 Wortprotokollierung auf einer Ausschusssitzung einer Gemeinde

Von einem Betroffenen erhielt ich Kenntnis von einer Tonbandaufzeichnung und einer anschließenden vollständigen Wortprotokollierung von Teilen einer Ausschusssitzung einer Gemeinde. Dass zu Protokollzwecken eine Tonaufzeichnung erfolgte, war bekannt. Die vollständige Protokollierung erfolgte jedoch ohne Kenntnis und Einwilligung der Betroffenen. Nach der Ausschusssitzung wurde ein offizielles Protokoll ohne wörtliche Wiedergabe von Wortbeiträgen für die darauffolgende Sitzung vorbereitet. Das Wortprotokoll selbst verwahrte der Bürgermeister bei sich.

Nicht nur Bürger, sondern auch Stadträte (als Inhaber öffentlicher Ämter) sind als Grundrechtsträger im datenschutzrechtlichen Sinne und als Betroffene einzuordnen. Der Mitschnitt von Wortbeiträgen auf Ausschusssitzungen, um sie vollständig textlich wiedergeben zu können, ist eine Verarbeitung personenbezogener Daten im Sinne von § 3 Abs. 1 SächsDSG, da Wortmeldungen auch Angaben zu sachlichen und persönlichen Verhältnissen natürlicher Personen beinhalten. Die Aufzeichnung von Sitzungen

zur Erstellung von Protokollen ist durchaus üblich. Die Verarbeitung personenbezogener Daten hat aber transparent zu erfolgen.

Das Verfahren in der erfolgten Weise ließ sich nicht mit datenschutzrechtlichen und den gemeinde- und ortsrechtlichen Bestimmungen rechtfertigen. Die Datenverarbeitung in der durchgeführten Weise ging zumindest, was die weitere Nutzung der Tonbandaufnahme angeht - über das Erforderliche im Sinne von § 13 Abs. 1 Nr. 1 SächsDSG hinaus. Insbesondere fand die weitergehende Nutzung des Wortprotokolls ohne Wissen und Kenntnis der Betroffenen statt, was nach allgemeinen Geschäftsordnungsregeln als ungewöhnlich zu betrachten war. Betroffene sind grundsätzlich über den Inhalt, Umfang und Tiefe der vorgesehenen Datenverarbeitung zu informieren. Damit entsprach das Verfahren auch nicht allgemeinen Geschäftsordnungsregeln, denn selbstverständlich ist es ein erheblicher Unterschied, ob eine wörtliche Rede in einer Niederschrift festgehalten werden soll oder ob lediglich eine Wiedergabe von Redebeiträgen erfolgt. Dies ist auch gerade ein entscheidender qualitativer Unterschied in der Tiefe der Verarbeitung personenbezogener Daten. Dass vor diesem Hintergrund neben dem offiziellen Protokoll eine nur dem Bürgermeister und in seiner Umgebung vertrauten Personen bekannte und eine damit quasi geheime Niederschrift der wörtlichen Redebeiträge der Ausschusssitzung angefertigt wurde, war zur Aufgabenerfüllung des gemeindlichen Gremiums - so stellte es sich mir wegen des Hergangs dar - wohl auch nicht erforderlich gewesen.

Ich forderte die Gemeinde daher auf, die Wort-Niederschrift vollständig zu löschen (§ 20 SächsDSG) bzw. das Wortprotokoll nachträglich von den Betroffenen genehmigen und autorisieren zu lassen.

5.5.9 Öffentlichkeitsgrundsatz der Gemeinderatssitzungen

1. Behandlung von Grundstücksverkäufen gemäß § 37 SächsGemO

Der Ortsvorsteher einer Gemeinde wandte sich mit der Frage an mich, ob Einzelangaben bei Grundstücksverkäufen der öffentlichen Hand, die auf Beschlussvorlagen beruhen, in öffentlicher Gemeinderatssitzung beraten werden dürfen. Konkret ging es um die Höhe einer einzutragenden Grundschuld des Erwerbers.

Hierzu habe ich mich folgendermaßen geäußert. Nach § 37 SächsGemO gilt zunächst der Öffentlichkeitsgrundsatz der Sitzungen. Auch Grundstücksverkaufsangelegenheiten der Gemeinde sind grundsätzlich öffentlich zu erörtern. Von Interesse für die Öffentlichkeit sind sowohl der Kaufpreis als auch die wesentlichen Verkaufsmodalitäten, z. B. Bebauungs- und Nutzungsauflagen. Der Öffentlichkeitsgrundsatz trägt bei Leistungsaustauschverhältnissen dazu bei, dass das Handeln der Gemeinde nicht im Verborgenen

stattfindet und Vertragspartner der Gemeinde als öffentlicher, der Wirtschaftlichkeit und der kommunalen Gemeinschaft verpflichteter Stelle nicht eine ungerechtfertigte Vorzugsbehandlung erfahren. Von der Interessenlage her können Verkäufe der Gemeinde daher letztendlich nicht anders behandelt werden als Ausschreibungen bzw. die Vergabe von Aufträgen der Gemeinde. Und diese sind ebenfalls, was die wesentlichen Vertragsbestandteile (Vergabesumme bzw. Auftragswert, Name der Firma oder des erfolgreichen Bieters) angeht, öffentlich.

Die Gemeinde hat aber bereits darauf zu achten, dass keine über die erforderlichen Daten hinausgehende personenbezogene Daten, z. B. Namen und Anschriften der Grundstückskaufparteien, in die Beschlussvorlagen aufzunehmen sind. Die Grundstücksverkäufe können insofern auch zunächst samt der dazu gehörenden Kaufverträge ohne unmittelbaren Namensbezug in öffentlicher Sitzung des Gemeinderats verhandelt werden. Aus den Grundstücksangaben sollte dabei deutlich werden, um welche Grundstücke oder Sachen es im Einzelnen geht. Im Übrigen bin ich der Auffassung, dass das Transparenzgebot auch dann gewahrt bleibt, wenn die gewählten Repräsentanten der Gemeinde über die Angelegenheit in nichtöffentlicher Sitzung abstimmen und die Entscheidung sodann bekanntgemacht wird.

Das Grundrecht auf informationelle Selbstbestimmung des Einzelnen ist aber auch in nichtöffentlicher Sitzung zu wahren. Das bedeutet, dass auch die Stadt- und Gemeinderäte den Bedingungen des Sächsischen Datenschutzgesetzes unterliegen und nur die Daten zu ihrer Kenntnis gegeben werden dürfen, die zur Erfüllung der jeweils anstehenden Aufgaben erforderlich sind, § 13 Abs. 1 und 2 SächsDSG.

Ich bin der Auffassung, dass die Höhe einer Grundschuld nichts über die tatsächlichen Vermögensverhältnisse der Käufer aussagt. Die Grundschuld ist nach deutschem Sachenrecht das dingliche Recht, aus einem Grundstück die Zahlung eines bestimmten Geldbetrages zu fordern. Die abstrakte Belastung eines Grundstücks nach § 1191 BGB, die beinhaltet, dass an diejenigen eine Summe aus dem Grundstück zu zahlen ist, zu dessen Gunsten die Belastung erfolgte, ist aus meiner Sicht kein Gegenstand, der auf Grund des Öffentlichkeitsgrundsatzes in der Sächsischen Gemeindeordnung/Sächsischen Landkreisordnung in den kommunalen Vertretungskörperschaften Behandlung finden kann. Da das verkaufte Grundstück belastet wird und nicht der Käufer des Grundstücks, verbleibt die Grundschuld beim Grundstück, wenn der Eigentümer wechselt. Damit gehört die Verhandlung über die Gewährung einer Grundschuld und die Festlegung von deren Höhe, verbunden mit der Kenntnisnahme personenbezogener Daten des Käufers, im Regelfall nicht zu den Aufgaben der Gemeinderäte. Auch Gemeinderäte unterliegen den Regelungen des Sächsischen Datenschutzgesetzes, wo-

nach das Nutzen personenbezogener Daten nur zulässig ist, wenn es zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist, § 13 Abs. 1 und 2 SächsDSG.

Im vorliegenden Fall war auch darauf zu achten, dass personenbezogene Daten nicht schon im Vorfeld von Ratssitzungen durch die Versendung von Beschlussvorlagen oder auch Tagesordnungen in der Öffentlichkeit bekannt gemacht werden.

2. Abwesenheitsgründe von Ratsmitgliedern in Niederschriften

Eine Große Kreisstadt wandte sich mit der Frage an mich, wie die von Ratsmitgliedern angegebenen Abwesenheitsgründe in die Sitzungsniederschrift aufzunehmen seien. Mit der Frage, ob durch den Zugang der Öffentlichkeit das Grundrecht der Gemeinderäte auf informationelle Selbstbestimmung beeinträchtigt werden könnte, hatte ich mich bereits in einem zurückliegenden Tätigkeitsbericht befasst.

In 9/5.5.2 war meinerseits den Kommunalverwaltungen empfohlen worden, tatsächliche Abwesenheitsgründe zu verallgemeinern, um eine die Betroffenen zu tiefgehende Verarbeitung personenbezogener Daten zu vermeiden.

Grundsätzlich gilt jedoch, dass an Informationen über kommunale Mandatsträger ein berechtigtes Interesse der Öffentlichkeit besteht. Sie gelten insoweit als relative Personen der Zeitgeschichte. Sie sind Inhaber öffentlicher Ämter und Teil der Gemeindeverwaltung. Datenschutzrechtliche Fragestellungen in Bezug auf die Gemeinderäte sind stets vor diesem Hintergrund zu bewerten. Das Gesetz schränkt den Persönlichkeitsschutz der Gemeinderäte bzw. Kreisräte ein. Dass die Niederschrift über die Ratssitzung die Namen der abwesenden Gemeinderäte bzw. Kreisräte unter Angabe des Grundes der Abwesenheit zu enthalten hat (§ 40 Abs. Abs. 2 Satz 1 SächsGemO, § 36 Abs. 1 Satz 1 SächsLKrO), ist nicht weiter interpretationsfähig. Es sind daher tatsächliche Gründe der Abwesenheit anzugeben, die regelmäßig nicht durch bewertende und verallgemeinernde Angaben ersetzt werden können. Die Pflicht zur Angabe von Abwesenheiten entspricht der grundsätzlichen Teilnahmepflicht der Gemeinderäte an Sitzungen und hat ihren Grund auch in möglichen Ordnungsmaßnahmen im Falle der Nichtteilnahme. Insofern wird gesetzlich eine authentische Angabe der Abwesenheitsgründe gefordert.

Das Erteilen einer *Erlaubnis* zum Fernbleiben (etwa durch den Bürgermeister) sehen die Kommunalordnungen nicht vor. Sich „entschuldigt“ zu haben, ist daher kein *Grund* im Sinne der gesetzlichen Bestimmung. *Der vom Ratsmitglied angegebene Abwesenheitsgrund ist also zu vermerken*. Erfolgt ein angekündigtes Fernbleiben (zunächst) ohne Angabe von Gründen, kann dies in der Niederschrift wie folgt vermerkt werden: „abgemeldet ohne Angabe von Gründen“; das Nachreichen einer (rechtfertigenden) Begründung bleibt davon ebenfalls unberührt. Dem Ratsmitglied ist es auch aufgegeben, den

Grund seiner Abwesenheit vorab anzugeben bzw. rechtzeitig - i. d. R. bis zur Beschlussfassung über das Protokoll - nachzureichen.

Hinsichtlich der Abwesenheit und der Begründung ist ein Glaubhaftmachen i. d. R. ausreichend. Arbeits- oder beamtenrechtlichen Anforderungen muss nicht genügt werden. Die Einreichung von Arbeitsunfähigkeitsbescheinigungen oder gar ärztlichen Befunden kommt nicht in Betracht.

Als häufige Gründe, wie sie der gesetzlichen Anforderung zumeist genügen werden, kommen die nachstehenden Beispiele in Betracht:
- Urlaub;
- Arztbesuch / Krankheit / Entbindung / OP / Kur / Rehabilitationsmaßnahme;
- dienstliche / geschäftliche Verhinderung;
- familiäre Verpflichtungen / Ereignisse;
- Wahrnehmung eines öffentlichen Amtes / Auftrags.

Gesetzlich nicht weiter geregelt ist das *mündliche Verlautbaren* der Abwesenden und der Gründe ihrer Abwesenheit in der Ratssitzung. Die Feststellung der Beschlussfähigkeit könnte also durchaus auch summarisch erfolgen. Eine Verlegung dieser Prozedur in nichtöffentliche Sitzung wäre allerdings unzulässig, rechtfertigen nach § 37 Abs. 1 SächsGemO nur das öffentliche Wohl oder berechtigte Interessen Einzelner zum Ausschluss der Öffentlichkeit (vgl. Quecke/Schmid, Gemeindeordnung für den Freistaat Sachsen, Ktr. Rdnr. 516 ff.).

3. Personenbezogene Daten in Sitzungsvorlagen (§§ 36, 37 SächsGemO)

Aus Kommunen erreichen mich regelmäßig Anfragen zur *Sitzungsöffentlichkeit* des Hauptorgans. Starre Festlegungen, die alle Lebenssachverhalte berücksichtigen, kann es hierfür nicht geben. Die Rechtsanwendung erfolgt durch Einzelfallentscheidungen. Eine Beurteilung erfordert daher die Würdigung aller entscheidenden Sachverhaltsbestandteile. Bestenfalls lassen sich theoretische Auskünfte zu klar umrissenen Regelfallgruppen erteilen. Dabei ist jedoch zu berücksichtigen, dass schon geringgradige Abweichungen vom Regelfall zu entgegengesetzten Rechtsfolgen führen können.

Damit vom Öffentlichkeitsgrundsatz abgewichen werden kann, müssen jedoch gewichtige Gründe vorliegen. Inhaltlich entscheidend ist dabei die Überlegung, welche Informationen in welcher Detailtiefe zur gesetzlichen Aufgabenerfüllung erforderlich sind und den Gemeinderäten gem. § 36 Abs. 3 Satz 1 SächsGemO daher *vorab* auszuhändigen sind. Im Regelfall bildet dies die Voraussetzung dafür, dass eine formell rechtmäßige Stadtratsentscheidung überhaupt zustande kommen kann (Gern, Sächsisches Kommunalrecht (1994), Rdnr. 498). Wer den Stadträten entscheidungserhebliche Infor-

mationen oder den Hinweis auf deren Vorhandensein vorenthält, kann sich nicht darauf berufen, dass diese im Wege einer Anfrage gemäß § 28 Abs. 5 SächsGemO (jederzeit) mitgeteilt worden wären. Keine Vorabübersendung findet statt, soweit das *öffentliche Wohl* oder *berechtigte Interessen Einzelner* entgegenstehen. Damit diese Schutzvorschrift aus tatsächlichen Gründen überhaupt wirksam werden kann, sind potentiell „undichte Stellen“ zu reduzieren, d. h. die entscheidungserheblichen Informationen sind auf weniger gefährdete Weise (z. B. mittels Tischvorlage) kundzutun (ebd., Rdnr. 499).

Aufgrund der wortgleichen Voraussetzung für den Ausschluss der Öffentlichkeit (§ 37 Abs. 1 Satz 1 SächsGemO) kommt eine Einschränkung der Vorabübersendung *nur für nichtöffentlich zu beratende Gegenstände* in Betracht (Brüggen/Heckendorf Sächsische Gemeindeordnung, Komm. (1994), § 36). Mit anderen Worten: „Muss die Übersendung unterbleiben ..., so kann auch die Sitzung ... nur nichtöffentlich sein“ (Menke/Arens, Sächsische Gemeindeordnung, Komm. (2004), § 36 Rdnr. 7). Beratungsunterlagen für öffentliche Sitzungen sind *öffentlich zugängliche Unterlagen*; die Öffentlichkeit besitzt ein Einsichtsrecht (Quecke/Schmid (Menke), SächsGemO, Ktr. § 37 Rdnr. 14).

Wie zu verfahren ist, ist für jeden Beratungsgegenstand im Einzelfall zu prüfen (zu § 36: Gern, a. a. O, Rdnr. 498; Menke/Arens, a. a. O. § 36 Rdnr. 7; zu § 37: Quecke/Schmid (Menke), a. a. O., Rdnr. 16). Bestimmte Fallgruppen - etwa durch Geschäftsordnungsbestimmung - von vornherein einer nichtöffentlichen Beratung zuzuweisen, ist nach dem sächsischen Gemeinderecht unzulässig (Quecke/Schmid (Menke), a. a. O., Rdnr. 16).

Ausnahmen vom Grundsatz der Öffentlichkeit hat der Gesetzgeber von der Gefährdung des *öffentlichen Wohls* bzw. vom Vorliegen *berechtigter Interessen Einzelner*, mithin von Gründen erheblicher Bedeutung abhängig gemacht (Hinweise liefern bspw. Menke, Die Handhabung des Öffentlichkeitsgrundsatzes in den Gemeinderatssitzungen, in: Sachsenlandkurier 10/2002, S. 470 (472); Quecke/Schmid (Menke), a. a. O., § 37, Rdnr. 19 f.). Ihrer rechtsdogmatischen Natur nach handelt es sich dabei um *unbestimmte Rechtsbegriffe* (die keine Ermächtigung zum Ermessensgebrauch darstellen). In Zweifelsfragen sollten die Kommunalaufsichtsbehörden und meine Behörde mit der Bitte um Stellungnahme gefragt werden.

4. Internetveröffentlichung von Niederschriften der Sitzungen eines Ortschaftsrats

Aufgrund einer Anfrage eines Ortschaftsrates stieß ich auf dessen amtliche Sitzungsniederschriften im Internet. Zu der Frage der Zulässigkeit habe ich mich wie nachstehend geäußert.

Bei Ortschaftsräten sind die Bestimmungen für Gemeinderäte anzuwenden, § 69 Abs. 1 Satz 1 SächsGemO. Die amtlichen Sitzungsniederschriften sind nach § 40 Abs. 2 Satz 5 SächsGemO nur den Einwohnern zugänglich zu machen. Eine Veröffentlichung amtlicher Niederschriften im Internet, die damit weltweit veröffentlicht werden, findet daher keine gesetzliche Stütze. Zwar sind die Gemeinderatssitzungen öffentlich und für die Allgemeinheit zugänglich, jedoch werden auch auf den öffentlichen Sitzungen bzw. in den sie zusammenfassenden Niederschriften personenbezogene Daten verarbeitet. Insofern bleibt die gesetzliche Beschränkung bei der Veröffentlichung amtlicher Niederschriften aus Datenschutzsicht zu beachten.

Sofern jedoch interessierte Einwohner Mitschriften anfertigen oder anhand ihrer Erinnerung den Hergang der Sitzungen darstellen und im Internet veröffentlichen, ist dies aufgrund der Meinungsäußerungsfreiheit zulässig.

5.6 Baurecht; Wohnungswesen

5.6.1 Anerkennungsverfahren für Sachverständige nach der Sächsischen Bauordnung

Die zeitgleich mit der novellierten Sächsischen Bauordnung vom 28. Mai 2004 am 1. Oktober 2004 in Kraft getretene Verordnung des SMI zur Durchführung der Sächsischen Bauordnung (DVOSächsBO), die mir im Rahmen des Anhörungsverfahrens nach § 26 SächsDSG zur Stellungnahme vorgelegt worden war, ist aufgrund einer von mir behandelten datenschutzrechtlichen Fragestellung modifiziert worden.

Zur Nachweisführung über die Erfüllung der besonderen Voraussetzungen im Anerkennungsverfahren zum Prüfingenieur wurden in der alten Fassung der Durchführungsverordnung (SächsBO-DurchführVO) konkrete Angaben, darunter personenbezogene Daten aus den durch die Bewerber zu erbringenden Tätigkeitsbelege erhoben und verarbeitet (vgl. § 24 Abs. 2 Nr. 3 a SächsBO-DurchführVO). Die neue Durchführungsverordnung verzichtet in ihrem § 19 Abs. 2 Nr. 6 DVOSächsBO auf konkrete Angaben über die Nachweisführung zur Erfüllung der besonderen Voraussetzungen im Anerkennungsverfahren als Prüfingenieur.

Aufgrund einer Anfrage eines Prüflings, eines ehemals bei einer unteren Bauaufsichtsbehörde Beschäftigten, erfuhr ich, dass die Übersendung von Angaben zu bearbeiteten Projekten mit dem Ziel der Nachweisführung hinsichtlich der besonderen Voraussetzungen im Anerkennungsverfahren (§ 19 Abs. 2 Nr. 6 DVOSächsBO) bei der unteren Bauaufsichtsbehörde auf datenschutzrechtliche Bedenken stieß. Diese datenschutzrechtlichen Bedenken beziehen sich insbesondere auf die Weitergabe der personenbezogenen Daten der Bauherren des angegebenen Referenzprojektes. Es muss jedoch davon ausge-

gangen werden, dass man bei Nachweisen über die Erfüllung der besonderen Voraussetzungen im Anerkennungsverfahren für Prüfingenieure z. B. auf personenbezogene Daten des Bauherrn eines Referenzobjektes nicht wird verzichten können. Ich habe deshalb mitgeteilt, dass ich diese Bedenken gegen eine derartige Datenübermittlung im Rahmen des Anerkennungsverfahrens nicht teile.

Wenn im Anerkennungsverfahren gemäß § 19 Abs. 2 Nr. 6 DVOSächsBO vom Antragsteller Nachweise mit personenbezogenen Daten verlangt werden, die er gegebenenfalls nur von einer Behörde erhalten kann, ist die Zulässigkeit der Datenverarbeitung nach § 4 Abs. 1 SächsDSG zu prüfen. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das Sächsische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt, oder soweit der Betroffene eingewilligt hat. Die Übermittlung personenbezogener Daten an natürliche Personen - wie im vorliegenden Fall - ist nach § 16 Abs. 1 Nr. 2 SächsDSG zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat. Der Betroffene ist vor der Übermittlung zu hören und im Falle der Übermittlung zu unterrichten (§ 16 Abs. 3 SächsDSG). Die übermittelnde Stelle hat den Empfänger auf die Zweckbindung der Daten hinzuweisen (§ 16 Abs. 4 SächsDSG). Da von einem berechtigten Interesse eines Antragstellers zur Zulassung als Prüfingenieur an der Übermittlung der erforderlichen Daten nach § 19 Abs. 2 Nr. 6 DVOSächsBO ausgegangen werden muss, ist eine Übermittlung dieser Daten an ihn durch die Behörde nach dem Sächsischen Datenschutzgesetz zulässig.

Darüber hinaus besteht die Möglichkeit, dass auf Hinweis des Antragstellers die oberste Bauaufsichtsbehörde, das SMI, selbst die entsprechenden Nachweise gemäß § 19 Abs. 2 Nr. 6 DVOSächsBO von der betreffenden unteren Bauaufsichtsbehörde anfordert (§ 19 Abs. 2 Satz 3). In diesem Fall richtet sich die Übermittlung personenbezogener Daten nach § 14 SächsDSG. Das SMI teilte mir auch dementsprechend mit, dass es, soweit es sich bei dem Antrag auf Anerkennung als Prüfingenieur um einen Mitarbeiter einer unteren Bauaufsichtsbehörde handeln sollte, die geforderten Nachweise selbst dort anfordern werde. Im konkreten Fall konnte das Prüfungsverfahren durch meine Mitwirkung abgeschlossen werden.

5.7 Statistikwesen

5.7.1 Das sog. Forschungsdatenzentrum der Statistischen Landesämter

Aufgrund von Empfehlungen einer vom Bundesministerium für Bildung und Forschung eingesetzten Kommission, den Zugang von Wissenschaftlern zu den bei der Durchführung von Bundesstatistiken anfallenden Einzeldatensätzen zu erleichtern, die bei den

statistischen Ämtern der Länder vorhanden sind, und überhaupt eine bessere Zusammenarbeit zwischen Amtlicher Statistik und Wissenschaftlern herbeizuführen, haben diese Ämter sich im Wege eines Verwaltungsabkommens auf verschiedene organisatorische Vorkehrungen und abgestimmte Verhaltensweisen geeinigt, deren Gesamtheit jeweils als „Forschungsdatenzentrum“ bezeichnet wird.

Erreicht werden soll damit Folgendes: Wissenschaftler sollen ortsnah, d. h. bei jedem der genannten statistischen Ämter, einen bundesweiten Zugang zu Einzelangaben (in der Fachsprache „Mikrodaten“ genannt) erhalten, und man will durch engere Zusammenarbeit zwischen amtlicher Statistik und Wissenschaftsbetrieb die Entwicklung statistischer Methoden fördern und außerdem bessere, insbesondere auf aktuelleren Daten beruhende Vorhersagen für die Politik zustandebringen; dabei könne die nötige Schnelligkeit, wie es heißt, nur bei Benutzung der Einzel-Datensätze der Länder-Ämter erreicht werden, und die Bearbeitung der Einzel-Datensätze durch die Länder müsse vereinheitlicht werden.

Zu diesem Zweck soll für die verschiedenen Statistik-Fachgebiete jeweils ein einzelnes Statistisches Landesamt bundesweit die Einzelangaben aus der gesamten Bundesstatistik zusammenführen und sie auf entsprechende Nachfrage, nach positiver Entscheidung aller beteiligten Landesämter, an Wissenschaftler übermitteln, was dann wiederum in jedem beliebigen der Landesämter geschehen können soll.

Diese sog. *fachlich zentralisierte Datenhaltung*, also die Zusammenführung und Aufbereitung der Einzeldatensätze („Einzelangaben“ im Sinne der üblichen statistikrechtlichen Terminologie, namentlich § 16 Abs. 1 BStatG) aller Landesämter („*Eignerämter*“) bei dem für die betreffende Fachstatistik aufgrund der Absprache zuständigen Landesamt (dem „fachlich federführenden *Serveramt*“ - Datenausgabestelle für den Wissenschaftler) wirft deswegen datenschutzrechtliche Fragen auf, weil die Statistischen Landesämter sich nicht veranlasst gesehen haben, den Aufwand zu treiben, die Einzelangaben nur *verschlüsselt* an das die Daten ausgebende Amt weiterzugeben, mit Entschlüsselungsmöglichkeiten nur für den Wissenschaftler; dann wäre ja, was das Datenempfängeramt betrifft, jeder Personenbezug vermieden gewesen.

Auch *mit* Personenbezug sollte diese *fachlich zentralisierte Datenhaltung* nach Auffassung der Statistikbehörden als Datenverarbeitung im Rahmen bloßer *Auftragsdatenverarbeitung* rechtmäßig sein, weil ja jede weitere Verarbeitung, insbesondere die Übermittlung an den Wissenschaftler, nur aufgrund „schriftlicher Weisung“ der betroffenen Eignerämter erfolgen soll, denen zudem vollständige automatisierte Protokollierungen solcher Verarbeitungen übermittelt werden sollen.

Diese Auffassung setzt voraus, dass für die in Frage stehende Verarbeitung personenbezogener Daten, nämlich statistischer Einzelangaben, der Rechtssatz gilt, dass eine nicht an die für die Datenübermittlung geltenden Vorraussetzungen gebundene Weitergabe an „Gehilfen“ bei der Statistik-Durchführung zulässig ist. Dieser Rechtssatz darf *kein ungeschriebener Rechtssatz sein.* Denn das widerspräche dem Verfassungsgrundsatz des *Vorbehaltes des Gesetzes* im Hinblick auf den Grundgedanken des Datenschutzrechtes, nämlich auf das Recht des Privaten, zu wissen, wer was in welchem Zusammenhang über ihn weiß, vor allem bei Betätigung der öffentlichen Gewalt. Denn auch der Auftragsdatenverarbeiter ‚hat’ ja die Daten, „weiß“ also etwas im Sinne dieser Formulierung.

Gegenstand der Tätigkeit des Forschungsdatenzentrums sind ausschließlich Bundesstatistiken. Die maßgeblichen Regelungen für die Verarbeitung von Daten im Rahmen der Durchführung solcher (Einzel-)Statistiken für Bundeszwecke sind ausschließlich (Art. 73 Nr. 11 GG) dem Bundesrecht, also in erster Linie dem allgemeinen Regelwerk für die Verfahrensweise bei der Durchführung von Bundesstatistiken zu entnehmen, das das Bundesstatistikgesetz enthält. Dieses weist bisher - im Unterschied zu den meisten Landesstatistikgesetzen, die jedoch insoweit eben nicht anwendbar sind - keine Vorschrift der gesuchten Art auf. (Eine analoge Anwendung der genannten Sondervorschriften, die die meisten Landesstatistikgesetze - nicht aber das sächsische - enthalten, wie sie Walz in Simitis u. a. 5. A., Rdnrn. 35 f. zu § 11 BDSG zu befürworten scheint, ist naturgemäß bei Grundrechtseingriffen ausgeschlossen!)

Zusätzlich habe ich geltend gemacht, dass das nach der Planung vom *Server*-Amt zu übernehmende S*peichern* und P*rüfen auf Vollständigkeit und formale Korrektheit* Bestandteil der eigentlichen, der Kern-Aufgaben der statistischen Ämter ist und daher eben gar nicht Datenverarbeitung im Auftrag sein kann - anders als bei gewöhnlicher Verwaltungsvollzugs-Tätigkeit, bei der Datenverarbeitungsvorgänge Hilfstätigkeit für die eigentliche Verwaltungstätigkeit, etwa den Erlass von Bescheiden, ist. Das bedeutet, dass für die Anwendung der Regeln über die Datenverarbeitung im Auftrag bei der Durchführung von Statistiken nur wenig Spielraum bleibt.

Diese meine Auffassung wird bestätigt dadurch, dass die allermeisten Landesstatistikgesetze eine Vorschrift enthalten, die die Übertragung einzelner Arbeiten bei der Durchführung amtlicher Statistiken auf Dritte erlauben: Diese Landesgesetzgeber haben in ihrem Wortlaut von den üblichen Auftragsdatenverarbeitungs-Vorschriften deutlich abweichende Regelungen geschaffen, sie mithin auch für notwendig gehalten. Zugleich drücken die in diesen Gesetzen verwendeten Formulierungen, wie hier nicht im Einzelnen dargelegt werden soll, deutlich aus, was tatsächlich stattfindet, wenn Phasen

der Durchführung einer Statistik Dritten übertragen werden: Funktionsübertragung, nicht bloße Datenverarbeitung im Auftrag.

Wie ebenfalls an dieser Stelle nicht näher ausgeführt werden soll, ergeben sich für die von mir vertretene Auffassung außerdem zusätzliche Argumente aus den begrenzten Übermittlungserlaubnissen in § 16 Abs. 3 Satz 2, § 16 Abs. 2 und § 16 Abs. 3 Satz 1 BStatG.

Aus alledem war zu folgern, dass die *fachlich zentralisierte Datenhaltung* schlicht und einfach gegen § 16 Abs. 1 Satz 1 BStatG, die Grundregel des Statistikgeheimnisses, verstößt, dass mit anderen Worten ein systematischer Bruch des Statistikgeheimnisses in der Form, wie es nun einmal für Bundesstatistiken geltendes Recht ist, stattfinden sollte - auch wenn eine abweichende Regelung, wie sie die erwähnten landesstatistikgesetzlichen Vorschriften enthalten, nicht verfassungsrechtlich unzulässig wäre.

Diese von mir vorgebrachte, bei Anwendung des geltenden Rechtes meines Erachtens unvermeidliche rechtliche Überlegung, hat das Statistische Landesamt des Freistaates nachvollziehen können. Andererseits war der eine oder andere meiner Kollegen in den anderen Bundesländern nicht meiner Ansicht. Auf eine Anerkennung der Rechtswidrigkeit der *fachlich zentralisierten Datenhaltung* haben sich die Landesdatenschutzbeauftragten nicht vollständig einigen können, eine Einigung sämtlicher Datenschutzbeauftragten auf eine zeitlich und sachlich begrenzte faktische Duldung für eine Erprobungszeit ist damit auch nicht zustande gekommen, sodass die Lage insoweit bis heute ungeklärt ist, zumal sich die Statistikbehörden nicht auf diese von Datenschützerseite ins Gespräch gebrachten Beschränkungen haben einlassen mögen.

Einige meiner Kollegen sind schon zufrieden gewesen, dass wir Datenschutzbeauftragten jedenfalls erreicht haben, dass die Statistischen Landesämter ihren in diesem Zusammenhang verfolgten Plan aufgegeben haben, pro forma - oder sagen wir es lieber deutsch: nur zum Schein - in den Ämtern angestellten Wissenschaftlern Daten zur Verfügung zu stellen, die ihnen als Forschern wegen mangelnden Anonymisierungsgrades nach dem Bundesstatistikgesetz gerade nicht hätten übermittelt werden dürfen.

Mein Widerstand gegen die Hinnahme der *fachlich zentralisierten Datenhaltung* war überdies auch darin begründet, dass sich bald abgezeichnet hat, dass für die Statistikbehörden der Länder, allen voran Bayerns, das Forschungsdatenzentrum der Statistischen Landesämter nur Vorläufer für ein Vorhaben war, welches den im Forschungsdatenzentrum der Länder liegenden Rechtsverstoß geradezu zum *System* erheben wollte bzw. will.

Angesichts dessen hat der Bundesgesetzgeber, unter besonderer Mitwirkung Bayerns, vorsichtshalber - und dies kann man sicher als einen Erfolg des von mir mit einigen Kollegen seit 2003 geleisteten Widerstandes ansehen - das Bundesstatistikgesetz nunmehr um eine Regelung ergänzt, die das Forschungsdatenzentrum zusammen mit einem weit über dieses hinausgehenden Umbau der Tätigkeit der Statistischen Landesämter legalisieren soll. Dazu nachstehend 5.7.2.

5.7.2 Durchführung von Bundesstatistiken durch ein statistisches Landesamt zugleich für alle anderen Bundesländer („ämterübergreifende Aufgabenerledigung“)

1. Zwecks Kosteneinsparung bei der Bundesstatistik haben sich die Statistikämter der Länder zusammen mit den für sie zuständigen Ministerien auf einen sogenannten *Masterplan zur Reform der amtlichen Statistik* geeinigt, dem zufolge etliche Abschnitte der Durchführung von Bundesstatistiken - einschließlich solcher Abschnitte und Statistiken, bei denen die verarbeiteten Daten (noch) Personenbezug haben - nach Fachgebieten verteilt von jeweils einem einzigen statistischen Amt für jeweils alle anderen Bundesländer übernommen werden sollen.

Bei diesem Versuch einer Umverteilung der Aufgaben und Befugnisse der statistischen Landesämter bei der Durchführung der Bundesstatistiken handelt es sich, wie auf der Hand liegt, um die Erhebung der im *Forschungsdatenzentrum der statistischen Landesämter* punktuell angestrebten Arbeitsteilung zum Grundprinzip der Bundesstatistik, die nunmehr, was die statistischen Landesämter betrifft, nach der Devise *Einer für alle* durchgeführt werden soll.

2. Gegenüber dem im August 2004 vorgelegten Entwurf einer dementsprechenden „Verwaltungsvereinbarung über eine ämterübergreifende Aufgabenerledigung in der amtlichen Statistik“ habe ich unter Anknüpfung an meine Stellungnahme zum Vorhaben *Forschungsdatenzentrum der statischen Ämter der Länder* (vorstehend 5.7.1) Folgendes geltend gemacht:

(1) Auftragsdatenverarbeitung bedarf wegen des obersten Grundsatzes des Datenschutzes, nämlich dass die Rechtsordnung zu gewährleisten hat, dass, zumindest im Hinblick auf die Betätigung öffentlicher Stellen, jeder wissen können muss, wer was in welchem Zusammenhang über ihn weiß (BVerfGE 65, 1, 43), einer rechtlichen Erlaubnis.

(2) Eine solche fehlt im Bundesstatistikgesetz. Dieses ist jedoch als Regelung für die Durchführung von Bundesstatistiken (durch die Länder) gemäß Art. 73 Nr. 11 GG im Verhältnis zu den Landesgesetzen die allein maßgebliche Vorschrift.

(3) Selbst wenn man das Fehlen einer Ermächtigung zur Einschaltung eines Auftragsdatenverarbeiters nicht als Negativ-Aussage des Bundesstatistikgesetzes zu interpretieren hätte, sondern annehmen dürfte, das Gesetz lasse insoweit Raum für eine Ergänzung durch landesrechtliche Vorschriften, die auf Art. 84 GG gestützt wären (eine sehr unsichere Abgrenzung, vgl. Hermes in: Dreier, Hrsg., GG-Kommentar, Rdnrn. 27 f. zu Art. 84), gälte Folgendes:

(3.1) Das Sächsische Statistikgesetz enthält im Unterschied zu den meisten anderen Landesstatistikgesetzen keine Erlaubnis irgendeiner Aufgabenübertragung auf Dritte. (In derselben Lage sind zumindest Schleswig-Holstein und Berlin.) Daher folgt schon aus § 3 Abs. 2 Nr. 1 i. V. m. § 2 Abs. 1 Nr. 1 und 2 SächsStatG, dass EG- und Bundesstatistiken in Sachsen ausschließlich vom Statistischen Landesamt des Freistaates durchzuführen sind, also namentlich die Arbeiten des Erhebens, Sammelns und Aufbereitens (§ 1 Abs. 1 Satz 1 SächsStatG).

Im Hinblick auf Art. 83 Abs. 1 SächsVerf ist das als vollständige Zuständigkeitsfestlegung auszulegen: Genau das Statistische Landesamt ist insoweit zuständig, niemand anderes. Eine Verlagerung der Zuständigkeit, wie sie ausnahmsweise in § 4 Abs. 1 Satz 1 SächsStatG erlaubt wird, ist insoweit nicht vorgesehen.

(3.2) Eine Prüfung des Vorhabens im Hinblick auf die in den meisten Landesstatistikgesetzen - meist mit Beschränkungen - enthaltenen Aufgabenübertragungserlaubnisse wäre für jedes einzelne der betreffenden Länder durchzuführen. Als Grundlage für die geplante Verwaltungsvereinbarung reichte das schon deswegen nicht aus, weil ja alle Länder einbezogen werden sollen.

(4) Für eine ergänzende Anwendung des Bundesdatenschutzgesetzes, namentlich dessen § 11, ist kein Raum. Es handelt sich um eine Materie, die durch Landesgesetze geregelt ist, so dass die Voraussetzungen des § 1 Abs. 2 Nr. 2 BDSG nicht erfüllt sind.

(5) Die auf welche diesbezügliche (ungenannt gebliebene!) Erlaubnisnorm auch immer bezogene Vorstellung der geplanten Verwaltungsvereinbarung, bei dem Vorhaben handele es sich, soweit das Grundrecht auf informationelle Selbstbestimmung bzw. das Statistikgeheimnis betroffen ist, um *Auftragsdatenverarbeitung* (im üblichen Sinne des Datenschutzrechtes), ist unzutreffend. Denn:

(5.1) Die geplante Erledigung von Aufgaben der Durchführung der amtlichen Bundesstatistik durch ein fremdes Landesamt, genauer gesagt das geplante Speichern und *Bearbeiten* (Verändern und Nutzen), also *Aufbereiten* im Sinne der statistikrechtlichen Terminologie, mithin das Plausibilisieren durch
- Prüfen der Vollständigkeit,

- Prüfen der (sonstigen) formellen Korrektheit,
- sonstiges Prüfen der Plausibilität,
- Plausibilisieren durch *Nachfragen beim Auskunftspflichtigen* (Erläuterung zu § 3 Abs. 2 des Entwurfes) und entsprechende Datenveränderung (Erläuterung zu § 3 Abs. 2)

ist Bestandteil der eigentlichen, der Kern-Aufgaben der statistischen Ämter und daher eben *keine Datenverarbeitung im Auftrag* - anders als bei gewöhnlicher Verwaltungsvollzugs-Tätigkeit, bei der Datenverarbeitungsvorgänge Hilfstätigkeit für die eigentliche Verwaltungstätigkeit, nämlich die konkrete Gestaltung der Wirklichkeit durch Verwaltungsakte, ergänzend auch durch Realakte, ist.

Hinter dieser Datenverarbeitungs-Tätigkeit bei der Durchführung der amtlichen Statistiken steht keine weitere konkrete Verwaltungstätigkeit, der sie dient. Die Verarbeitung der Daten ist hier Selbst-Zweck, der eigentliche Zweck der staatlichen Tätigkeit. (Ähnlich: Archivbehörden, Registerbehörden, Verfassungsschutz bzw. Nachrichtendienste.) Der Erlass von Bescheiden, der auch der Tätigkeit der Statistikbehörden nicht fremd ist, dient hier gerade dazu, personenbezogene Daten erst zu bekommen, und er dient ausschließlich dazu, Daten zu bekommen. Dagegen hat bei gewöhnlicher Verwaltungsvollzugs-Tätigkeit umgekehrt die Erhebung und Weiterverarbeitung personenbezogener Daten gerade den Zweck, seitens der Behörde die richtigen konkreten Maßnahmen gegenüber Einzelnen treffen zu können.

(5.2) Die zur Begründung des gegenteiligen Ergebnisses, also der Subsumierbarkeit der betreffenden Teile des Vorhabens unter die Regeln der Auftragsdatenverarbeitung, angestellten Erwägungen des vorgelegten Entwurfes gehen fehl: Die geplante Zusammenarbeit beschränkt sich nicht auf Vorgänge, die als *Datenverarbeitung im Auftrag* einzustufen wären.

(5.2.1) Die Erläuterung zu § 3 Abs. 2 der Verwaltungsvereinbarung geht davon aus, dass „schlicht-hoheitliches Nachfragen beim Auskunftspflichtigen“ noch Auftragsdatenverarbeitung und nicht schon Funktionsübertragung sei. Dies kann nicht richtig sein, weil solches schlicht-hoheitliche Nachfragen der Statistikbehörde der Sache nach das Geltendmachen des öffentlich-rechtlichen Auskunftsanspruches der Statistikbehörde gegenüber dem Auskunftspflichtigen ist, nur eben Geltendmachung eines restlichen Teiles dieses Anspruches. Datenschutzrechtlich handelt es sich auch dabei um *Datenerhebung*, wenn auch eben in Form einer ‚Nachlese’. Man kann dasselbe auch begrifflich-dogmatisch begründen: Schlicht-hoheitliches Handeln unterliegt dem öffentlichen Recht (vgl. Maurer, Allgemeines Verwaltungsrecht, § 3 Rdnr. 11).

Es würde also durch das nachfragende Amt eine öffentlich-rechtliche Befugnis gegenüber dem Befragten in Anspruch genommen. Deren Übertragung durch bloßes Verwal-

tungsabkommen wäre, zumindest weil ein Grundrecht (das Grundrecht auf informationelle Selbstbestimmung) betroffen ist, unwirksam.

(5.2.2) Weiter meint die genannte „Erläuterung“ der Verwaltungsvereinbarung, die schlichte Übernahme einer Angabe des Auskunftspflichtigen in die Datenbestände sei mangels Ausübung von „Entscheidungskompetenz“, also mangels „Beurteilungsspielraumes bei der Klärung von Zweifelsfragen“, bloße Auftragsdatenverarbeitung.

Abgesehen davon, dass ein solches Handeln wohl gesetzwidrig wäre, weil sich die Statistikverwaltung den absurdesten Angaben der Auskunftspflichtigen auslieferte und somit in dieser Phase auf Bemühungen um die Richtigkeit der erhobenen Daten bewusst verzichtete: Die Korrektur der zum Betroffenen gespeicherten Daten (Einzelangaben) gestaltet unmittelbar das öffentlich-rechtliche Verhältnis zwischen Auskunftspflichtigen und Statistikverwaltung, in dem den Auskunftspflichtigen ja eine - bußgeldbewehrte, § 23 BStatG - Wahrheitspflicht trifft: Die Entgegennahme und richtige Verbuchung der Leistung des kraft öffentlichen Rechtes Auskunftspflichtigen ist ein unmittelbar in dessen Grundrecht eingreifender Akt. Es werden auch in diesem Vorgang Informationsansprüche der öffentlichen Gewalt verwaltet.

Um den von mir immer wieder mit großem Nutzen herangezogenen Vergleich von Informations-Verwaltung mit der Verwaltung von Geld zu bemühen: Auch die Übertragung der Einziehung von Abgaben-Forderungen auf einen dritten (eben nicht forderungsberechtigten bzw. zuständigen) Träger öffentlicher Gewalt bedürfte sicherlich, weil sie die Ausübung von Kompetenzen bzw. Gläubigerrechten im Verhältnis zum Abgabenschuldner berührte, einer Rechtsvorschrift.

(5.2.3) Dem Entwurf hat ferner die Vorstellung zugrunde gelegen, die betreffenden geplanten arbeitsteiligen Verarbeitungsschritte hätten trotz ihres Personenbezuges keinen „Eingriffscharakter“. Das aber ist falsch. Denn die
- Beschaffung (Erhebung),
- Speicherung und
- inhaltliche Umgestaltung

personenbezogener Daten (vgl. § 3 Abs. 2 SächsDSG, § 3 Abs. 4 BDSG) ist ein *Grundrechtseingriff*, wie das Volkszählungsurteil des Bundesverfassungsgerichts herausgearbeitet hat (BVerfGE a. a. O.).

Es ist das Besondere dieses Grundrechtseingriffes, dass er sich ohne Beteiligung des Betroffenen, sozusagen hinter dessen Rücken, vollziehen kann (vgl. BVerfGE a. a. O. S. 46). Den Schein, dass damit in Grundrechte des Betroffenen nicht eingegriffen

werde, für die rechtliche Wirklichkeit zu nehmen hieße, die Grunderkenntnis des Volkszählungsurteils zu ignorieren.

(6) Ergebnis - also auch hier -: Es handelte sich um einen systematischen Bruch des Statistikgeheimnisses in der Form, wie es zurzeit nun einmal für Bundesstatistiken geltendes Recht ist, auch wenn das nicht notwendig, d. h. von Verfassungs wegen, so sein muss. Daran ändert es auch nichts, dass die Datenempfänger ihrerseits dem Statistikgeheimnis unterliegen. Es ist insoweit nicht anders als beim Arzt-, Sozial- und Steuergeheimnis.

Deswegen habe ich gefolgert, dass ohne Änderung des Bundesstatistikgesetzes und des Sächsischen Statistikgesetzes - gegebenenfalls durch Staatsvertrag - die Verwaltungsvereinbarung weitgehend gegen geltendes Recht verstoßen und ihre Umsetzung dementsprechend weitgehend rechtswidrig sein würde, dabei aber warnend hinzugefügt, dass man bei etwaigen Gesetzesänderungen die Grenzen, die das geltende Verfassungsrecht des Bundes mutmaßlich solchen Aufgabenverlagerungen setze, zu beachten haben würde.

3. Mit Art. 2 des Gesetzes zur Änderung des Statistikregistergesetzes und sonstiger Statistikgesetze vom 9. Juni 2005 (BGBl. I, S. 1534) hat der Bundesgesetzgeber (mit Beschlüssen im März und April 2005) im Bundesstatistikgesetz einen § 3 a eingeführt, der unter der Überschrift „Zusammenarbeit der statistischen Ämter“ den Wortlaut

> „(1) Das Statistische Bundesamt und die statistischen Ämter der Länder dürfen, soweit sie für die Durchführung von Bundesstatistiken und für sonstige Arbeiten statistischer Art im Rahmen der Bundesstatistik zuständig sind, die Ausführung einzelner Arbeiten oder hierzu erforderliche Hilfsmaßnahmen durch Verwaltungsvereinbarung oder aufgrund einer Verwaltungsvereinbarung auf andere statistische Ämter übertragen. Davon ausgenommen sind die Heranziehung zur Auskunftserteilung und die Durchsetzung der Auskunftspflicht.
>
> (2) Zu den statistischen Arbeiten nach Abs. 1 gehört auch die Bereitstellung von Daten für die Wissenschaft.“

hat, und § 16 Abs. 2 BStatG um den Satz

> „Darüber hinaus ist die Übermittlung von Einzelangaben zwischen den an einer Zusammenarbeit nach § 3 a beteiligten statistischen Ämtern und die zentrale Speicherung dieser Einzelangaben in einem oder mehreren statistischen Ämtern zulässig.“

ergänzt. Im Gesetzgebungsverfahren ist zu diesen von Bayern über den Bundesrat in das Gesetzgebungsverfahren eingebrachten Ergänzungen zur Begründung ausgeführt worden (BR-DS 878/1/04 [neu] vom 8. Dezember 2004):

> „Die vorgeschlagene Einführung eines § 3 a BStatG und die Ergänzung des § 16 Abs. 2 BStatG stellen die rechtliche Grundlage für eine neue Arbeitsteilung unter den statistischen Ämtern des Bundes und der Länder sowie für die hierzu erforderliche Übermittlung von Einzelangaben dar. Sie dienen der Klarstellung der Rechtmäßigkeit der geplanten Weitergabe von Einzeldaten im Rahmen der (im Entwurf vorliegenden) Verwaltungsvereinbarung über eine ämterübergreifende Aufgabenerledigung in der Statistik. Das Grundrecht auf informationelle Selbstbestimmung wird gewahrt, da die Daten nur innerhalb des geschützten Raumes der amtlichen Statistik übermittelt werden dürfen."

4. § 3 a Abs. 1 BStatG soll das Verfahren, die geplante Arbeitsteilung auf der Grundlage bloßer Verwaltungsvereinbarungen einzuführen, juristisch retten, er soll dem schon fertigen Entwurf einer solchen Verwaltungsvereinbarung die „rechtliche Grundlage" verschaffen, wie es heißt, auch wenn im nächsten Satz im Widerspruch dazu (gesichtswahrend) von einer bloßen *Klarstellung* die Rede ist.

(a) In der (gegenüber dem bayerischen Vorschlag in § 3 a vorgenommenen) Einschränkung des Abs. 1 Satz 1 durch Satz 2 hat man entweder die Arbeitsteilung gegenüber dem Betroffenen verschleiern oder aber die Verfassungsmäßigkeit der Regelung des Satzes 1 retten wollen: Allem Anschein nach hat man Bedenken gehabt, in einem Bundesgesetz vorzusehen, dass die Bundesländer durch bloße Verwaltungsvereinbarung anderen Bundesländern die Zuständigkeit für die *Heranziehung zur Auskunftserteilung* und für die *Durchsetzung der Auskunftspflicht* zu übertragen.

Auf diese Weise werden diejenigen Handlungen der Statistikbehörde, in denen sie mit Ausübung staatlicher Befehls- bzw. Zwangsgewalt in Erscheinung tritt, von der Arbeitsteilung ausgenommen. Konkret: Die Aufforderung, pflichtgemäß einen Fragebogen der amtlichen Statistik auszufüllen und einzusenden, soll der Sachse auch weiterhin nicht vom Bayerischen Statistischen Landesamt bekommen können, auch wenn dieses die Daten z. B. der Binnenfischereistatistik „bundesweit" überlassen bekommen und weiterverarbeiten soll, wohlgemerkt auch schon vor einer vollständigen Beseitigung des Personenbezuges.

Damit gibt es zwei Möglichkeiten: Entweder scheint der Gesetzgeber schon für die schlichte „Nachfrage“ (vorstehend 3 unter [5.2.1]) keine zutreffende Einordnung vorgenommen zu haben, vor allem aber übersehen zu haben, dass auch die vom Wortlaut des Satzes 2 ja nicht erfasste schlichte, für den Betreffenden erkennbare Inempfangnahme der Daten - also die „Erhebung“ -, aber auch die ohne Zutun und Wissen des Betroffenen stattfindende Weiterverarbeitung seiner Daten (solange sie noch Personenbezug aufweisen) durch die Statistikverwaltung einen *Grundrechtseingriff* darstellt, der auf der Grundlage des öffentlichen Rechtes stattfindet und damit zumindest schlicht-hoheitliches Verwaltungshandeln ist.

Oder aber es gibt nur noch die andere Möglichkeit, dass der Gesetzgeber von der Vorstellung ausgegangen ist, dass es verfassungsrechtliche Grenzen der Übertragung der Ausführung von Bundesgesetzen durch die Länder auf eine einziges, für alle anderen tätig werdendes Bundesland nur für die Übertragung *obrigkeitlicher,* nicht aber schlicht-hoheitlicher Befugnisse sowie derjenigen Aufgaben gibt, der die Ausübung dieser Befugnisse dient.

(b) Eine solche Unterscheidung ist dem geltenden Verfassungsrecht nach meinem Kenntnisstand jedoch fremd. Vielmehr spricht vieles dafür, dass die in § 3 a Abs. 1 Satz 1 BStatG erhaltene Erlaubnis einer Übertragung der Aufgabe der Ausführung der Bundesstatistikgesetze durch die Länder auf ein einziges Bundesland (durch bloße Verwaltungsvereinbarung) auch in ihrer durch Satz 2 vorgenommenen Einschränkung *verfassungswidrig* ist.

Das gilt zunächst wohl schon im Hinblick auf die Zuständigkeitsordnung des Grundgesetzes: Das Bundesverfassungsgericht hat der grundsätzlichen Länderzuständigkeit gemäß Art. 30, Art. 83 GG die *Pflicht* der Länder, die Bundesgesetze auszuführen, entnommen (zuletzt wohl in der Entscheidung vom 15. Juli 2003 - 2 BvF 6/98, DöV 2003, 902, unter C I 1 der Gründe unter Hinweis insbesondere auf BVerfGE 55, 274, 318). Das ist auch im Schrifttum unbestritten. Zwar ist der Grundsatz der „Unverfügbarkeit der Kompetenzen“ in diesen Entscheidungen konkret immer nur im Hinblick auf das Verhältnis der Länder zum Bund formuliert worden. Aber er gilt „mit Abschwächung“ auch für das Verhältnis zwischen den Ländern (Isensee, Idee und Gestalt des Föderalismus im Grundgesetz, in: HStR IV, § 98 Rdnr. 177). Und selbst ein Verfechter einer insoweit eher großzügigen Auffassung formuliert: „Die bundesstaatliche Regel ist die eigenverantwortliche Aufgabenerfüllung. Die Abweichung von der Regel bedarf der Rechtfertigung durch Gründe, die in der Aufgabenmaterie und ihren rechtlichen wie faktischen Anforderungen liegen“ (Isensee a. a. O. Rdnr. 178) und nennt als solche Gründe die Überforderung der einzelnen Bundesländer und die um der bundesweiten Freizügigkeit willen bestehende Notwendigkeit zentraler Einrichtungen

(a. a. O. Rdnr. 175). Beispiele sind die Zentrale Vergabestelle für Studienplätze (deren Kompetenzen ja zurzeit zugunsten der Eigenständigkeit der Hochschulen im Abbau begriffen sind), die Filmbewertungsstelle in Wiesbaden und das ZDF (Blümel, Verwaltungszuständigkeit, in: HStR IV, § 101 Rdnr. 172) - alles Fälle, die von einer Ausführung von Gesetzen, für die ausschließliche Bundesgesetzgebungszuständigkeit besteht und bei der es gemäß Art. 87 Abs. 3 Satz 1 GG eine selbständige Bundesoberbehörde, eben das Statistische Bundesamt (§ 2 BStatG), gibt, weit entfernt sind.

Die punktuelle oder auf wenige Länder beschränkte Zusammenarbeit, sei es durch neugeschaffene besondere rechtsfähige Einrichtungen oder durch Kompetenzübertragung zur Ausübung („quoad usum“, Rudolf, Kooperation im Bundesrat, in: HStR IV, § 105 Rdnr. 53). wird wohl noch nicht gegen die im Grundgesetz geregelte bundesstaatliche Ordnung verstoßen, wohl aber ein Vorhaben, bei dem - erstmals - nicht in bloßen Versagungen bestehende Grundrechtseingriffe (Studienplatzvergabe!), für die die einzelnen Länder zuständig sind, in bundesweiter Zuständigkeit auf ein einzelnes Bundesland (zur Ausübung) übertragen werden. Hier schaffen die Länder eine Zentralverwaltungszuständigkeit, die das Grundgesetz insoweit dem Bund gerade verwehrt hat, und das begründet genau die Gefahren, die durch die vom Grundgesetz vorgesehene Zuständigkeit der einzelnen Bundesländer gerade vermieden werden sollen. Diese Gefahr ist hier eine datenschutzrechtlich relevante, und sie ist evident: Es entstehen branchenbezogen *zentrale* Datensammlungen, die es sonst nicht gäbe, weil das Statistische Bundesamt gerade nicht alle Einzelangaben, sondern schon vielfach nur zusammengefasste Daten bekommt.

(c) Demgegenüber gibt es auch die Auffassung, die Grenzen für die möglichen Formen einer Kooperation der Länder untereinander seien nicht der verfassungsrechtlichen Regelung des Bundesstaates als ganzen, also dem Grundgesetz, zu entnehmen, mithin namentlich auch nicht Art. 83 GG, sondern den Länderverfassungen (so Hermes in: Dreier, GG-Kommentar, Rdnr. 53 zu Art. 83), so dass also diese bestimmten, in welcher Weise die zuständigen Landesorgane die bundesverfassungsrechtlich den einzelnen (!) Ländern zugewiesenen Exekutivkompetenzen wahrzunehmen hätten (Hermes a. a. O.). Aber auch bei dieser Auffassung ergibt sich, wie schon oben (2 unter [3.1]) ansatzweise angesprochen, ein verfassungsrechtliches Problem: § 3 a BStatG widerspricht insoweit, als er eine Verlagerung der Zuständigkeit für Aufgaben und Befugnisse durch bloße Verwaltungsvereinbarung für zulässig erklärt, Art. 83 Abs. 1 SächsVerf.

Sieht man nun aber mit dieser Auffassung - *in Auslegung des Grundgesetzes* - die maßgebliche Regelung der Möglichkeit der Übertragung von Verwaltungszuständigkeit von Ländern auf andere Länder gerade in den Landesverfassungen, also im Landesverfassungsrecht, kann eine solche Übertragungserlaubnis schon von Bundesverfassungs-

rechts wegen nicht durch einfaches Bundesrecht ausgesprochen werden, ist mithin § 3 a BStatG zumindest insoweit wegen mangelnder Gesetzgebungskompetenz des Bundes grundgesetzwidrig. Das gilt nicht nur insoweit, als die Vorschrift die Kompetenzübertragung durch bloße Verwaltungsvereinbarung zulässt, sondern insgesamt: Weil ja die Möglichkeit der Übertragung von Verwaltungskompetenzen insgesamt danach ausschließlich Landesrecht zugehört. Denn es könnte ja sein, dass eine Landesverfassung eine solche Kompetenzverlagerung nach auswärts generell verböte (was wohl nicht grundgesetzwidrig wäre) oder an Voraussetzungen knüpfte, die über den Tatbestand des § 3 a Abs. 1 Satz 1 BStatG hinausgehen.

Soll § 3 a Abs. 1 BStatG als eine von der Gesetzgebungskompetenz des Bundes gedeckte Regelung für das Verwaltungsverfahren der Bundesstatistik Bestand haben, muss die Vorschrift zumindest mit der Einschränkung versehen werden, dass sie vorbehaltlich länderrechtlicher Regelungen gilt.

(d) Hinzu kommt wohl ein Verstoß gegen das *Demokratieprinzip* des Art. 20 Abs. 2 Satz 1 GG (und des gleichlautenden Art. 3 Abs. 1 Satz 1 SächsVerf), wonach das Handeln der Exekutive der demokratischen Legitimation bedarf, d. h. die Exekutive demokratisch gesteuert werden muss (vgl. Dreier in Dreier, GG-Kommentar, Rdnr. 113 zu Art. 20), was schon kraft Art. 28 GG auch für die Länder gelten muss.

Aus dem Zusammenwirken der im Grundgesetz vorgenommenen Begründung der Verwaltungszuständigkeit der einzelnen (Hermes in Dreier, Hrsg., GG-Kommentar, Rdnr. 53 zu Art. 83) Länder mit dem Demokratieprinzip folgt, dass die auf das Gebiet eines Bundeslandes bezogene, von der Exekutive des Bundeslandes nach der Kompetenzzuweisung des Grundgesetzes auszuübende Staatsgewalt von denjenigen, die ihr als in diesem Bundesland ansässige Deutsche unterworfen sind, über die Landes-Volksvertretung demokratisch kontrolliert wird.

Eine Erlaubnis, die Ausübung der Exekutivzuständigkeit auf ein anderes Bundesland zu übertragen, erlaubt die Beseitigung dieser demokratischen Bindung (Legitimation) der Verwaltungstätigkeit an die von ihr infolge Ansässigkeit im betreffenden Bundesland betroffenen Staatsbürger. Organisatorisch-personelle Legitimation (mit dem „Prinzip der individuellen Berufung der Amtswalter durch das Volk bzw. durch volksgewählte Organe“ [!] - R. Herzog zitiert bei Böckenförde, Demokratie als Verfassungsprinzip, in HStR, I, § 22 Rdnr. 16) und die übrige parlamentarische Kontrolle der Verwaltung findet dann nämlich insoweit seitens der in den übertragenden Ländern ansässigen Betroffenen (soweit deutsche Staatsbürger) nicht mehr statt.

Ohnehin ist die bundesstaatliche Aufgliederung der Staatsgewalt, einschließlich der mit ihr gegebenen Kompetenzzuweisung an die einzelnen Länder, vermöge der Dezentralisation und der mit ihr gegebenen Bürgernähe engstens mit dem freiheitlich-rechtsstaatlichen und dem demokratischen Charakter der grundgesetzlichen Staatsordnung verbunden (vgl. etwa auch Kruis, Finanzautonomie und Demokratie im Rechtsstaat, DöV 2003, 10, 13 f., vgl. dort insbesondere auch 14 rSp Mitte: *Soweit den Bundesländern nur die vollziehende Gewalt zusteht, wird der legislative Akt der Legitimation durch das Bundesvolk, der Vollzugsakt jedoch auch der Legitimation durch das Teilvolk des Landes zugeordnet*).

Das Problem hat Presseberichten zufolge kürzlich auch der Bundesverfassungsrichter Hans-Joachim Jentsch angesprochen. Die Zeitung „Die Welt“ vom 26. April 2005 (dem Pressespiegel der Landtagsverwaltung sei Dank!) gibt ihn folgendermaßen wieder:

> „Wenn wichtige Verwaltungseinheiten oder Gerichte von Ländern zusammengelegt werden, kann das nach Ansicht des Verfassungsrichters auch rechtliche Probleme bergen. ‚Richter oder Verwaltungsleute müssen legitimiert sein’, sagte Jentsch. ‚Wenn die Länder gemeinsame Gerichte haben, müssen sie unterschiedliche Senate haben, von den Ländern legitimiert.’“

Weniger rechtlich, eher politisch hat der Staatsrechtler Prof. Rudolf, zugleich seit langem rheinland-pfälzischer Datenschutzbeauftragter, dies in seiner Abhandlung zur „Kooperation im Bundesstaat“, in HStR IV, § 105 Rdnr. 81 formuliert:

> „Die eigentlichen Verlierer des kooperativen Föderalismus … sind die Landtage. Die von den Regierungen betriebene Kooperation zwischen den Ländern und zwischen Bund und Ländern hat den politischen Einfluss der Landtage *faktisch* gemindert“.

(e) Es handelt sich um ein neuartiges Problem: Während es früher fast nur positive Kompetenzkonflikte gegeben hat, sehen in Zeiten leerer Kassen Kompetenzträger zu, wie sie sich ihrer ausgabenträchtigen Zuständigkeit entziehen können (persönliche Mitteilung des Staatsrechtlers C. Heitsch, in dessen Habilitationsschrift *Die Ausführungen der Bundesgesetze durch die Länder* von 2001 das Problem noch nicht erörtert ist).

5. Praktische Folgerungen aus diesen auch dem einen oder anderen Verantwortlichen in der Statistikämter-Szene keineswegs fremden rechtlichen Überlegungen: Im Falle der Einführung der ämterübergreifenden Aufgabenerledigung dürften Klagen auf Unterlassung der ämterübergreifenden Verarbeitung statistischer Einzelangaben, etwa von

Mikrozensus-Daten, mit einiger Wahrscheinlichkeit begründet sein (mit Verwerfungsmonopol des Bundesverfassungsgerichts aus Art. 100 GG). Telefonische Anfragen Betroffener wegen der Rechtmäßigkeit namentlich der Mikrozensusstatistik oder der neu eingeführten Dienstleistungsstatistik dürften nicht mehr uneingeschränkt im Sinne einer Empfehlung, der rechtmäßigen Durchführung der von den Datenschutzbeauftragten gründlich geprüften und beobachteten Statistik zu vertrauen, beantwortet werden können.

5.7.3 Verbund der mitteldeutschen Statistischen Landesämter

Im November 2004 haben die Innenminister Sachsens, Sachsen-Anhalts und Thüringens eine *Verwaltungsvereinbarung über die Bildung eines Mitteldeutschen Verbundes Statistischer Landesämter* unterzeichnet, die neben rechtlich weniger weitgehender Zusammenarbeit unter anderem auch „arbeitsteilige Statistikproduktion“ (§ 2 Abs. 1 Satz 4 der Vereinbarung) vorsieht, wozu (laut Satz 5 der genannten Vertragsbestimmung) unter anderem auch „die Erhebung“ und „die Aufbereitung“ gehört. *Was* erhoben und aufbereitet werden soll, wird im Text der Vereinbarung gar nicht ausdrücklich gesagt, ist aber spätestens nach einem Blick in § 1 Abs. 1 Satz 1 SächsStatG klar: Daten - und die sind eben in den Anfangsabschnitten der Durchführung einer Statistik, namentlich während der Erhebung, Sammlung und Aufbereitung, personenbezogen.

§ 4 Abs. 5 der Vereinbarung bestimmt, dass die gesamte vereinbarte *länderübergreifende Zusammenarbeit* (vgl. auch dort § 1 Abs. 1) „im Einklang mit bestehenden und künftigen Initiativen der Zusammenarbeit auf Ebene Bund und Länder“ durchzuführen ist. Man hat somit den Eindruck, dass die beteiligten Länder schon einmal mit der *ämterübergreifenden Aufgabenerledigung*, wie sie vorstehend in Abschnitt 5.7.2 dargestellt worden ist, beginnen wollen, dabei sich dann aber, wenn es so weit kommt, in die mehr oder weniger alle Bundesländer umfassende Arbeitsteilung eingliedern wollen.

Dieser Teil des Vorhabens ist aus Gründen, die sich alle aus den vorstehend in den Abschnitten 5.7.1 und 5.7.2 angestellten Überlegungen ergeben und die für das SMI im September 2004 weitgehend nicht neu gewesen sind, in wesentlichen Teilen rechtswidrig. Für diese besondere Zusammenarbeit aller Länder ist aus den Ausführungen zu 5.7.2 nämlich zu folgern:

(1) Hineingreifen eines anderen Partnerlandes nach Sachsen:
§ 2 Abs. 1 Satz 4 i. V. m. Satz 5 der Verwaltungsvereinbarung sieht eine auch bei Geltung des § 3 a Abs. 1 BStatG und des in § 16 Abs. 2 BStatG hinzugefügten Satzes 2

(s. vorstehend 5.7.2 unter 4) gegen § 3 Abs. 2 Nr. 1 i. V. m. § 2 Abs. 1 Nr. 1 und 2 SächsStatG verstoßende Verhaltensweise vor: Vorstehend Abschnitt 5.7.2 unter 2 (3.1).

Jeder Versuch des Statistischen Landesamtes eines der beiden anderen beteiligten Bundesländer, Daten von in Sachsen Ansässigen zu erheben, insbesondere diese zur Auskunft heranzuziehen, ist, soweit sich der Vorgang auf sächsischem Gebiet abspielt, wegen Verstoßes gegen das Sächsische Statistikgesetz rechtswidrig.

Jede Handlung sächsischer Stellen, die eine solche abkommensgemäße Übertragung von Aufgaben und Befugnissen auf das Statistische Landesamt eines der beiden anderen beteiligten Bundesländer unternimmt, ist unwirksam, sie ist zumindest ein Verstoß gegen das Sächsische Statistikgesetz.

(2) Hinausgreifen des Statistischen Landesamtes des Freistaates Sachsen in ein anderes Partnerland:
Man wird die in § 3 Abs. 2 Nr. 1 SächsStatG enthaltene Bezugnahme auf § 2 Abs. 1 Nr. 1 und 2 SächsStatG so auszulegen haben, dass jeweils nur Verhältnisse in Sachsen ansässiger Personen bzw. in Sachsen belegener Erhebungseinheiten gemeint sind, dass also schlicht die Zuständigkeit des Sächsischen Statistischen Landesamtes *beschränkt* auf Sachsen *begründet* wird.

Durch dieses grenzüberschreitende Hineingreifen in eines der anderen Partnerländer verstieße das Statistische Landesamt des Freistaates Sachsen gegen diese für es im Sächsischen Statistikgesetz bestimmten Schranken seiner Zuständigkeit.

(3) Insoweit mit der „Erhebung“ auch die Heranziehung zur Auskunftserteilung und die Durchsetzung der Auskunftspflicht gemeint ist, sieht die Vereinbarung, und zwar auch bei Anwendung von dessen § 3 a Abs. 1 und § 16 Abs. 2 Satz 2, eine gegen das Bundesstatistikgesetz verstoßende Verarbeitung statistischer Einzelangaben vor.

Insoweit § 3 a Abs. 1 BStatG (mit § 16 Abs. 2 Satz 2 BStatG) verfassungswidrig ist, wäre die genannte § 2 Abs. 1 Satz 4 der Verwaltungsvereinbarung entsprechende Verfahrensweise der Statistikbehörden natürlich erst recht ein Verstoß gegen das Bundesstatistikgesetz.

(4) Inwieweit der Umstand, dass die Verwaltungsvereinbarung zu rechtswidrigem Handeln gegenüber den Betroffenen verpflichtet, sich auf die Gültigkeit der Verwaltungsvereinbarung zwischen den Vertrags-Parteien auswirkt, ist von zweitrangiger Bedeutung:

Die Vorschriften der Verwaltungsverfahrensgesetze über den öffentlich-rechtlichen Vertrag sind auf Verwaltungsabkommen nicht anwendbar (Hennecke, in: Knack, Hrsg., VwVfG-Komm., Rdnr. 3 zu § 54 - man wüsste auch schon nicht, *welches* Verwaltungsverfahrensgesetz jeweils anwendbar sein könnte). Aber der Grundgedanke des § 54 VwVfG des Bundes gilt auch hier: Verwaltungsvereinbarungen zwischen Trägern öffentlicher Gewalt, die Verpflichtungen zu Leistungen vorsehen, deren Erbringung gegen die Verfassungsgrundsätze des *Vorbehaltes* oder des *Vorranges des Gesetzes* verstoßen (vgl. Kopp, VwVfG-Komm., Rdnr. 24 zu § 54) dürfte wegen „entgegenstehender Rechtsvorschriften“ (§ 54 Satz 1 VwVfG) wohl nichtig sein, weil auch im Anwendungsbereich der ja die Nichtigkeitsgründe beschränkenden Regelungen des § 59 VwVfG nach Abs. 1 dieser Vorschrift in entsprechender Anwendung von § 134 BGB auch solche Vertragsinhalte als nichtig anzusehen sind, die gegen ein Verbot verstoßen, welches man dem Verfassungsrecht einschließlich der allgemeinen verfassungsrechtlichen Grundsätze entnehmen kann, wobei die Auswirkung eines Verstoßes gegen Regeln über die sachliche und örtliche Zuständigkeit umstritten sind (Kopp a. a. O. Rdnr. 7 zu § 59 VwVfG).

Es dürfte sich um eine Teilnichtigkeit handelt (vgl. § 139 BGB, § 59 Abs. 3 VwVfG).

Noch einmal: Unabhängig von der Frage der rechtlichen Wirksamkeit der in § 2 Abs. 1 Satz 4 und 5 des Verwaltungsabkommens begründeten Verpflichtung zur *arbeitsteiligen Erhebung und Aufbereitung* statistischer Einzelangaben ist unzweifelhaft, dass die Erfüllung dieser Verpflichtung im Verhältnis zum Betroffenen rechtswidrig wäre.

(5) Die Übertragung der Aufgaben und Befugnisse auf ein fremdes Amt *durch Staatsvertrag* (statt durch bloße Verwaltungsvereinbarung) widerspräche nach geltendem Recht dem Bundesstatistikgesetz, weil dieses in § 16 eine über § 3 a Abs. 1 BStatG hinausgehende Befugnis zur Übertragung von Aufgaben und Befugnissen auf Dritte (bei der Durchführung von Bundesstatistiken) ausschließt (wie in § 3 a Abs. 1 Satz 2, § 16 Abs. 2 Satz 2 BStatG deutlich zum Ausdruck kommt).

(6) Anders zu beurteilen wäre eine *Zusammenlegung* der drei Statistischen Landesämter durch Staatsvertrag (vgl. vorstehend 5.7.2 unter 4 [b]).

5.7.4 Probleme der Wahlstatistik

Wenn an Wahltagen um 18:00 Uhr die Wahllokale geschlossen werden und noch kein einziger Stimmzettel ausgezählt ist, gibt es schon ganz frische Ergebnisvorhersagen privater Meinungsforschungsunternehmen, die erstaunlich genau sind und auch nach Wählergruppen unterscheiden. Sie beruhen auf der Befragung der Wähler ausgewählter Stimmbezirke nach der Wahlhandlung. Staatlicherseits verlässt man sich freilich nicht

allein auf die auf diese Weise erhobenen Zahlen, die, bezogen auf den einzelnen Wähler, naturgemäß aggregierte statistische Ergebnisse sind. Für eine gründliche Auswertung nach Alter und Geschlecht der Wähler - nach mehr, d. h. zusätzlichen Merkmalen, aber auch nicht! - sehen die Wahlgesetze bzw. die auf ihrer Grundlage als Verordnungen erlassenen Wahlordnungen die Durchführung von Wahlstatistiken vor (für die Landtagswahl: § 51 Abs. 2 Satz 1 SächsWahlG; im Bund gibt es sogar ein eigenes Wahlstatistikgesetz). Andererseits schreiben die Verfassungen für die vom Volk vorzunehmenden Wahlen (und Abstimmungen) vor, dass diese *geheim* zu sein haben: Art. 4 Abs. 1 SächsVerf, Art. 38 Abs. 1 GG. Das Wahlgeheimnis dient der Freiheit der Wahl. Die informationelle Selbstbestimmung hinsichtlich des Wahlhandelns ist ein Musterbeispiel für den freiheitssichernden Zweck des Datenschutzes. Aus verfassungsrechtlichen Gründen hat das Wahlgeheimnis den Vorrang vor der Durchführung der Wahlstatistik. Mit anderen Worten: Die Statistik darf nur so durchgeführt werden, dass das Wahlgeheimnis unberührt bleibt. Entsprechend formuliert § 51 Abs. 2 Satz 2 SächsWahlG für die Landtagswahlen: *Die Trennung der Wahl nach Altergruppen und Geschlechtern ist nur zulässig, soweit die Stimmabgabe der einzelnen Wähler dadurch nicht erkennbar wird.*

Es liegt auf der Hand, dass es nicht ganz einfach ist, eine Wahlstatistik zu organisieren, die das Wahlgeheimnis unbeeinträchtigt lässt. Einzelfragen, die sich dabei stellen und bei denen es teilweise darum geht, Fallbeispiele durchzurechnen, habe ich mit dem SMI in Hinblick auf die Überarbeitung der Wahlordnung im Jahre 2003 diskutiert.

(1) Zunächst und vor allem: Die neue, im Oktober 2003 in Kraft getretene Landeswahlordnung (LWO) hat ins einzelne gehende Vorschriften eingeführt, die das pauschale Gebot der Wahrung des Statistikgeheimnisses mit konkretem Inhalt füllen:

- Es wird eine bestimmte Mindestgröße (Wahlberechtigtenanzahl) für die Stichprobenwahlbezirke festgelegt (§ 70 Abs. 2 Satz 3 LWO),
- es wird die Zusammenfassung von Altersjahrgängen vorgeschrieben (§ 70 Abs. 3 Satz 4 LWO),
- es wird die Trennung der für die Stimmenauszählung zuständigen von den für die statistische Auswertung zuständigen Stellen vorgeschrieben (§ 71 Abs. 2 Satz 3 und 5 LWO) und
- es wird die Zusammenführung von Wählerverzeichnis und gekennzeichneten Stimmzetteln verboten (§ 71 Abs. 3 LWO).

Alle diese beträchtlichen Verbesserungen hatte das SMI von sich aus von vornherein in seinen Entwurf eingebaut.

(2) Die wichtigste Vorkehrung zum Schutz des Wahlgeheimnisses ist dabei natürlich, dass dieses nicht durch die *Bekanntgabe der Ergebnisse an die Öffentlichkeit* verletzt wird. Wichtigste Vorschrift ist insoweit das nunmehr in § 73 Satz 4 LWO genauer als bisher ausgesprochene Verbot, die Ergebnisse einzelner Wahlbezirke zu veröffentlichen. Allerdings bietet die Vorschrift für sich genommen insoweit noch keinen vollständigen Schutz des Wahlgeheimnisses. Wenn, so habe ich dem SMI vorgerechnet, sehr kleine Gemeinden eine kommunale Statistikstelle einrichten, dürfen sie Ergebnisse aus mindestens zwei Wahlbezirken (§ 73 Satz 4 LWO ist dann eingehalten!) mit jeweils mindestens 400 (§ 70 Abs. 2 Satz 3 LWO ist eingehalten), also im ungünstigen Fall lediglich 800 Wahlberechtigten veröffentlichen. Halbiert man diese Zahl wegen der Wahlbeteiligung und des Abzuges der Briefwähler und außerdem noch einmal wegen der Geschlechtsaufteilung, also zweimal, kommt man bei unterstellten 87 wahlberechtigten Altersjahrgängen auf durchschnittlich ungefähr 2,3 Stimmabgaben je Jahrgang, so dass bei der Einhaltung der Regel für die Zusammenfassung von Altersjahrgängen nach § 70 Abs. 3 Satz 4 LWO (mindestens sieben Altersjahrgänge sind in einer Geburtsjahresgruppe zusammenzufassen) im ungünstigen Fall nur 16,1 Personen einer Merkmalskombination von Alter und Geschlecht angehören. Bei Wahlvorschlägen, die im einstelligen Prozentbereich der Stimmen bleiben - davon hat es bei der letzten Landtagswahl ja dann einige gegeben - ergeben sich dann Tabellenfeldwerte zwischen null und zwei, so dass das Statistik- und damit auch das Wahlgeheimnis nicht gewahrt wären. Tabellenfeldwerte kleiner als drei sind nicht hinreichend personenbezugsfrei, im Hinblick auf vereinzelt vorhandenes Zusatzwissen, mit dessen Vorhandensein im Publikum aber mit Sicherheit zu rechnen ist (vgl. auch Simitis/Dammann, 5. A. Rdnr. 16 zu § 3 BDSG).

Es ist daher für die Einhaltung des Gebotes des § 51 Abs. 1 Satz 2 SächsWahlG wie auch für die Vermeidung eines Widerspruches zu dessen Gebot des Vorranges des Wahlgeheimnis wiederholenden § 70 Abs. 1 Satz 2 LWO erforderlich, dass die Veröffentlichung von Tabellenfeldwerten unter drei untersagt wird. Ein entsprechendes Verbot ist § 19 SächsStatG (i. V. m. § 18 SächsStatG) zu entnehmen (vgl. insbesondere § 19 Abs. 4): Ich habe gegenüber dem SMI argumentiert, dass § 51 SächsWahlG keinerlei Anhaltspunkte dafür biete, dass diese Vorschrift als Ausnahmeregelung die Geltung der allgemeinen statistikrechtlichen Vorschrift des § 19 SächsStatG ausschlösse, dass aber andererseits § 73 LWO in diesem Sinne verstanden werden könne, mit der Folge, dass die Vorschrift insoweit wegen Verstoßes gegen höherrangiges Recht rechtswidrig wäre. Deshalb habe ich es für dringend geboten gehalten, eine klarstellende Bezugnahme auf § 19 SächsStatG einzufügen, also § 73 Satz 4 als eigenen Satz einzufügen, dass *§ 19 SächsStatG im Übrigen unberührt bleibt.* (Man hätte zusätzlich auch § 18 SächsStatG nennen können.)

Das SMI ist dieser Anregung, wie man in der Landeswahlordnung sieht, nicht gefolgt, und hat das damit begründet, dass eine Vorschrift des Sächsischen Statistikgesetzes, als höherrangiges Recht, doch nicht von einer Vorschrift einer Rechtsverordnung außer Kraft gesetzt werden könne, weswegen man „aus Deregulierungsgründen“ auf eine solche klarstellende Regelung zu verzichten habe. Das hat, wie ich erwidert habe, nicht ganz die Fragestellung getroffen, die nämlich die gewesen ist, ob der Verordnungsgeber eine Vorschrift erlassen soll, die ihrem Wortlaut nach Datenübermittlungen zulässt, die wegen Verstoßes gegen höherrangiges Recht rechtswidrig sind, und die dadurch selbst gegen höherrangiges Recht verstößt. Aber immerhin: Nach der Argumentation des SMI ist das nur ein *falscher Schein: § 73 LWO ist nur in den Grenzen des § 19 SächsStatG (mit § 18 SächsStatG) anzuwenden.* Man könnte auch sagen: Die Vorschrift ist gesetzeskonform in diesem Sinne auszulegen.

Das SMI sollte dafür sorgen, dass das allen, die § 73 LWO anwenden, klargemacht wird.

(3) Aber auch schon *vor* der Phase der Veröffentlichung von Zahlentabellen, also des bezweckten Statistik-Endproduktes, muss das Wahlgeheimnis und damit das Grundrecht auf informationelle Selbstbestimmung bei der Durchführung der Wahlstatistik gewahrt bleiben - also auch schon *innerhalb der mit der statistischen Auszählung der Stimmzettel betrauten Statistikbehörden* (Statistisches Landesamt nach § 71 Abs. 2 Satz 3, kommunale Statistikstellen nach § 71 Abs. 2 Satz 5 oder § 72 LWO). Das Wahlgeheimnis ist in dieser Hinsicht in demjenigen Falle nicht mehr vollständig gewahrt, dass ein Bearbeiter Kenntnis einzelner Wahlentscheidungen von Angehörigen selten vertretender Altersjahrgänge in jedem Wahlkreis hat. Das folgt aus der vorstehend zu zwei zusammengeführten Stimmbezirken aufgestellten Berechnung im Wege des Erst-recht-Schlusses. Die Gebote, mindestens sieben Altersjahrgänge zusammenzufassen und höchstens sechs Geburtsjahresgruppen zu bilden (§ 70 Abs. 3 Satz 4 LWO), verhindert diese Möglichkeit jedoch nicht, reicht also insofern nicht aus. Es ist aber die ausschließliche Funktion dieser Vorschriften, den Schutz des Wahlgeheimnisses gerade *gegenüber den mit der Durchführung der Statistik befassten Bediensteten* zu gewährleisten. Das folgt daraus, dass für die Geheimhaltung gegenüber der Öffentlichkeit oder sonstigen Datenempfängern außerhalb der Statistikbehörde die Vorkehrungen des § 73 - in der gebotenen Ergänzung durch §§ 18 f. SächsStatG - ausreichen, wie vorstehend dargelegt.

Es spricht daher eine Menge dafür, dass diese Einschränkung des Wahlgeheimnisses gegen das bereits zitierte Gebot des § 51 Abs. 2 Satz 2 SächsWahlG verstößt. Denn dieser Vorschrift ist nicht zu entnehmen, dass sich das Gebot, die Statistik so durchzuführen, dass das Stimmverhalten einzelner Wähler nicht erkennbar wird, ausschließ-

lich auf die Erkenntnisse der Öffentlichkeit, nicht aber auf Erkenntnismöglichkeiten der Bediensteten der Statistikbehörde bezieht.

Dagegen ließe sich wohl nur einwenden, dass es sich dann um eine Ausnahmevorschrift handelte. Denn das Personal der statistischen Behörden erfährt ja normalerweise durchaus personenbezogene Daten. Auch wäre es ja nicht erforderlich, die Auswertung der Statistikbehörde zu übertragen, wenn das Wahlgeheimnis ohnehin schon von Anfang an vollständig gewahrt wäre, ein Personenbezug von Anfang an nicht bestünde, eine Geheimhaltung also gar nicht erforderlich wäre.

Ob nun die Freiheit der Wahl höher einzuschätzen ist als andere Freiheiten und deswegen die Geheimhaltung des Wahlverhaltens von Verfassungs wegen weiter reichen muss als die Geheimhaltung anderer persönlicher Verhältnisse, die staatlich erfasst werden (z. B. Krebsregister-Daten, Daten des Mikrozensus), so dass insoweit nur von vornherein absolut personenbezugsfreie Statistiken - die auch außerhalb des Anwendungsbereiches des Statistikgesetzes stünden - zulässig wären, scheint mir nicht sicher zu sein. (Die strenge Auffassung, wonach *in allen Stadien der Durchführung der Wahlstatistik* das Wahlgeheimnis gewahrt bleiben müsse, hat jedoch ausdrücklich der 16. TB des LfD BW, 1995, LT-DS 11/6900, S. 74 vertreten.)

Ich habe mit dieser Begründung dem SMI erklärt, dass § 70 Abs. 3 Satz 4 LWO mit einiger Wahrscheinlichkeit, aber nicht unbedingt zwingend, rechtswidrig sein würde.

Was die Möglichkeit der Abhilfe betrifft, habe ich die Auffassung geäußert, dass sich annähernde Sicherheit für das Wahlgeheimnis auch im innerstatistischen Bereich wohl noch nicht erreichen ließe, wenn man als zusätzliche Regel einführte, dass je Wahlvorschlag (‚Partei') in jeder durch Alterstufe und Geschlecht gebildeten Gruppe mindestens 25 Wahlberechtigte vorhanden sein müssen (so der Vorschlag im TB des LfD BW a. a. O. S. 75). In diesem Falle entspräche die Entscheidung von 4 % der Wähler der Abgabe *einer* Stimme. Denn Negativ-Aussagen ließen sich auch dann nicht völlig ausschließen (Beispiel: Wähler X hat nicht die kleine Partei P gewählt - obwohl er ihr womöglich, wie mancher in dem betreffenden Wahlbezirk weiß, angehört -, weil niemand oder nur der Statistikbehördenbedienstete oder ein diesem persönlich gut bekannter Wahlberechtigter in dieser Geschlechts- und Altersgruppe die Partei gewählt hat).

Abhilfe könnte, dies habe ich dem SMI vorgeschlagen, aber die Regel schaffen, dass kein Wahlbezirk in die Statistik einbezogen werden darf, in dem ein im Statistikamt mit der Wahlstatistik befasster Bediensteter wohnt - oder umgekehrt, dass der Personaleinsatz so gesteuert wird, dass kein Bediensteter damit befasst wird, der in einem der ausgewerteten Wahlbezirke wohnt. Auch diese Regelung wäre nicht einhundertpro-

zentig sicher, das Restrisiko wäre jedoch äußerst beschränkt. Meiner Einschätzung, dass eine solche Verfahrensweise auf jeden Fall statistikunschädlich und ohne weiteres praktikabel durchzuführen sei, ist das SMI mit der wenig überzeugenden Behauptung entgegengetreten, bei der Auswahl der Wahlbezirke (sc. nach statistischen Gesichtspunkten) dürfe der Umstand, dass in einem zunächst ausgewählten Wahlbezirk ein vom Statistikamt mit der Durchführung der Wahlstatistik zu betrauender Bediensteter wohne, nicht berücksichtigt werden, weil dies im Hinblick auf die „nach rein statistischen Gesichtspunkten“ zu treffende Auswahl der Wahlbezirke „eine sachfremde Erwägung wäre“. Nur: Die amtliche Statistik kann nur in den Grenzen des Rechts stattfinden. Bei der Durchführung von Wahlstatistiken, so habe ich erwidert, ist die Wahrung des Wahlgeheimnisses auch im innerstatistischen Bereich niemals eine „sachfremde Erwägung“. Und bei einer Stichprobengröße von höchstens 10 v. H. aller Wahlbezirke (§ 70 Abs. 2 Satz 2 LWO, bzw. 15 v. H. bei kommunalen Wahlstatistiken, § 72 Satz 2 LWO) ist es auch im Einzugsbereich der Stadt Kamenz als des Sitzes des Statistischen Landesamtes und zugleich einem Gebiet, das natürlich unter Regionalitätsgesichtspunkten ebenfalls in der Stichprobe vertreten sein muss, möglich, unter den in Frage kommenden Wahlbezirken auszuwählen bzw. den Personaleinsatz entsprechend zu steuern.

Eine andere, von einem Statistik-Fachmann des SMI ins Gespräch gebrachte Möglichkeit wäre eine Beschränkung der Erhebung auf eine 95 %-Stichprobe, was einfach darauf hinausliefe, 5 % ungekennzeichnete Stimmzettel unter die hinsichtlich Altersgruppe und Geschlecht gekennzeichneten Stimmzettel zu mischen.

Der praktische Effekt einer solchen Lösung, also der Beschränkung der Erhebung auf eine 95 %-Stichprobe, wird jedoch durch etwas anderes erreicht, sofern nicht ausnahmsweise eine Wahlbeteiligung von 100 % festzustellen ist: Das SMI hat nämlich mir gegenüber mit Recht darauf verwiesen, dass der Wahlstatistik nicht zu entnehmen ist, ob nicht ein in dem betreffenden Wahlbezirk Wahlberechtigter mithilfe eines schlichten Wahlscheines gemäß § 13 Abs. 3 SächsWahlG in einem anderen Wahlbezirk des Wahlkreises seine Stimme abgegeben hat oder ob er per Briefwahl gewählt hat. Die durch fehlende Erfassung sowohl der Briefwähler wie auch der Fälle des § 13 Abs. 3 SächsWahlG bedingte Ungenauigkeit der Statistik sichert also im Endeffekt das statistikbehördeninterne Wahlgeheimnis.

(4) Für rechtswidrig muss ich weiterhin den unverändert aus dem Entwurf übernommenen § 72 LWO halten, der Gemeinden, die über eine die Voraussetzungen des § 9 Abs. 1 SächsStatG erfüllende Statistikstelle verfügen, erlaubt, *mit Zustimmung des Landeswahlleiters* außer in den von diesem für die landesweite Wahlstatistik ausgewählten Wahlbezirken in weiteren Wahlbezirken für eigene statistische Zwecke reprä-

sentative Wahlstatistiken durchzuführen (mit einer Stichprobenobergrenze von 15 v. H. der im Gemeindegebiet gelegenen Wahlbezirke): Einiges spricht dafür, dass diese Regelung schon gegen § 51 Abs. 2 Satz 1 SächsWahlG verstößt, der bestimmt, dass es der Landeswahlleiter (im Einvernehmen mit dem Statistischen Landesamt) ist, der die Wahlbezirke bestimmt, in denen die Statistik durchgeführt wird. § 72 Satz 1 LWO sieht demgegenüber vor, dass der Landeswahlleiter nicht bestimmt, sondern nur zustimmt. Das heißt, der Landeswahlleiter kann nach dieser Regelung nur negativ, nicht aber positiv entscheiden, also nicht eigentlich *bestimmen*. Das SMI hat demgegenüber zwischen einem Bestimmungsrecht und einem Zustimmungs-Erfordernis nicht so genau unterscheiden wollen. Vor allem hat das Ministerium aber kein Argument gegen meinen Hinweis darauf vorgebracht, dass § 72 LWO zumindest in folgender Hinsicht gegen höherrangiges Recht verstößt: Wie dem Sächsischen Statistikgesetz zu entnehmen ist, gilt für die Durchführung von Statistiken durch Kommunen der *Vorbehalt des Gesetzes* insofern, als diese einer - allgemeinen - gesetzlichen Ermächtigung bedürfen; denn diese Ermächtigung wird in § 8 SächsStatG ausgesprochen. Andernfalls hätte es des § 8 Abs. 1 SächsStatG nicht bedurft. Die Vorschrift ist in engem Zusammenhang mit § 6 Abs. 1 SächsStatG zu verstehen, der ein besonderer bereichsspezifischer Ausdruck des (verfassungsrechtlich gewährleisteten) Vorbehaltes des Gesetzes ist. Nun soll die Ermächtigung der Kommunen in § 72 LWO jedoch offensichtlich gerade *neben* derjenigen des § 8 SächsStatG stehen, und zwar schon deswegen, weil ersichtlich kein Satzungserfordernis bestehen soll. Daher bedarf die Ermächtigung des § 72 LWO als Ermächtigung gerade der Kommunen einer hinreichend deutlichen *gesetzlichen* Grundlage. Eine solche ist in § 51 Abs. 2 Satz 1 SächsWahlG jedoch nicht zu erkennen. Kurz: § 72 LWO verstößt gegen § 8 SächsStatG, weil dem Sächsischen Wahlgesetz eine dieser Vorschrift gleichwertige Ermächtigung der Kommune zur Durchführung kommunaler Wahlstatistiken nicht zu entnehmen ist. Auch sehen § 2 Abs. 1 Nr. 3 und Nr. 4 SächsStatG nicht den Fall vor, dass *einzelne* Kommunalstatistiken durch Rechtsvorschriften des Freistaates angeordnet oder auch nur erlaubt, also vorgesehen werden.

Damit ich recht verstanden werde: Es gibt keine zwingenden, verfassungsrechtlich begründeten Gründe gegen Kommunalstatistiken, wie sie § 72 LWO vorsieht. Nur hat der Verordnungsgeber ignoriert, dass er die ihm durch Landesgesetze gesetzten Grenzen insoweit überschritten hat.

(5) Gemäß § 42 Abs. 2 LWO hat die Gemeinde gegebenenfalls darauf hinzuweisen, in welchen Wahlbezirken des Gemeindegebietes eine Wahlstatistik nach §§ 70 oder 72 LWO durchgeführt wird. Dies dient der Transparenz, es beugt Befürchtungen in der Bevölkerung vor, die faktisch die Freiheit der Wahl beeinträchtigen könnten. Damit ist eine von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder schon

im Jahr 1995 erhobene Forderung erfüllt worden (vgl. den Abdruck der betreffenden Entschließung in 3/16.2.14 unter Nr. 1, im ersten Absatz). Vorzuziehen wäre allerdings, dieser Regelung nach dem Vorbild von Vorschriften wie § 3 Satz 4 WStatG, § 58 Abs. 2 Satz 5 LWahlG BW, § 55 Abs. 2 Satz 5 LWahlG ST, § 50 a Abs. 2 Satz 4 LWahlG MV Gesetzesrang zu verleihen.

Fazit: Hier sind Nachbesserungen erforderlich, ggf. auch solche durch den Gesetzgeber.

5.7.5 Schulstatistik: Auswirkungen des Vorbehaltes des Gesetzes; auf dem Weg zu einem bundesweiten Schülerregister?

Zweimal bin ich im Berichtszeitraum mit Fragen der Schulstatistik befasst gewesen; beide Male ist es darum gegangen, eine Verletzung des Verfassungsgrundsatzes des *Vorbehaltes des Gesetzes* zu vermeiden.

(1) Im Hinblick auf den Entwurf der dann im Jahr 2004 in Kraft getretenen Änderungen des Schulgesetzes habe ich zu der Möglichkeit, im Gesetz zum Erlass von Rechtsverordnungen zu ermächtigen, mit denen Schulstatistiken angeordnet werden, u. a. Folgendes geltend gemacht:

(1.1) Aus § 6 Abs. 2 SächsStatG - wie aus seinem Vorbild § 5 Abs. 2 BStatG - kann man nicht folgern, dass die verfassungsrechtlichen Anforderungen an Verordnungsermächtigungen, also die in Art. 75 Abs. 1 Satz 1 und 2 SächsVerf, Art. 80 Satz 1 und 2 GG enthaltenen Folgerungen aus dem Verfassungsgrundsatz des *Vorbehaltes des (Parlaments-)Gesetzes* im Statistikrecht herabgesetzt wären.

Dasselbe gilt auch für § 6 Abs. 1 SächsStatG: Zwar sieht die Vorschrift vor, dass auch in einer untergesetzlichen Rechtsvorschrift, also in einer Verordnung, eine Landesstatistik angeordnet werden kann. Das besagt jedoch nichts anderes, als was selbstverständlich ist, nämlich dass der Gesetzgeber in einer gesetzlichen Vorschrift den Verordnungsgeber ermächtigen kann, die eigentliche Anordnung der Durchführung der Statistik selbst zu treffen. Auch damit werden jedoch nicht die allgemeinen Anforderungen an eine gesetzliche Vorschrift herabgesetzt, die den Verordnungsgeber zum Erlass einer Rechtsvorschrift ermächtigt, die Grundrechtseingriffe erlaubt.

Die Anforderungen, die kraft Verfassungsrechtes an gesetzliche Vorschriften zu stellen sind, in denen der Verordnungsgeber ermächtigt wird, die Durchführung von Statistiken anzuordnen, kann man § 109 SGB XI entnehmen, also einer Vorschrift über Pflegestatistiken, mitsamt der dazugehörigen Pflegestatistik-Verordnung vom 24. November 1999, BGBl. I S. 2282. Man sieht daran, dass der Gesetzgeber die Erhebungsmerkmale im Wesentlichen selbst nennen muss, sich also nicht auf eine allgemeine Themen-An-

gabe wie etwa z. B. „schul- und ausbildungsbezogene Tatbestände“ beschränken darf. Auch die Frage der Auskunftspflicht, einschließlich der Bestimmung des verpflichteten Personenkreises, hat, wie § 109 Abs. 1 Satz 3, Abs. 2 Satz 3 SGB XI zeigt, im Wesentlichen der Gesetzgeber zu regeln. Beides sind nämlich die wesentlichen Gesichtspunkte für den Grundrechtseingriff.

(1.2) Vorsorglich habe ich ferner darauf hingewiesen, dass die statistischen Erhebungen an den Schulen nicht durch Lehrer oder andere Bedienstete der Schulverwaltung durchgeführt werden dürften, sondern ausschließlich durch Bedienstete bzw. Erhebungsbeauftragte des Statistischen Landesamtes. Dies folgt, soweit es wie hier um Primärstatistiken, also um von vornherein zu statistischen Zwecken erhobenen Daten geht, aus dem Grundsatz der Trennung von Statistik und Verwaltungsvollzug (BVerfGE 65, 1, 61), einer Ausprägung des das Datenschutzrecht beherrschenden Zweckbindungsgrundsatzes (vgl. BVerfGE a. a. O. S. 46). Deswegen kämen als Ersatz allenfalls gemäß § 4 Abs. 1 SächsStatG besondere Erhebungsstellen innerhalb der Schulverwaltung in Frage, die räumlich, organisatorisch und personell abzutrennen wären und der Fachaufsicht des Statistischen Landesamtes unterstünden. Die Maßstäbe, die sich § 9 Abs. 1 und 2 SächsStatG entnehmen lassen, geben an, wie eine solche räumliche, organisatorische und personelle Abtrennung auszusehen hätte.

Diese Ausführungen haben das SMK allem Anschein nach nicht unbeeindruckt gelassen.

(2) Von geringerer datenschutzrechtlicher Sensibilität war ein Schreiben des Statistischen Landesamtes an das SMK, in dem dieses aufgefordert wurde, seine Bedenken gegen „die Weiterentwicklung der schulstatistischen Verfahren zu einer modernen Schulstatistik“ aufzugeben, weil sich doch „die Anforderungen an die amtliche Schulstatistik zur Bereitstellung neuer oder ergänzender Daten für überregionale und internationale Zwecke in den letzten Jahren erhöht“ hätten. Das Schreiben bemühte auch die Autorität der Kultusministerkonferenz und ferner das Vorbild anderer statistischer Landesämter, die die Schulstatistik bereits auf die Erhebung von Einzeldatensätzen zu jedem einzelnen Schüler (und wohl auch Lehrer) umstellten. Kurz: Das Statistische Landesamt hat das Kultusministerium aufgefordert, ihm (insbesondere) schülerbezogene Einzeldatensätze zu übermitteln.

(2.1) Ich habe daraufhin gegenüber dem Statistischen Landesamt, dem SMI als dessen Aufsichtsbehörde und dem SMK Folgendes geltend gemacht: Als Verarbeitung personenbezogener Daten bedarf die Durchführung von Schulstatistiken einer gesetzlichen Grundlage (vgl. auch § 2 Abs. 1 Nr. 3 Buchst. a, § 6 Abs. 1, Abs. 6 SächsStatG). Grundlage der Schulstatistik ist nach sächsischem Recht unverändert ausschließlich § 7

Abs. 1 SächsStatG: Es handelt sich ausschließlich um *Statistik im Verwaltungsvollzug*, insbesondere also ausschließlich um Sekundärstatistik. Das Ausmaß der erlaubten Nutzung der bei Durchführung des Schulgesetzes anfallenden personenbezogenen Daten bestimmt diese Vorschrift: Die Daten dürfen zu statistischen Zwecken insoweit genutzt werden, wie dies der Erfüllung der Aufgaben der öffentlichen Stelle, in deren Geschäftsgang die Daten angefallen sind, oder der jeweils übergeordneten öffentlichen Stelle *dienlich* ist. Da Aufgabe des SMK die Gesamt-Gestaltung ist, sowohl in aufsichtlicher wie in planerischer Hinsicht, markiert der daraus für dieses entstehende Bedarf an personenbezogenen Daten die Grenzen, in denen § 7 Abs. 1 SächsStatG die Weitergabe der Daten innerhalb der Schulbehörden ‚nach oben' sowie ihre Nutzung zu statistischen Zwecken erlaubt. Statistik als Selbstzweck oder als Sammlung von Daten für die Zwecke Dritter, jenseits von Berichtsaufgaben des Freistaates Sachsen, gehören nicht dazu.

Auch die (vom Willen des SMK abhängige!) Übertragung statistischer Aufbereitungen von *Statistiken im Verwaltungsvollzug* auf das Statistische Landesamt ist von Rechts wegen auf Auswertungen beschränkt, die sich im Rahmen dessen halten, was dem SMK im erläuterten Sinne *zu dessen Aufgabenerledigung dienlich* ist.

Ich habe daher nur folgern können, dass das besagte Schreiben des Statistischen Landesamtes an das SMK jeden Ansatz einer Überlegung zur rechtlichen Zulässigkeit der angestrebten „Umstellung der vom Statistischen Landesamt durchgeführten Schulstatistik auf Individualdaten" hat vermissen lassen.

(2.2) Das SMK hat mir daraufhin dargelegt, dass es sich dem erheblichen Druck von Beschlüssen der Kultusministerkonferenz ausgesetzt sieht, die daraus hinauslaufen, dass

- auf Landesebene in einer Datei für jeden Schüler und jeden Lehrer ein umfangreicher Datensatz angelegt wird, in dem die Person jeweils durch eine für sie vergebene Nummer identifiziert wird, was auf ein pseudonymisiertes Register hinausläuft, und dass
- diese Länderdateien überdies zu einer bundesweiten gemeinsamen Datenbank zusammengefasst werden sollen.

Die Vorstellungen der Kultusministerkonferenz von einer Notwendigkeit einer „Sicherstellung eines einheitlichen Aufkommens schulstatistischer Daten für überregionale und internationale Zwecke … für die Koordinierung politischer und planerischer Maßnahmen sowie für die internationale Zusammenarbeit auf dem Gebiet des Schulwesens" werden im SMK allem Anschein nach so nicht ohne weiteres geteilt. Das ist datenschutzrechtlich gut so.

(2.3) Es ist, nach dem oben ausgeführten, klar, was nötig wäre, um dieses Vorhaben rechtmäßig werden zu lassen:
In jedem Bundesland müsste durch Schulstatistikgesetz eine Erhebung und Speicherung sowie statistische Nutzung der Daten angeordnet werden (u. a. Verkehrssprache in der Familie; Jahr des Zuzuges nach Deutschland und Geburtsland; Geburtsmonat; Geburtsland des Vaters; Geburtsland der Mutter - alles Daten, die im Verwaltungsvollzug nicht anfallen).

Für die Zusammenlegung der Datensammlung zu einer bundesweiten Datei gäbe es selbst bei einer Grundgesetzänderung mit Übertragung des Schulwesens auf den Bund nicht die nötige Grundlage. Denn selbst dann verhinderte das aus dem Verhältnismäßigkeitsgrundsatz (Verfassungsgebot als Teil des Rechtsstaatsprinzips!) folgende Gebot der *frühestmöglichen statistikunschädlichen Anonymisierung* (vgl. § 1 Abs. 2 SächsStatG) der Daten, dass es erlaubt wäre, alle Datensätze bundesweit unaggregiert in eine Datenbank zu stellen. Bei bundesweiter Auswertung wäre schon die Zuordnung der Daten zu einzelnen Schulen, ja Klassen - was auf Landesebene vielleicht noch sinnvoll sein könnte, nicht mehr statistiknützlich. Außerdem bedürfte es eines Gesetzes über die Schulstatistik als Bundesstatistik, mit Verarbeitung in der Endstufe durch das Statistische Bundesamt.

Soweit Daten im Verwaltungsvollzug nicht anfallen, müssten sie von den statistischen Landesämtern bei den Schülern bzw. ihren Eltern unmittelbar erfragt werden.

In Anbetracht des gerade auf die amtliche Statistik einwirkenden Kostendruckes mutet das Vorhaben merkwürdig an. Anders als bei der Rechtschreibreform wird dieses Unternehmen der Kultusministerkonferenz sogar vom Bundesverfassungsgericht (vgl. Urteil vom 14. Juli 1998 - 1 BvR 1640/97, NJW 1998, 2525 mit SächsOVG 28. Oktober 1997 - 2 S 610/97, SächsVBl. 1997, 298!) nicht außerhalb des Geltungsbereiches des Verfassungsgrundsatzes des *Vorbehaltes des Gesetzes* gesehen werden können.

Ich werde daran arbeiten, dass die landesweiten (pseudonymisierten) Schüler- und Lehrerregister und gar das bundesweite (pseudonymisierte) Schüler- und Lehrerregister nicht zustande kommen.

5.7.6 Beteiligung eines sächsischen Hochschulforschers an einer unzulässigen (amtlichen) Statistik einer außersächsischen Hochschule

Ende des Jahres 2003 bin ich darauf aufmerksam gemacht worden, dass an einer Hochschule in Mecklenburg-Vorpommern von der Hochschulverwaltung unter dem Motto „Gesunde Hochschule“ eine Befragung zum Gesundheitszustand und zu gesundheitserheblichen Verhaltensweisen von Bediensteten und Studierenden der Hochschule

durchgeführt wurden. Im Rahmen einer freiwilligen Fragebogenaktion zur angeblichen „Erfassung des Gesundheitszustandes“ wurden mittels des mir vorliegenden 19-seitigen (!) Fragebogens umfangreich Daten zu Tätigkeiten erhoben, die außerhalb des Hochschulbetriebes stattfinden, wie z. B. Alkohol- und Drogenkonsum, Geschwindigkeitsüberschreitungen im Straßenverkehr und häusliches Zähneputzen; auch wurden in erheblichem Maße Daten zum Sexualverhalten erfragt, so z. B. zur Anzahl der Sexualpartner, Methoden der Empfängnisverhütung, angewandten Sexualpraktiken und vieles mehr. Angaben des Teilnehmers zu Alter, Geschlecht, Körpergröße, Familienstand, Anzahl der Kinder, Wohnsituation, Schulbildung, Krankenkasse und in Bezug auf die Bediensteten auch die Dauer des Beschäftigungsverhältnisses an der Hochschule waren ebenfalls Gegenstand der Befragung.

Da die Befragung in Zusammenarbeit mit einem sächsischen Hochschulwissenschaftler erfolgte, dem die Auswertung der ausgefüllten Fragebögen übertragen worden war, war meine Zuständigkeit berührt:

Gemäß § 2 Abs. 1 SächsDSG bin ich für die Verarbeitung personenbezogener Daten durch der Aufsicht des Freistaates Sachsen unterstehende juristische Personen des öffentlichen Rechts zuständig, also auch im Falle der Verarbeitung personenbezogener Daten durch Universitäten. Was die Erhebung personenbezogener Daten durch mit der Aufgabe wissenschaftlicher Forschung betraute öffentliche Stellen bzw. deren Bedienstete zu Forschungszwecken angeht, habe ich allerdings nur zu prüfen, ob der Forscher sich die Daten auf eine rechtlich einwandfreie Weise selbst beschafft hat, vor allem auf der Grundlage wirksamer Einwilligungserklärungen, oder ob bei der Ausnutzung von Beschaffungsmöglichkeiten, über die ein Dritter verfügt, dieser bei der Erhebung der Daten rechtmäßig handelt. Dies letztere, was man auch gewissermaßen als Verbot der Datenhehlerei öffentlicher Stellen bezeichnen könnte, lehnt sich an den Rechtsgedanken des § 13 Abs. 1 Nr. 1 SächsDSG an: Die Rechtmäßigkeit der Weiterverarbeitung hängt von der Rechtmäßigkeit der Erhebung der Daten ab.

Die Verarbeitung der im Zusammenwirken mit der außersächsischen Hochschule erhobenen Daten durch den sächsischen Hochschulforscher habe ich als rechtswidrig bemängelt, da bereits die Befragung der Bediensteten und der Studenten durch die Hochschulleitung mangels der insoweit erforderlichen Rechtsgrundlage rechtswidrig gewesen ist.

Bei der Befragung handelte es sich seitens der Hochschulverwaltung rechtlich gesehen um die Durchführung einer amtlichen Statistik. Denn zur Gewinnung von Erkenntnissen über Massenerscheinungen wurden Daten („Einzelangaben“ im Sinne der statistikrechtlichen Terminologie) gesammelt, aufbereitet, erhoben, dargestellt und analysiert (vgl.

z. B. § 1 Abs. 1 SächsStatG). Für die Anwendbarkeit des Statistikrechts reicht bereits ein ausgesprochen schwacher Personenbezug der Einzelangaben aus. Der Begriff der *Einzelangabe* im Statistikrecht ist weiter als der datenschutzrechtliche Grundbegriff des *personenbezogenen Datums*; das Statistikrecht erfasst auch Datenerhebungen mit von vornherein sehr, wenn nicht äußerst hohem Anonymisierungsgrad. Hinzu kam, dass es die im Fragebogen genannten Merkmale manchem ermöglichten, aus der Kombination der jeweils angegebenen Merkmalsausprägungen ohne allzu großen Aufwand auf den konkreten Hochschulmitarbeiter zu schließen.

Zwar findet das Statistikrecht natürlich insoweit keine Anwendung, als nicht die Hochschule als solche, insbesondere die Hochschulverwaltung (Kanzler), öffentliche Gewalt ausübt, sondern einzelne Hochschulmitarbeiter (unter Anwendung statistischer Methoden) forschen. Dies ist namentlich dann der Fall, wenn bei der Datenerhebung nicht an die Eigenschaft des Betroffenen, Hochschulangehöriger zu sein, angeknüpft wird. Für die rechtliche Einordnung ist dabei das objektive Erscheinungsbild der Handlung maßgeblich. Dieses Erscheinungsbild war bei der mir bekannt gewordenen Untersuchung eindeutig: Die Hochschule wandte sich als solche an ihre Bediensteten, sprach diese gerade in ihrer Stellung als Hochschulangehörige an. Sie handelte demgemäß als Träger öffentlicher Gewalt und nicht im Rahmen freier Forschung. Ich habe dies bereits ausführlich in 10/5.7.2 erörtert.

Bei der Datensammlung der Hochschule handelte es sich demnach um eine amtliche Statistik. Eine Hochschule darf als juristische Person des öffentlichen Rechts nach allgemeinem Datenschutzrecht bzw. nach Statistikrecht zwar Sekundärstatistiken, also Statistiken im Verwaltungsvollzug, durchführen. Das Mecklenburg-Vorpommernsche Landesstatistikgesetz hat die dortige Hochschule jedoch nicht ermächtigt, wie hier geschehen eine Primärstatistik zu erstellen. Einer gesetzlichen Erlaubnis zur Durchführung der Statistik bedarf es auch dann, wenn, wie es hier der Fall war, das Ausfüllen des Erhebungsbogens nicht zur Pflicht gemacht, sondern die Teilnahme der Befragung vielmehr ausdrücklich für freiwillig erklärt wird. Auch wenn nach dem jeweils anzuwendenden Statistikgesetz - anders als z. B. nach sächsischem Recht - auf freiwilliger Grundlage durchgeführte Statistiken keiner Anordnung durch Rechtsvorschrift bedürfen, enthält eine solche Regelung noch nicht die notwendige Ermächtigung bzw. Zuständigkeit der Hochschule zur Erstellung von Primärstatistiken.

Hinzu kam: Selbst wenn die Hochschule (nach jeweiligem Landesrecht) befugt gewesen wäre, Primärstatistiken in dem Maße durchzuführen wie Kommunen, wäre die hier in Streit stehende Erhebung rechtswidrig gewesen. Denn die Beobachtung und Hebung des Gesundheitszustandes der Bediensteten oder Studierenden gehört zumindest nach den herkömmlichen Hochschulgesetzen nicht zu den Aufgaben einer Hochschule, zumindest

soweit Tätigkeiten betroffen sind, die nach geltendem Recht außerhalb des Hochschulbetriebes stattfinden wie Drogenkonsum, Geschwindigkeitsüberschreitungen im Straßenverkehr, häusliches Zähneputzen oder Geschlechtsverkehr. (Es wäre auch nicht „gesund“, wenn ein Staat, der finanziell große Mühe hat, die Hochschulen mit den nötigen Gebäuden, Geräten und Personal auszustatten, sich in solcher Weise als „gesundheitsfördernde Hochschule“ um das Privatleben der Hochschulbediensteten und der Studenten kümmerte. Datenschutz ist geeignet, sichtbar zu machen, wenn öffentliche Stellen Allotria treiben.)

Eine gesetzliche Ermächtigung in einem anderen Gesetz war für mich ebenso nicht erkennbar. Eine entsprechende Datenerhebung durch die Hochschule ließ sich insbesondere auch nicht auf das Landesdatenschutzgesetz stützen. Namentlich auch die in den Datenschutzgesetzen geregelte Einwilligung des Betroffenen konnte nicht als Rechtsgrundlage herangezogen werden. Da es sich bei der vorliegenden Datensammlung - wie dargelegt - um eine amtliche Statistik handelte, war das Statistikgesetz das speziellere Gesetz, das dem Datenschutzgesetz als dem allgemeineren Gesetz vorging. Die strengeren Anforderungen des Statistikgesetzes (keine Primärstatistiken durch Hochschulen bzw. Bindung an die Dienlichkeit für die Erfüllung der Körperschaft durch geltendes Recht übertragener Aufgaben) dürfen insoweit nicht durch die Anwendung des Datenschutzgesetzes (Primärstatistiken durch Hochschulen bei Einwilligung der Betroffenen) umgangen werden. Aber auch unabhängig davon können Einwilligungen die nötigen gesetzlichen Aufgabenzuweisungen nicht ersetzen (Verfassungsgrundsatz des Vorbehaltes des Gesetzes).

Auch eine Beurteilung nach sächsischem statt mecklenburg-vorpommerischem Recht, die man zugunsten der durch die TU Dresden stattfindenden Verarbeitung personenbezogener Daten wohl hätte erwägen müssen, hätte zu keinem anderem Ergebnis geführt.

Der sächsische Hochschulforscher hat „die Rechtsauffassung des Sächsischen Datenschutzbeauftragten zur Richtschnur seines Handelns“ genommen: Es wurden von seiner Seite aus keine Ergebnisse der Befragungen an die betroffene Hochschulleitung mitgeteilt. Mit den bereits aggregierten Daten hat er wissenschaftlich weiterarbeiten dürfen.

5.7.7 Hinweise zur Kommunalstatistik

Aus gegebenen Anlass, nämlich Erfahrungen mit verbreiteten Fehl-Vorstellungen, folgende Hinweise für Gemeinden, die Rechtsgrundlagen für die Durchführung von Kommunalstatistiken schaffen wollen:

(1) Die Einrichtung einer kommunalen Statistikstelle bedarf, wie § 9 Abs. 1 bis 3 SächsStatG zeigt, keiner Satzung.

Es bedarf lediglich einer förmlichen Dienstanweisung gemäß § 9 Abs. 3 SächsStatG, die den Vorgaben des Gesetzes (§ 9 Abs. 1, 2 und 4) entspricht.

(2) Für Satzungen, die gemäß § 9 Abs. 6 Satz 3 SächsStatG regelmäßige Weitergaben personenbezogener Daten aus dem Geschäftsgang von Verwaltungsstellen der Gemeinden an die kommunale Statistikstelle vorsehen, gelten die inhaltlichen Anforderungen des § 6 Abs. 6 SächsStatG (§ 9 Abs. 6 Satz 4 SächsStatG). Dies entspricht dem, was auch im staatlichen Bereich für die Anordnung von Statistiken in Verwaltungsvollzug aufgrund des Verfassungsgrundsatzes des *Vorbehaltes des Gesetzes* gilt, nämlich, dass der Gesetzgeber selbst die Statistik anordnen muss, wenn sie regelmäßig und zweckändernd und nicht nur, wie in § 7 Abs. 1 SächsStatG vorausgesetzt, ausschließlich für die Erfüllung eigener Aufgaben oder von Aufgaben der übergeordneten öffentlichen Stelle durchgeführt wird.

(3) In Satzungs-Vorschriften, in denen Primärstatistiken (vgl. § 8 Abs. 1 SächsStatG) oder regelmäßige Weitergaben gemäß § 9 Abs. 6 Satz 1 und 3 SächsStatG vorgesehen werden, müssen insbesondere sämtliche Erhebungsmerkmale aufgezählt werden. Die Dienlichkeit der Daten für die Aufgabenerfüllung durch die Gemeinde muss erkennbar sein.

(4) Bei der Erarbeitung von Entwürfen solcher Satzungen sollten Regeln, die sich bereits aus dem Sächsischen Statistikgesetz ergeben, in der Satzung nicht noch einmal wiederholt werden: Dies macht die Satzung unübersichtlich und birgt die Gefahr, dass durch unvollständige Übernahme gesetzlicher Regelungen die Satzung so ausgelegt werden kann - wenn nicht muss -, dass die nicht übernommenen Regelungen gerade nicht gelten sollen, was dazu führte, dass die Satzung wegen Verstoßes gegen höherrangiges Recht teilweise nichtig wäre.

5.7.8 Beschwerden gegen die Dienstleistungsstatistik

Mehrfach wurde ich von Petenten um Prüfung der Datenerhebung des Statistischen Landesamtes im Rahmen der Durchführung der Dienstleistungsstatistik gebeten.

Auf der Grundlage des 2001 in Kraft getretenen, der zunehmenden wirtschaftlichen Bedeutung der Dienstleistungen Rechnung tragenden Dienstleistungsstatistikgesetzes führen die Statistischen Landesämter jährlich in verschiedenen Dienstleistungsbereichen repräsentative Erhebungen über die wirtschaftliche Tätigkeit gewerblicher *Unternehmen bzw. Einrichtungen zur Ausübung einer freiberuflichen Tätigkeit* (§ 2 Abs. 2 Dienstleistungsstatistikgesetz) durch, wobei die Unternehmen bzw. Einrichtungen für die Stichprobe mittels eines mathematisch-statistischen Verfahrens ausgewählt werden. Auch Rechtsanwälte, die so in die Erhebung einbezogen worden waren, sahen durch die

Pflicht zum Ausfüllen des vom Statistischen Landesamt übersandten Erhebungsbogens, u. a. unter Angabe des Namens sowie der Anschrift ihrer Kanzlei, ihre „Datenanonymität“, wie einer von ihnen formuliert hat, nicht ausreichend gewährleistet.

Die Bedenken der Rechtsanwälte, deren Eingaben zeigten, dass auch unter Fachanwälten für Verwaltungsrecht mit universitärem Lehrauftrag Grundkenntnisse des Datenschutzrechtes nicht immer als präsent vorausgesetzt werden können, waren unbegründet:
Das Statistische Landesamt macht durch die Anforderung von Daten mittels des auszufüllenden Erhebungsbogens von einer Befugnis Gebrauch, die ihm durch das Dienstleistungsstatistikgesetz sowie ergänzend das Bundesstatistikgesetz eingeräumt ist und die das Statistische Landesamt insbesondere berechtigt, vom Auskunftspflichtigen die Daten auch in einer Form zu erheben, bei der Name und Anschrift erkennbar bleiben. Dies ist mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar: Nach dem grundlegenden, ja gerade das Statistikrecht betreffenden Volkszählungsurteil des Bundesverfassungsgerichts (vom 15. Dezember 1983, E 65,1 ff., NJW 1984, 419 ff.) gewährt das aus Artikel 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abzuleitende Grundrecht auf informationelle Selbstbestimmung keinen Anspruch darauf, dass Daten nur in einer Form erhoben werden, die den Auskunftgebenden und damit die Person, auf die sie sich beziehen, nicht erkennen lässt. Zu den Schranken, die das Bundesverfassungsgericht dem - auch vom Gericht nicht in Frage gestellten - Recht des Staates, für statistische Zwecke Daten zu erheben, gezogen hat, gehört gerade *nicht* das Verbot, Daten nur mittels eines Verfahrens zu erheben, bei dem der Auskunftsverpflichtete von vornherein anonym bleibt. Mit anderen Worten: Für Zwecke der amtlichen Statistik dürfen gerade auch *personenbezogene* Daten erhoben werden. Als notwendige Sicherung des Rechts auf informationelle Selbstbestimmung bei der Weiterverarbeitung dieser Daten durch die öffentliche Gewalt fordert das Bundesverfassungsgericht vielmehr, neben der Wahrung des Statistikgeheimnisses nach außen, nur Vorkehrungen bei der Durchführung und Organisation der Datenerhebung und -verarbeitung einschließlich Trennungs- bzw. Löschungsregelungen (dies aber wiederum nur, soweit die erhobenen Daten nicht z. B. für bundesstatistische Zwecke, hier: zum Aufbau und zur Führung des Statistikregisters, weiter benötigt werden und verwendet werden dürfen) für die im Statistikrecht „Hilfsmerkmale“ genannten (vgl. §§ 10 Abs. 1, 12 BStatG, §§ 12 Abs. 1 und 2, 14 SächsStatG) Identifikationsmerkmale, mittels deren die Person des Auskunfterteilenden unmittelbar festgestellt werden kann und die im die jeweilige Statistik anordnenden Gesetz eigens genannt sein müssen (hier: § 4 Dienstleistungsstatistikgesetz). („Hilfsmerkmale“ deswegen, weil es den Statistikern auf das Individuum als solches letztlich gar nicht ankommt, sondern nur auf die „Erhebungsmerkmale“, die es - in Kombination - aufweist, also z. B. sein Alter, sein Geschlecht, sein Einkommen, seinen

Familienstand, seine Bildungsabschlüsse; die Hilfsmerkmale helfen aber, an die Erhebungsmerkmale heranzukommen und die Merkmalsausprägungen einer Person als Einheit zusammenzuführen.) Wenn jedoch die Trennung und - in der Regel - die spätere Löschung der Identifikationsmerkmale verlangt wird, dann folgt daraus geradezu, dass die Erhebung der Daten in einer Weise zulässig ist, welche es ermöglicht, die Person des Auskunfterteilenden festzustellen.

5.8 Archivwesen

5.8.1 Wahrung der Befugnisse der staatlichen Archivverwaltung bei der vorweggenommenen generalisierenden Entscheidung über die Archivwürdigkeit der ihr anzubietenden Unterlagen und: Verstoß gegen § 26 SächsDSG

Nach § 5 Abs. 1 Satz 1 und 2 SächsArchivG haben alle öffentlichen Stellen des Freistaates Sachsen dem Sächsischen Staatsarchiv alle Unterlagen zur Übernahme anzubieten, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen. Vorbehaltlich durch Rechts- oder Verwaltungsvorschriften besonders bestimmter längerer Aufbewahrungsfristen entsteht diese Anbietungspflicht spätestens 30 Jahre nach Entstehung der Unterlagen. (Für die Kommunalverwaltung und die Hochschulen sieht das Sächsische Archivgesetz keine Anbietungspflicht vor, vgl. § 13 Abs. 3, § 14 Abs. 2, mangels Verweisung auf § 5 Abs. 1 SächsArchivG. Anderes gilt gemäß § 15 für die sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechtes.)

Nach § 5 Abs. 4 entscheidet die zuständige staatliche Archivbehörde, seit dem 1. Januar 2005 das Sächsische Staatsarchiv, im Benehmen mit der anbietenden Stelle innerhalb von sechs Monaten über die Archivwürdigkeit der Unterlagen. Lässt sie diese Frist verstreichen, ist die Stelle, die ihre Unterlagen angeboten hat, nicht mehr zur Aufbewahrung verpflichtet, sofern nicht Rechtsvorschriften oder schützwürdige Belange der Betroffenen - also derjenigen, auf die sich die Unterlagen beziehen - entgegenstehen (§ 5 Abs. 5 Satz 3 SächsArchivG).

Datenschutzrechtlich bedeutet das: Sofern nicht ausnahmsweise eine längere Aufbewahrungsfrist vorgesehen ist, ist nach spätestens 30 Jahren zu entscheiden, ob die in den Unterlagen enthaltenen personenbezogenen Daten zu einer zweckändernden Speicherung, gegebenenfalls auch Nutzung oder Übermittlung, an die Archive übermittelt werden und dann bei der abgebenden Stelle nicht mehr vorhanden sind, weil die Datenträger ohne Anfertigung von Kopien haben übergeben werden müssen. Andernfalls sind die Daten, außer im Fall der in § 5 Abs. 5 Satz 2 vorgesehenen Ausnahme, mangels eines Grundes für ihre fortgesetzte Speicherung zu löschen, wie sich aus § 20 Abs. 1

bis 3 SächsDSG ergibt (vorbehaltlich der in § 5 Abs. 1 Satz 2 und Abs. 5 Satz 2 vorgesehenen Ausnahmetatbestände, § 20 Abs. 4 SächsDSG).

Die Entscheidung darüber, ob Unterlagen bzw. Daten den Weg in das „Datenendlager" Archiv gehen oder, vorbehaltlich der genannten Ausnahmefälle einer ausnahmsweisen fortgesetzten Speicherung in der Ursprungsstelle, vernichtet werden, überträgt das Gesetz in § 5 Abs. 4 Satz 1 der Archivbehörde.

Angesichts der Massen von Unterlagen, die in der Arbeit der öffentlichen Stellen des Freistaates entstehen, ist es verständlich, ja geboten, dass sich die beteiligten Stellen des Freistaates bemühen, diese Entscheidung zwischen Übergang ins Archiv, Löschung oder ausnahmsweiser fortgesetzter Aufbewahrung in der Ausgangsbehörde zu rationalisieren, vor allem, was vorhersehbare gleichartige und zugleich in größerer Menge anfallende Unterlagen betrifft.

Mittel dazu sind generelle verwaltungsinterne Anweisungen in Form von Verwaltungsvorschriften. Zu diesen bin ich, da die meisten Unterlagen ja einen Personenbezug aufweisen, gemäß § 26 SächsDSG anzuhören. Im Berichtszeitraum hat man mir Gelegenheit zur Stellungnahme zu Entwürfen der VwV des SMK über die Aufbewahrung und Aussonderung schulischer Unterlagen vom 7. Oktober 2004 (ABl. S. 1154) sowie der VwV des SMF über die Aufbewahrung und Aussonderung von Unterlagen der Finanzämter (vom 4. Januar 2005, veröffentlicht am 8. März 2005 im SächsMBl. SMF) gegeben.

Sowohl hinsichtlich der Verfahrensweise bei meiner Beteiligung als auch inhaltlich ist der Vorgang datenschutzrechtlich nicht in allem zufriedenstellend verlaufen.

(1) Stutzig machen musste und muss Abschnitt 4.1 Satz 5 der VwV des SMK, d. h. die Vorschrift, dass alle Unterlagen bestimmter (in einer Anlage der VwV aufgeführter) Kategorien „ohne Anbietung an das Archiv von der Schule selbständig zu vernichten" sind. (Entsprechendes gilt für Abschnitt III 3.1 der VwV des SMF.)

Als ich demgegenüber Anfang August 2004 geltend gemacht habe, dass das nach § 5 Abs. 1 Satz 1, Abs. 4 Satz 1 SächsArchivG nicht das SMK bzw. die Schulverwaltung entscheiden könne, hat mir das SMK mit Schreiben vom 15. Oktober 2004 mitgeteilt, es handele sich ja gar nicht um eine Entscheidung der Kultusverwaltung, sondern, auch und vor allem, um eine der Archivverwaltung, genauer gesagt des SMI. Denn das SMI sei ja „beteiligt", einschließlich „des Mitzeichnungsverfahrens". Es handele sich eben um eine antizipierte Entscheidung über Massenunterlagen, ein sog. archivisches „Bewertungsmodell".

Daraus war zu folgern, dass die Eingangsformel der VwV, wonach das SMK „im Einvernehmen mit dem Sächsischen Staatsministerium des Innern“ bestimme, irreführend ist, nämlich den Einfluss des SMI auf das Zustandekommen der VwV untertrieben darstellt.

Somit handelt es sich, das habe ich gern anerkannt, doch tatsächlich um eine vorweggenommene Pauschal-Entscheidung der Archivverwaltung (wobei, wie ich mich habe belehren lassen, für dergleichen seinerzeit nach dem alten § 3 Abs. 2 Satz 2 SächsArchivG noch das SMI zuständig gewesen und erst mit dem 1. Januar 2005 das Sächsische Staatsarchiv zuständig geworden ist).

Nur: Eine Entscheidung der zuständigen Archivbehörde stellt das Regelwerk nur dann dar, wenn diese, also jetzt das Sächsische Staatsarchiv, die Möglichkeit hat, seine Entscheidung jederzeit mit Auswirkung gegenüber der Schulverwaltung zu revidieren. Das wiederum wäre aber nur dann der Fall, wenn die zuständige Archivbehörde die VwV jederzeit durch einseitige Willenserklärung insoweit außer Kraft setzen könnte. Denn nur dann bestünde die in § 5 Abs. 1, Abs. 4 SächsArchivG vorausgesetzte fachliche Unabhängigkeit der Archivbehörde von der zur Anbietung verpflichteten Behörde. Darum hatte ich dies gegenüber SMK und SMI geltend gemacht und beide aufgefordert, bis zur Klärung der noch offenen Rechtsfragen die Unterzeichnung und die Inkraftsetzung der Verwaltungsvorschrift zurückzustellen. Da musste ich im Amtsblatt lesen, dass VwV schon am 7. Oktober unterzeichnet und am 18. November 2004 im Amtsblatt veröffentlicht und damit in Kraft getreten war.

(2) Das bedeutete: Das SMK hatte erst am 15. Oktober 2004 zu meinen Schreiben vom 4. August 2004 Stellung genommen und sich darauf beschränkt, darzulegen, aus welchen Gründen es die von mir vertretene Rechtsauffassung nicht teilte; einen Hinweis darauf, dass die Verwaltungsvorschrift bereits am 7. Oktober bereits unterzeichnet worden war, hatte es jedoch unterlassen. Dadurch hat das SMK, wie ihm bewusst gewesen sein muss, den Eindruck erweckt, dass der Prozess des Austausches der Argumente für die jeweils vertretene Auffassung noch nicht abgeschlossen war und somit für mich weiterhin die Möglichkeit bestand, auf eine Verfahrensweise hinzuwirken, die nicht gegen das Sächsische Archivgesetz verstoßen würde. Dementsprechend hatte ich ja die im Schreiben des SMK vom 15. Oktober 2004 vorgebrachten Argumente erwogen und meine Rechtsauffassung insoweit geändert, als ich die Möglichkeit einer antizipierten Entscheidung über die Archivwürdigkeit nach § 5 Abs. 4 Satz 1 SächsArchivG für grundsätzlich zulässig erachtet und das Vorliegen der Voraussetzungen einer solchen Entscheidung geprüft habe. Zu der befremdenden Vorgehensweise, in erster Linie des *SMK*, habe ich angemerkt, dass das Institut der Anhörung nach § 26 SächsDSG nicht als bloße Formalie zu begreifen ist, sondern dass sich nach dieser

Vorschrift die Behörde mit von mir geäußerten datenschutzrechtlichen Bedenken auseinanderzusetzen hat, *bevor* sie die in Frage stehende Verordnung oder Verwaltungsvorschrift erlässt. Das heißt: Hält eine Behörde meine Bedenken nicht für begründet, ist sie verpflichtet, mir gegenüber dazu Stellung zu nehmen, bevor sie die Rechtsverordnung oder die Verwaltungsvorschrift in unveränderter Form veröffentlicht.

(3) Ein Argument gegen meinen Einwand, dass die Archivverwaltung durch die gewählte Konstruktion der VwV als einer VwV allein des SMK bzw. des SMF ihrer vom Archivgesetz verlangten Freiheit der Entscheidung über die Archivwürdigkeit beraubt werde, was eben gegen Gesetzesrecht verstößt, ist dem SMK und dem SMF, die sich nicht mehr geäußert haben, aber auch dem SMI nicht eingefallen. Denn der in dessen (immerhin *vor* der Unterzeichnung der VwV des SMF ergangenen) Antwort an mich als Erwiderung formulierte Hinweis, dass derartig vorweggenommene Pauschalentscheidungen sinnvoll und dass man verstärkt zu ihnen übergehen wolle, ist ganz offensichtlich *kein* solches Argument. Vielmehr: Man muss sich rechtlich etwas einfallen lassen. Die einseitige Außerkraftsetzung einer z. B. für die Schulverwaltung oder für die Finanzbehörden geltenden Verwaltungsvorschrift durch das SMI oder genauer gesagt die zuständige Archivbehörde (also jetzt das Sächsische Staatsarchiv) wird sich juristisch wohl nicht bewerkstelligen lassen. Ausreichen könnte aber vielleicht eine Verwaltungsvereinbarung zwischen Archivbehörde und Fachministerium, die dieses verpflichtet, auf erstes Anfordern der Archivbehörde seine VwV insoweit aufzuheben.

5.8.2 Nutzung archivierter Personalakten für Nachrufe oder ähnliche Ehrungen

Öfter stellt sich die Frage, ob archivierte Personalakten früherer Inhaber herausgehobener Ämter, z. B. Bürgermeister, von Verwaltungsstellen genutzt werden dürfen, um eine Trauerrede oder Ähnliches auszuarbeiten.

Bei der Entscheidung, ob das Archiv als Behörde Einsicht in die Personalakten gewähren darf, sind die Schutzfristen des § 10 SächsArchivG zu beachten, und zwar insbesondere die dem Persönlichkeitsrechtschutz dienenden Schutzfristen des § 10 Abs. 1 Satz 3 SächsArchivG. Gemäß dieser Vorschrift dürfen, unbeschadet der allgemeinen Schutzfristen, Akten und Daten, die sich auf eine natürliche Person beziehen, also personenbezogenes Archivgut, erst zehn Jahre nach dem Tod der betroffenen Person Dritten zugänglich gemacht werden. Diese Schutzfrist gilt gemäß § 10 Abs. 2 Satz 3 SächsArchivG insoweit nicht, als der Inhalt der Unterlagen sich auf *Amtsträger in Ausübung ihrer Ämter* bezieht. Unter diese letztere Vorschrift fallen Personalakten jedoch nicht, und auch die Personalakten z. B. eines Bürgermeisters betreffen diesen

nicht in der *Ausübung seines Amtes*, sondern in seinem sogenannten Grundverhältnis zu seiner Gemeinde als Körperschaft, zu der er in einem Dienstverhältnis gestanden hat.

Diese gesetzliche Regelung leuchtet, wenn man die praktischen Folgen betrachtet, auch ein: Alles, was der Verstorbene zu Gunsten oder auch zum Schaden seiner Gemeinde in Ausübung seines Amtes getan hat, kann den zugänglichen Archiv-Unterlagen entnommen werden. Was die persönlicheren Dinge betrifft, also das, was sich in einer Personalakte befindet, ist eine amtliche Würdigung vor Ablauf der genannten Frist darauf angewiesen, öffentliche Quellen, (z. B. alte Zeitungen im Archiv) auszuwerten und zu versuchen, von bzw. mit Hilfe von Hinterbliebenen, aber auch ehemaligen Mitarbeitern, Mitstreitern oder Gegnern des Verstorbenen Informationen zu bekommen.

Selbstverständlich ist schon vor Ablauf der in § 10 Abs. 1 Satz 3 und 4 bestimmten Schutzfristen gemäß § 10 Abs. 4 Satz 3 SächsArchivG die Nutzung personenbezogener Akten auch dann zulässig, wenn die Person, auf die sich das Archivgut bezieht, oder im Falle ihres Todes ihre Angehörigen eingewilligt haben; die Einwilligung ist von dem überlebenden Ehegatten, nach dessen Tod von seinen geschäftsfähigen Kindern und, wenn weder ein Ehegatte noch Kinder vorhanden sind, von den Eltern der betroffenen Person einzuholen.

Anderes gälte nur für eine Würdigung im Rahmen eines bestimmten Vorhabens wissenschaftlicher Forschung (§ 10 Abs. 4 Satz 2 SächsArchivG), was allerdings nur in den allerseltensten Fällen in Betracht kommen dürfte: Dann könnte bei entsprechend hohem öffentlichem Interesse an der Durchführung des Forschungsvorhabens die Schutzfrist verkürzt werden.

5.8.3 Suchaktion in einem Kommunalarchiv

Die Anfrage eines von den DDR-Organen schon in jungen Jahren aus politischen Gründen über längere Zeit und in vielfältiger Weise Verfolgten, der nach diese Maßnahmen betreffenden Unterlagen suchte, jedoch aufgrund verschiedener Umstände dem einen oder anderen in dem zuständigen Landratsamt Beschäftigten aus nachvollziehbaren Erwägungen im Hinblick auf dessen - tatsächliche oder mögliche - Beziehung zu den früheren Verfolgungsmaßnahmen nicht traute, hat dazu geführt, dass ich in dem betreffenden Kreisarchiv nach diesen Unterlagen gesucht und in dieser Behörde die Einhaltung der Vorschriften über den Datenschutz, insbesondere des Sächsischen Archivgesetzes, kontrolliert habe, und zwar im Hinblick auf die Aufbewahrung und Benutzung von Altdaten wie Unterlagen zu Übersiedlungs- bzw. Ausreiseanträgen des ehemaligen *Rates des Kreises* (1), Patientenakten der aufgelösten Polikliniken, ehe-

maligen staatlichen Arztpraxen und betrieblichen Sanitätsstellen (2) sowie der sog. Kreismeldekartei (3).

Das Kreisarchiv hat insgesamt einen gutorganisierten Eindruck gemacht, und die Bediensteten des Archivs sind mir sehr behilflich gewesen und den Fragen des Datenschutzes offen begegnet. Nichtsdestoweniger hat sich herausgestellt, dass einiges hat verbessert werden müssen, was möglicherweise auch für andere Kommunalarchive in Sachsen gilt:

(1) Die Unterlagen des ehemaligen *Rates des Kreises* zu Übersiedlungs- bzw. Ausreiseanträgen waren vom Kreisarchiv soweit erkennbar vollständig übernommen worden.

Zur Erschließung des aufbewahrten Materials waren jedoch zwei verschieden Listen (Ablieferungsverzeichnisse) in unterschiedlicher Weise auf gleichlautenden Vordrucken erstellt worden. Eine davon ist im Laufe der Kontrolle erst mit Verzögerung aufgefunden und herangezogen worden, und von dieser letztgenannten Liste konnte kein Zusammenhang zu den Kartons („Schriftgutbehältern“) hergestellt werden, in denen die einzelnen Vorgänge aufbewahrt werden. Es ist einem glücklichen Zufall (in Verbindung mit intensiven Suchbemühungen!) zu verdanken gewesen, dass die den Petenten betreffenden Unterlagen bei der Kontrolle haben aufgefunden werden können.

Wendet sich in solchen Fällen ein Betroffener selbst an das Archiv, steht unter diesen Umständen sehr zu befürchten, dass sein Antrag auf Auskunft bzw. Einsicht (§ 6 SächsArchivG) mit der Begründung abgelehnt wird, dass Unterlagen zu seiner Person nicht vorhanden seien, obwohl diese Unterlagen tatsächlich vorhanden und nur eben nicht auffindbar sind. Das darf im Hinblick auf das Gebot der „Sicherung berechtigter Belange betroffener Personen“ (§ 2 Abs. 3 SächsArchivG) und die Verpflichtung der Behörde, die Erfüllung des aus dem Grundrecht auf informationelle Selbstbestimmung fließenden Auskunfts- bzw. Einsichtsanspruchs (§ 6 SächsArchivG) sicherzustellen, nicht sein. Es hat also einer Vervollständigung des Bestandsverzeichnisses hinsichtlich der Listen über den Bestand (hier bezüglich der zurückgenommenen Ausreiseanträge) bedurft. Ich habe empfohlen, zu diesem Zweck darüber hinaus ein Findbuch anzulegen, in dem sämtliche Bestände des Kreisarchives der Art - z. B. zurückgenommene Ausreiseanträge - verzeichnet sind, oder eine gleichwertige Lösung zu finden.

(2) Die Patientenakten aufgelöster Polikliniken wurden sämtlich in einer Außenstelle des Kreisarchives aufbewahrt, wobei innerhalb der verschiedenen Bestände die ursprüngliche Ordnung beibehalten war. Das Auffinden der den Petenten betreffenden Unterlagen hat den zuständigen Bediensteten hier keine Schwierigkeiten bereitet.

Nichtsdestoweniger habe ich empfohlen, im Interesse der Benutzerfreundlichkeit auch insoweit ein Findbuch anzulegen.

Hinsichtlich der Benutzung der Patientenakten zum Zwecke der von Betroffenen selbst gewünschten Auskunftserteilung hatte man sich eine besondere Vorgehensweise ausgedacht: Wurden Auskunftsersuchen an das Archiv gerichtet, so suchte eine Archiv-Bedienstete die entsprechenden Unterlagen heraus und übersandte diese dem Gesundheitsamt des Landkreises, das dann die gewünschte Auskunft erteilte. Als Grund für diese Verfahrensweise ist mir gegenüber angegeben worden, dass die Archiv-Bediensteten nicht ausgebildet seien, fachspezifische - also hier medizinische - Auskünfte aus den Patientenakten zu erteilen. Diese Sachkunde besäßen dagegen die ärztlichen Mitarbeiter des Gesundheitsamtes, weshalb diese ‚dazwischengeschaltet' würden. Insbesondere seien nur fachkundige Personen in der Lage, einzuschätzen, welche Angaben dem Betroffenen zur Kenntnis gegeben werden können, ohne dass dieser möglicherweise seelische Schäden davonträgt. (Das Versenden der jeweiligen Patientenakte an das Gesundheitsamt wurde in einem Postausgangsbuch vermerkt, die Rückkehr der Unterlagen hingegen nur unzulänglich.)

Da das Gesundheitsamt mit Hilfe der Angaben in den Patientenakten etwas leisten soll, wozu einerseits das Archiv nicht in der Lage ist, was aber andererseits von der spezifischen, ureigenen Archivbehörden-Aufgabe der Auskunftserteilung nicht zu trennen ist, nämlich medizinisch fachkundige Auskünfte zu erteilen, kann man hier auch nicht von einer Datenverarbeitung im Auftrag sprechen, in deren Rahmen die Weitergabe personenbezogener Daten keine Übermittlung darstellt und somit keiner Rechtsgrundlage bedarf. Eher handelt es sich um Funktionsübertragung, und zwar gewissermaßen um Funktionsübertragung mit Steigerungswirkung.

Nichtsdestoweniger habe auch ich die gewählte Vorgehensweise für sinnvoll gehalten, nicht zuletzt deshalb, weil sie im Interesse des Betroffenen liegt. Um sie auf die gleichwohl erforderliche rechtliche Grundlage zu stellen, muss in diesen Fällen die Einwilligung des Betroffenen in die Übermittlung an das Gesundheitsamt eingeholt werden. Dies scheint mir auch nicht mit einem unverhältnismäßigen Aufwand verbunden zu sein. Soweit erkennbar gewesen ist, ersucht zumeist ein Sozialleistungsträger um Auskunft, sei es, dass er sich an das Archiv, sei es, dass er sich unmittelbar an das Gesundheitsamt wendet. Der Leistungsträger könnte die Einwilligung, die der Betroffene ohnehin erteilen muss und ohne die die Auskunft ja nicht erteilt werden darf, darauf erstrecken, dass das Gesundheitsamt in die Auskunftserteilung eingeschaltet wird. Der Einwand, dies sei nicht praktikabel, weil sich die Sozialleistungsträger unmittelbar an das Gesundheitsamt wendeten, das die Anforderung dann an das Kreisarchiv weitergebe, außerdem habe sich über diese Verfahrensweise bisher noch

niemand beschwert, hat mich nicht überzeugt: Archiv und Gesundheitsamt sind nun einmal in der für die datenschutzrechtliche Betrachtungsweise maßgeblichen funktionellen Hinsicht strikt von einander geschiedene Behörden, auch wenn sie in organisatorischer Hinsicht Teile desselben Landratsamtes sind. Sicherlich ist es archivrechtlich gewissermaßen ein außergewöhnlicher Sonderfall, dass im Gebiet der ehemaligen DDR die bei der ärztlichen Versorgung der Bevölkerung entstandenen Unterlagen in die Archive öffentlicher Stellen, also in Archiv*behörden*, gelangt sind (eben weil - historisch gesehen: ausnahmsweise - es der Staat selbst gewesen ist, der die ärztliche Versorgung unmittelbar in der Hand gehabt hat. Ähnliches gilt übrigens für die Auskünfte aus den Unterlagen, die aus der Eigenschaft des damaligen Staates entstanden sind, mittelbar fast jedermanns Arbeitgeber gewesen zu sein; insoweit hat allerdings die Sonderarchivierung durch ein von der Treuhandanstalt [bzw. BvS] beauftragtes Unternehmen dazu geführt, dass die das normale Archivpersonal notwendig überfordernden Auskünfte für Sozialversicherungszwecke von spezialisierten Kräften erteilt werden können.) Aber diese Überlegung rechtfertigt keine Abweichung von den allgemeinen Regeln. Das wird man den Sozialleistungsträgern erklären und zumuten können: Sie können die vorgefertigten Einwilligungserklärungen entsprechend (um-)formulieren, dann ergibt sich kein Mehraufwand.

Ich empfehle daher, allgemein in Sachsen entsprechend zu verfahren.

(3) Die Kreismeldekartei aus DDR-Zeiten wurde in der Organisationseinheit „Personenstandswesen und Staatsangehörigkeitsrecht“ des Ordnungsamtes verwaltet, obwohl sie im Kreisarchiv hätte aufbewahrt sein müssen. Denn gemäß § 1 Abs. 2 der Zweiten Verordnung des SMI zur Durchführung des Sächsischen Meldegesetzes (Verordnung über melderechtsfremde Daten) vom 25. Oktober 1995 (GVBl. 1995, S. 360) haben die Meldebehörden die bei ihnen vorhandenen Unterlagen mit Daten, die über die in § 5 SächsMG genannten Daten hinausgehen (melderechtsfremde Daten), den zuständigen kommunalen Archiven zu übergeben gehabt.

Die danach gebotene Übernahme der Kreismeldekartei in das Archiv - das betreffende Landratsamt hat diese Übernahme auf mein Verlangen dann alsbald nachgeholt - hat zur Folge, dass die übergebenen Unterlagen Archivgut im Sinne des § 2 SächsArchivG werden. Die Benutzung der Kreismeldekartei ist dann nur nach Maßgabe des Sächsischen Archivgesetzes zulässig.

In dem betreffenden Landratsamt ist es üblich gewesen, aus der Kreismeldekartei zwar Auskünfte an Betroffene über das Archiv (wohl auch um Gebühreneinnahmen zu erzielen!) nach Maßgabe des Sächsischen Archivgesetzes zu erteilen, die Auskünfte an die Meldebehörden jedoch unmittelbar. (Über die rechtliche Grundlage, auf der die

Daten gespeichert und an Meldebehörden übermittelt wurden, hat man sich keine Gedanken gemacht!) Auf die Auskunftsersuchen der Meldebehörden hin haben die Bearbeiter in zahlreichen Fällen einfach eine Kopie der entsprechenden Karteikarte übersandt. Das war unzulässig, da nicht von einer Rechtsgrundlage gedeckt. Die genannte Verordnung soll gerade verhindern, dass den Meldebehörden melderechtsfremde Daten aus DDR-Beständen zur Verfügung stehen. Die Übermittlung durch das Archiv wie auch die Erhebung durch die Meldebehörde hat sich auf diejenigen Daten zu beschränken, die nach geltendem Recht Meldedaten sind; die melderechtsfremden Daten sind dagegen nicht zur Erfüllung der Aufgaben der Meldebehörde erforderlich. Das Kreisarchiv (!) darf der Meldebehörde also - wenn nicht eine Auskunft durch bloße Wiedergabe von Inhalten in veränderter Zeichengestalt erteilt werden soll - nur eine auf melderechtliche Daten beschränkte Teil-Ablichtung übermitteln. Meinem Vorschlag, zu Vereinfachungszwecken dabei statt mit Schwärzungen mit einer Kopier-Maske zu arbeiten, ist das Landratsamt gefolgt: Damit wird sichergestellt, dass der Meldebehörde nur Daten übermittelt werden, die zu dem sich aus § 5 SächsMG ergebenden Datensatz gehören, also z. B. nicht zu dem zentral im Namensfeld dick eingerahmten Feld „Hinweis“ die Angabe „nicht geeignet“, Angaben zu Ausreisen oder Haft und auch kein „K-Vermerk“.

Vielleicht sogar noch wichtiger als das ist aber gewesen, dass ich dem Petenten habe mitteilen können, dass ich keinerlei Anhaltspunkte habe feststellen können, die seine Befürchtungen hätten bestätigen können, dass sich Bedienstete des Kreisarchivs oder des Ordnungsamtes von irgendwelchen Bediensteten des Landratsamtes in irgendeiner Weise dahin beeinflussen lassen könnten, seine, also des Petenten, Rechte zu beschneiden.

5.8.4 Am Rande des Archivrechtes: Auskunftsanspruch nach dem Tode des Betroffenen

Unter Berufung darauf, Lebenspartnerin eines Ende 1990 drei Wochen nach einer Operation in einer sächsischen Universitätsklinik verstorbenen Mannes gewesen zu sein, hatte eine Petentin von der Klinik eine Kopie der von dem Verstorbenen seinerzeit unterzeichneten Einwilligung in den Heileingriff verlangt. Nachdem die Frau, die vom Verstorbenen nicht als Erbin eingesetzt worden ist, abschlägig beschieden worden war, hat sie sich an mich gewandt. Ich habe ihr keinen günstigeren Bescheid geben können:

Datenschutzrechtlich hat sich das von der Petentin geltend gemachte Begehren nur im Wege des sog. datenschutzrechtlichen *Auskunftsanspruches* begründen lassen können. Nach der insoweit einschlägigen Spezialvorschrift des § 33 Abs. 5 SächsKHG steht ein solcher Anspruch nur dem Betroffenen (Patienten) zu, also demjenigen auf den sich das

Datum bezieht, mithin demjenigen, der die Einwilligung erklärt hat. Dieser ist in diesem Falle eben jedoch schon tot gewesen.

Da die Petentin weder Familienangehörige noch anderweitig zur Wahrnehmung des postmortalen Persönlichkeitsrechtes besonders Bestimmte (vgl. Rixecker in: Münchener Kommentar zum BGB, 4. A. 2001, Rdnr. 26 zu § 12 [Anh.] noch auch Erbin (Befugnis der Erben str., vgl. Rixecker a. a. O. mit Fn. 87) des Verstorbenen war, hat sich die Frage der Möglichkeit eines Überganges des Auskunftsanspruches des Betroffenen (oder eines anderweitigen, nämlich originären, Erwerbes eines inhaltsgleichen Anspruches?) hier nicht gestellt. Denn nur für diesen Personenkreis kommt ein solcher Übergang (bzw. originärer Erwerb?) eines Auskunftsanspruches in Frage (zum postmortalen Persönlichkeitsrecht vgl. die einschlägige ständige Rechtsprechung seit BGHZ 50, 133 ff. [„Mephisto“]; §§ 10 Abs. 4 Satz 3 SächsArchivG, § 8 Abs. 2 Satz 2 und 3 Krebsregistergesetz; § 22 Satz 4 KUG, § 77 Abs. 2 StGB). Es bestand somit keine datenschutzrechtlich begründete Pflicht des Universitätsklinikums, der Petentin den Inhalt der Einwilligungserklärung zugänglich zu machen.

Unabhängig davon hat sich datenschutzrechtlich die Frage gestellt, inwieweit das Universitätsklinikum *berechtigt* (gewesen) wäre, der Petentin den Text der Einwilligungserklärung des Verstorbenen zu überlassen.

Die Frage stellt sich freilich nur, wenn man auch den datenschutzrechtlichen Schutz des Persönlichkeitsrechts über den Tod hin andauern lässt, ihn also so weit reichen lässt, wie den sonstigen postmortalen Schutz des Persönlichkeitsrechts. Man wird dies, auch bei Herleitung des verfassungsrechtlichen Persönlichkeitsrechtes wie speziell des Grundrechtes auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bzw. der Anknüpfung an *jeden Menschen* in § 33 SächsVerf, bejahen müssen, weil sonst die zivilrechtlichen Einschränkungen der Handlungsfreiheit der lebenden Dritten zugunsten des Persönlichkeitsrechts des Toten verfassungswidrig wären.

Ausweichlösung wäre, den postmortalen Persönlichkeitsschutz als bloßen Reflex des Schutzes des Persönlichkeitsrechts der Angehörigen des Verstorbenen anzusehen, was aber nicht der Standpunkt der Lehre und Rechtsprechung im Zivilrecht ist (vgl. Rixecker a. a. O. Rdnr. 29) und auch wohl deswegen ausscheidet, weil es schwer zu begründen wäre, wieso mit dem Tode der unmittelbar Betroffenen ein akzessorisches, abgeleitetes Persönlichkeitsrecht des Angehörigen entstehen können soll, das vorher zweifellos nicht existiert hat: So hat namentlich der (öffentlich-rechtliche) Auskunftsanspruch des nahen Familienangehörigen vor dem Zeitpunkt des Todes nicht etwa als Anspruch auf Auskunft hinsichtlich eines latent-eigenen Datums des Angehörigen begründet werden können.

Unterstellt, das schwer greifbare (vgl. Rixecker a. a. O. Rdnr. 28) Ende des postmortalen Persönlichkeitsschutzes war im vorliegenden Fall noch nicht erreicht, was sich vielleicht schon an den Bemühungen der Petentin ablesen ließ, kam als Übermittlungsbefugnis nur § 16 Abs. 1 Nr. 2 SächsDSG in Betracht. Danach war die Übermittlung nur zulässig, wenn der Empfänger, also die Petentin, ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt und der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung gehabt hat. Das Universitätsklinikum hatte ein solches Interesse nicht anerkannt. Das Gegenteil, und damit das Vorliegen der notwendigen Voraussetzung der Erlaubtheit dieser Übermittlung, ist auch für mich nicht eindeutig erkennbar geworden: Die Petentin war weder die Witwe des Verstorbenen noch dessen Erbin, sie war auch nicht durch den erkennbar gewordenen Willen des Verstorbenen zu dergleichen legitimiert worden. Ein berechtigtes Interesse an der Übermittlung konnte allein auf eine tatsächliche Nähebeziehung zum verstorbenen Betroffenen gestützt werden. Ein emotionales Interesse („Affektionsinteresse“), nach 13 Jahren noch zu erfahren, ob der frühere Lebenspartner zutreffend aufgeklärt und gegebenenfalls an einer Operation gestorben ist, über deren Risiken er nicht hinreichend aufgeklärt worden ist, war infolge des Zeitablaufes doch sehr stark abgeschwächt. Auch haben Rückfragen bei der Petentin ergeben, dass sie die Daten stattdessen eigentlich eher deswegen haben wollte, weil sie einen Schadensersatzanspruch gegen das Universitätsklinikum geltend zu machen gedachte. Dabei war sie bereits unmittelbar nach der Operation mit einer entsprechenden Klage gescheitert. Auch aus dieser Absicht ließ sich ein berechtigtes Interesse im Sinne von § 16 Abs. 1 Nr. 2 SächsDSG kaum begründen. Denn eine erneute Klage hätte kaum Aussicht auf Erfolg gehabt: Zum einen würde ihr im Hinblick auf den schon abgeschlossenen früheren Rechtsstreit die Rechtskraft der damaligen Entscheidung entgegenstehen. Zum anderen wäre die Petentin - auch - für einen neuerlichen Prozess wohl nicht der richtige Kläger. Allein der Erbe könnte einen so begründeten Schadensersatzanspruch haben.

Darüber hinaus hätte selbst dann, wenn man ein berechtigtes Interesse der Petentin anzuerkennen gehabt hätte, geprüft werden müssen, ob schutzwürdige Interessen des Betroffenen der Datenübermittlung entgegenstanden. Hierzu wären wohl die Familienangehörigen gemäß § 16 Abs. 3 SächsDSG zu hören gewesen. (Eine solche Anwendung der Vorschrift wäre wohl die nötige Konsequenz einer Anerkennung datenschutzrechtlichen postmortalen Persönlichkeitsschutzes.) Eine Datenübermittlung an die Petentin ohne Zustimmung der Familienangehörigen wäre zumindest sehr bedenklich gewesen, eine solche Zustimmung hat nicht vorgelegen.

5.9 Polizei

5.9.1 Auskünfte aus polizeilichen Auskunftssystemen

Immer wieder fragen mich Bürger, ob ihre personenbezogenen Daten in polizeilichen Informationssystemen gespeichert sind und ob diese dann gelöscht werden können. In diesen Fällen weise ich die Petenten meistens darauf hin, dass sie zunächst selbst ein Auskunfts- und Löschungsersuchen bei der speichernden Stelle stellen können und sich im Fall der verweigerten oder unzureichenden Auskunft an mich wenden können. Um dies zu ermöglichen, möchte ich deshalb den grundsätzlichen Hergang eines solchen Auskunftsverfahrens schildern.

Daten zur Person des Betroffenen können in verschiedenen polizeilichen Informationssystemen gespeichert sein. In Betracht kommen dabei vor allem das beim LKA geführte Polizeiliche Auskunftssystem Sachsen (PASS), das beim BKA geführte Informationssystem der Polizei (INPOL) und das ebenfalls dort geführte Schengener Informationssystem (SIS).

PASS dient den Polizeidienststellen des Freistaates Sachsen zur landesweiten Erfassung, Speicherung und Auswertung von polizeilich relevanten Informationen, die im Freistaat Sachsen polizeilich bearbeitet werden, oder deren Ereignisort sich auf dem Gebiet des Freistaates Sachsen befindet. Damit Petenten überprüfen (lassen) können, ob ihre Daten rechtmäßig verarbeitet werden, können sie gemäß § 51 SächsPolG i. V. m. § 18 SächsDSG beim LKA (Neuländer Str. 60, 01129 Dresden) einen Antrag auf Auskunft zu den über sie von der Polizei gespeicherten Daten stellen. Die Auskunftserteilung darf nach § 18 Abs. 5 SächsDSG nur dann unterbleiben, soweit die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen überwiegender Geheimhaltungsinteressen der speichernden Stelle oder eines Dritten geheim gehalten werden müssen. Wenn die Auskunft verweigert wird, kann sich der Betroffene gemäß § 18 Abs. 6 SächsDSG an mich wenden und verlangen, dass die Auskunft mir erteilt wird.

Gelöscht werden die Daten gemäß § 49 SächsPolG i. V. m. § 20 SächsDSG, wenn die Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden, sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder der Löschung durch Rechtsvorschriften bestimmte Aufbewahrungsvorschriften entgegen stehen.

In Bezug auf Auskunftserteilungen aus dem INPOL und SIS kann sich der Betroffene an das BKA (Thaerstr. 11, 65173 Wiesbaden) bzw. dessen Kontrollbehörde, den BfD (Husarenstr. 30, 53117 Bonn) wenden.

5.9.2 Weitergabe von Daten aus polizeilichen Auskunftssystemen an private Sicherheitsdienste insbesondere für deren Zuverlässigkeitsprüfung von Einstellungsbewerbern

Im Februar 2003 erfuhr ich von der Verfahrensweise einer sächsischen Polizeidirektion, das polizeiliche Informationssystem nicht nur zur Bekämpfung von Straftaten zu nutzen, sondern auch zur Eignungsprüfung von Bewerbern bei Einstellungen und bei Beförderungen von Polizeibeamten.

Die Rücksprache mit meinen Kollegen in den anderen Bundesländern und dem BfD ergab, dass sie mehrheitlich der Ansicht sind, dass das Vorgehen bei *Neueinstellungen* im öffentlichen Dienst grundsätzlich zulässig sei, sofern die Abfrage auf der Grundlage einer freiwilligen Einwilligungserklärung des Bewerbers erfolge. Auf der anderen Seite läge jedoch ein besonderes Informationsinteresse des Dienstherrn bei *Beförderungen* nicht vor. Insoweit sei eine Abfrage nicht zulässig. Die Eignung ergebe sich aus dienstlichen Beurteilungen und sonstigen Eignungsnachweisen.

Auch andere Stellen bedienten sich bei der Personalauswahl aus dem PASS.

So habe ich festgestellt, dass private Sicherheitsdienste seit Dezember 2002 in mindestens 556 bekannten Fällen personenbezogene Daten von sächsischen Polizeidienststellen übermittelt bekamen. Im Einzelnen handelte es sich hierbei um sog. „Zuverlässigkeitsprüfungen“.

Die Daten aus polizeilichen Auskunftssystemen, die Bewerber für den Polizeidienst betreffen, dürfen weder nach dem Sächsischen Datenschutzgesetz noch nach den Vorgaben der PASS-Errichtungsanordnung für eine beabsichtigte Überprüfung genutzt werden. Nr. 2 der Errichtungsanordnung erlaubt, die dort verarbeiteten Daten im Rahmen der Gefahrenabwehr, zur Verhütung von Straftaten und zur Strafverfolgung zu verwenden. Nicht gestattet ist folglich die Nutzung für Aufgaben behördeninterner Personalverwaltung. Auch nach der Übermittlungsvorschrift des Sächsischen Datenschutzgesetzes (§ 13 Abs. 1 SächsDSG) ist die Erforderlichkeit des Zugriffs auf PASS-Daten zu verneinen. Die Personalverwaltung kann die für die Einstellung notwendigen Daten nur auf gesetzlicher Grundlage bei der jeweils zuständigen Behörde einholen. Besonders ins Gewicht fällt zudem, das eine Abfrage polizeilicher Auskunftssysteme zur Kenntnis einer Vielzahl personenbezogener Daten aus dem Bereich vollzugspolizeilicher Aufgaben führt, die für die anstehende Entscheidung der Personalverwaltung

keine Bedeutung haben. Zudem handelt es sich bei den Daten zu einem großen Teil um nicht gesicherte Erkenntnisse, denen lediglich Verdachtscharakter zukommt. Sie können nur Anhaltspunkte für weiteres präventives oder repressives Handeln geben.

Ich habe daher klar gefordert, dass die Polizei in Personalfragen nicht ihr fachliches Informationssystem in einen „Selbstbedienungsladen“ umfunktionieren darf. Denn alle Informationen, die für eine grundrechtsberührende Entscheidung, z. B. zum gleichen Zugang zu einem öffentlichen Amt nach Eignung, Befähigung und Leistung, zu verarbeiten sind, müssen stichhaltig, also überprüft und klar aussagekräftig sein. Hier bietet sich allein der Auszug aus dem Bundeszentralregister an; die dort gespeicherten Daten sind aufgrund rechtsgültiger Entscheidung zustande gekommen - sie sind valide. Eine Abfrage der Daten aus PASS nach einer vorherigen „freiwilligen Einwilligung“ des Bewerbers kann die fehlende Rechtsgrundlage für den Zugriff nicht ersetzen. Zudem ist zu beachten, dass der Betroffene keine Gewissheit über die gespeicherten Informationen hat. Im Übrigen würden Einwilligungsverweigerer ungerechtfertigt benachteiligt werden bzw. wäre die Einwilligung keine freiwillige mehr, da ein gewisser (auch selbst erzeugter) Druck zur Erteilung der Einwilligung in einer solchen Situation zu vermuten ist.

Zudem ist die Praxis der „Zuverlässigkeitsprüfung“ per Missbrauch des höchstpersönlich geltend zu machenden Auskunftsrechtes nach § 18 SächsDSG rechtswidrig, denn das Verfahren der Zuverlässigkeitsüberprüfung von Beschäftigten im privaten Sicherheitsgewerbe ist rechtlich abschließend geregelt (§ 9 BewachV). Die Vorschrift enthält keine Befugnis für private Unternehmen, die Zuverlässigkeit ihrer Bewerber oder Beschäftigten durch polizeiliche Selbstauskünfte oder eigene Auskunftsersuchen aus polizeilichen Informationssystemen zu überprüfen; vielmehr obliegt es der zuständigen Gewerbeaufsichtsbehörde, die Zuverlässigkeit dieser Beschäftigten mittels einer unbeschränkten Auskunft aus dem Bundeszentralregister nach § 41 Abs.1 Nr. 9 BZRG zu überprüfen. Die BZR-Daten sind - im Gegensatz zu Daten aus polizeilichen Auskunftssystemen - nämlich Ergebnisse aus rechtskräftig abgeschlossenen Verfahren und daher aussagekräftig.

Das Argument, das Gemeinwohl, zu dem auch die Funktionsfähigkeit des öffentlichen Dienstes gehört, rechtfertige den Zugriff auf in PASS gespeicherte Informationen, überzeugt nicht. Denn die Schwelle, die mit dem Erfordernis des „erheblichen Nachteils für das Gemeinwohl“ errichtet wurde, ist hoch. Nicht ausreichend ist insoweit, dass (ungesicherte) Eintragungen möglicherweise Beamte bzw. solche die es werden wollen, betreffen. Die Überprüfung aller Beamten anlässlich von Einstellungen, Beförderungen usw. mittels PASS würde sie einem Generalverdacht aussetzen, der in keinem Verhältnis zu der vielleicht zu erzielenden „Trefferquote“ steht.

Zudem ist es im Hinblick auf die beabsichtigte Gefahrenabwehr wenig effektiv, eine Überprüfung der Beamten nur bei so genannten Statusveränderungen vorzunehmen. Um wirklichen Schutz zu gewährleisten, wäre nämlich eine permanente Überprüfung der Beamten erforderlich, die aber bereits an den oben aufgezeigten Grenzen scheitert.

Folgt man im Übrigen der Argumentation der Befürworter, lässt sie sich über die Polizei hinaus auf den gesamten öffentlichen Dienst ausdehnen, denn auch bei Lehrern oder Finanzbeamten ist Zuverlässigkeit gefordert. Die Fragwürdigkeit des Vorgehens wird dann noch deutlicher. Die Begrenzung des obrigkeitlichen Handelns des Staates gilt eben auch dann, wenn es um seine Bediensteten geht. Denn diese sind in diesem Verhältnis Grundrechtsträger.

Aufgrund meiner Stellungnahme zu der Abfragepraxis in PASS für den öffentlichen Dienst und der Beanstandung nach § 29 SächsDSG vom 17. Dezember 2003 bzgl. der privaten Sicherheitsunternehmen habe ich erreicht, dass das SMI den nachgeordneten Bereich angewiesen hat, derartige Abfragen nicht mehr durchzuführen.

5.9.3 Fußballweltmeisterschaft 2006 - Akkreditierungsverfahren

Die Organisatoren der Fußball-Weltmeisterschaft 2006 in Deutschland haben in der Vorbereitung immense Aufgaben zu bewältigen. Impliziert ist auch die Beachtung datenschutzrechtlicher Vorgaben.

Mein Interesse gilt insbesondere dem so genannten Akkreditierungsverfahren. Diesem sollen Personen unterzogen werden, die während der WM Zugangsmöglichkeiten zu besonders geschützten Bereichen in den Stadien haben, z. B. Ordner, Presse-, Catering-, Security-, Medienvertreter, etc. Mit ihrem Einverständnis sollen die Betroffenen bestimmte personenbezogene Daten (wie Name, Anschrift, Geburtsdatum) an den Deutschen Fußballbund (DFB) melden. Dieser soll die Daten an das zuständige LKA übermitteln, welches sodann nach vom DFB vorgegebenen Kriterien beurteilen soll, ob der Betroffene „zuverlässig“ ist. Die Polizei stützt sich hierbei auf Informationen aus ihren Dateien, wie z. B. dem PASS. Der DFB soll dann aufgrund der Bewertung des LKA entscheiden, ob dem Betroffenen Zutritt gewährt werden kann.

Bezüglich dieses Verfahrens habe ich gegenüber dem SMI meine Bedenken angemeldet.

Die Zuverlässigkeitsüberprüfung von Betroffenen im Sicherheitsgewerbe ist bereits abschließend in der Gewerbeordnung geregelt. Bezüglich der anderen Betroffenen bietet - für die beabsichtigte Datenübermittlung vom LKA an den DFB - meines Erachtens das Polizeigesetz keine ausreichende Rechtsgrundlage. Voraussetzung für die Zulässigkeit

einer Datenübermittlung von der Polizei an nicht-öffentliche Stellen ist nach § 45 Abs. 2 Nr. 2 SächsPolG unter anderem, dass offensichtlich ist, dass die Datenübermittlung im Interesse des Betroffenen liegt, was hier nicht der Fall ist. Auch eine Einwilligung der Betroffenen scheidet als Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung aus, da die Betroffenen den Umfang und die Auswirkungen ihrer Einwilligung nicht ausreichend einschätzen können.

Einzig gangbarer Weg wäre, es den Betroffenen selbst zu überlassen, ob sie eine Selbstauskunft beim LKA oder einen Auszug aus dem Bundeszentralregister einholen und dann selbst entscheiden, ob sie die darin enthaltenen Daten dem DFB gegenüber offenbaren oder nicht.

Ich werde das weitere Verfahren begleiten und für ein datenschutzrechtlich unbedenkliches Prozedere eintreten.

5.9.4 Speicherung personenbezogener Daten im polizeilichen Informationssystem nach Verfahrenseinstellungen gemäß § 170 Abs. 2 StPO

Die Frage, wie im Fall der Einstellung strafrechtlicher Ermittlungsverfahren gemäß § 170 Abs. 2 StPO mit den gespeicherten personenbezogenen Daten des Beschuldigten im PASS verfahren wird, beschäftigt mich nicht erst in den vergangenen zwei Jahren.

Das Problem des einzelnen Betroffenen kann folgender Fall veranschaulichen, der im Berichtszeitraum aufgetreten ist. Ein Bürger, der sich an mich wandte, war in einem Unternehmen tätig, das auch Aufträge für sächsische Behörden ausführte. Wenn vorherzusehen war, dass die Mitarbeiter des Unternehmens im Rahmen ihrer Auftragserledigung auch mit sicherheitsempfindlichen Bereichen der öffentlichen Stelle in Berührung kommen würden, wurden diese Mitarbeiter einer Zuverlässigkeitsüberprüfung unterzogen, die eine Abfrage im PASS umfasste. Der Bürger, der seines Wissens strafrechtlich nie in Erscheinung getreten war, stellte erstaunt fest, dass zu seiner Person zwei Eintragungen zu gegen ihn geführten Ermittlungsverfahren im PASS enthalten waren. Beide Verfahren waren gemäß § 170 Abs. 2 StPO eingestellt worden. Die Eintragungen führten dazu, dass ihm der Zutritt zu bestimmten Bereichen des (öffentlichen) Auftraggebers verwehrt wurde. Die Vermutung liegt nahe, dass dem Bürger dadurch auch Nachteile im Verhältnis zu seinem Arbeitgeber erwuchsen. Es stellte sich heraus, dass der Bürger aufgrund einer durch eine Namensgleichheit verursachten Personenverwechslung ins Visier der Ermittler geraten und die Verfahren bei Bemerken dieses Umstands eingestellt worden waren. Die Eintragungen im PASS wurden allerdings nicht gelöscht.

Verantwortlich für die Speicherung im PASS ist die Polizei. Sie hat die Erforderlichkeit dieses Eingriffs in das Recht auf informationelle Selbstbestimmung des Betroffenen zu prüfen. Erhebt sie Daten im Rahmen strafrechtlicher Ermittlungen, richtet sich die Zulässigkeit der Speicherung für Zwecke der Gefahrenabwehr und vorbeugenden Verbrechensbekämpfung danach, ob ein Verdacht gegen den Betroffenen besteht. Daneben prüft die Polizei, ob Anhaltspunkte für die Bejahung einer Wiederholungsgefahr vorliegen.

Die Staatsanwaltschaft leitet das Ermittlungsverfahren und erhält von der Polizei die Ergebnisse der polizeilichen Ermittlungen. Über den Verfahrensausgang informiert die Staatsanwaltschaft die Polizei. Diese Mitteilung ist für die Prüfung der Erforderlichkeit der Speicherung personenbezogener Daten bedeutsam, kann sie doch Hinweise darauf enthalten, ob trotz eines verbleibenden, aber möglicherweise nicht nachweisbaren, Tatverdachts eingestellt wurde oder jegliche Verdachtsmomente ausgeräumt sind. Zu diesem Zweck kreuzt die Staatsanwaltschaft auf dem Formblatt der Mitteilung zum Punkt des Einstellungsgrundes eines der vorgesehenen Felder an. Erfolgt die Einstellung gemäß § 170 Abs. 2 StPO, weil die Tat unter keinen Straftatbestand fällt oder der Beschuldigte nicht der Täter ist, bedeutet dies für die Polizei, dass eine weitere Speicherung der anlässlich der Ermittlungen erhobenen Daten des Beschuldigten unzulässig ist und die Daten im PASS zu löschen sind.

In konstruktiven Gesprächen mit dem SMJus, der Generalstaatsanwaltschaft, dem SMI und dem LKA konnte für die Zukunft ein Verfahren entwickelt werden, das einen optimalen Rücklauf von Verfahrensausgangsmitteilungen an die Polizei gewährleisten und deren Prüfung der Erforderlichkeit der weiteren Speicherung personenbezogener Daten ermöglichen soll. Die Staatsanwaltschaft wird die Polizei frühzeitig über Verbindungen von Verfahren informieren; hier lag in den letzten Jahren eine Unsicherheitsquelle hinsichtlich abweichender Zahlen von Verfahren bei Polizei und Staatsanwaltschaften. Nach Ablauf von polizeiintern festgelegten Prüffristen wird - sollte bis dahin noch keine Mitteilung der Staatsanwaltschaft erfolgt sein - die Polizei bei der Staatsanwaltschaft den Verfahrensausgang erfragen. In den Fällen, in denen die Staatsanwaltschaft gemäß § 170 Abs. 2 StPO eingestellt hat und keinen Tatverdacht sieht, werden die personenbezogenen Daten zu diesem Verfahren im PASS gelöscht. In den anderen Fällen prüft die Polizei die Erforderlichkeit der Speicherung anhand der Aktenlage (Wiederholungsgefahr, Schwere des Delikts).

Die Polizei versicherte, die in der Vergangenheit aufgelaufenen Fälle von Speicherungen personenbezogener Daten aus Ermittlungsverfahren im PASS, deren Erforderlichkeit aufgrund nicht ausreichend erfolgter Mitteilungen über Verfahrensausgänge

unklar ist, schnellstmöglich zu prüfen und dabei einen großzügigen Maßstab anzulegen, was ich ausdrücklich begrüße.

Das gefundene Verfahren ist praktikabel und setzt die gesetzlichen Vorgaben um. Es ist für mich ein Musterbeispiel, wie bei konstruktivem Engagement aller Beteiligten eine für alle Betroffenen zufrieden stellende Lösung erreicht werden kann. Ich bin optimistisch, dass Fälle wie der oben beschriebene zukünftig nicht mehr auftreten.

5.9.5 Zur Bildaufzeichnung durch den Polizeivollzugsdienst

Das Sächsische Polizeigesetz sieht in § 38 Abs. 2 die Befugnis für den Polizeivollzugsdienst vor, an Kriminalitätsbrennpunkten personenbezogene Daten durch Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen von Personen zu erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an diesen Orten Straftaten begangen werden sollen, durch die Personen, Sach- oder Vermögenswerte gefährdet werden.

Der SächsVerfGH hat sich in seinem Urteil vom 10. Juli 2003 zur Verfassungsmäßigkeit einzelner Regelungen des Sächsischen Polizeigesetzes (Az.: Vf. 43-II-00) zur Frage der Zulässigkeit der Permanentaufzeichnung von Bildaufnahmen und ihrer präventiven Wirkung geäußert und darauf hingewiesen, dass „sich etwa auf die Anzeige einer Straftat hin, die der Polizeibeamte am Monitor nicht wahrgenommen hat, nur im Falle kontinuierlicher Aufzeichnung nachträglich das Geschehen verifizieren“ lasse und diese Möglichkeit einen wesentlichen Teil der angestrebten Abschreckungswirkung ausmachen könne. Vor diesem Hintergrund habe ich gegenüber dem SMI meine grundsätzliche Zustimmung zu derartigen Vorhaben erklärt.

Allerdings habe ich ausdrücklich darauf hingewiesen, dass in der oben zitierten Gerichtsentscheidung auch festgestellt wird, dass die Bildaufzeichnung einen gegenüber der Bildaufnahme schwerer wiegenden Eingriff darstellt.

Im Freistaat Sachsen hat der Wortlaut von § 38 Abs. 2 SächsPolG nun anscheinend die Konsequenz, dass zwei polizeiliche Maßnahmen unterschiedlicher Eingriffsintensität unter identischen Voraussetzungen durchgeführt werden dürfen. Dies aber kann so nicht richtig sein. Der SächsVerfGH stellt in seinem o. g. Urteil fest, dass die gleichen Voraussetzungen für die unterschiedlich schweren Grundrechtseingriffe die Befugnis zu permanenter Aufzeichnung - den tieferen Eingriff also - nicht von vornherein unverhältnismäßig machten. Dies bedeutet aber auch, dass die Aufzeichnung nicht von vornherein und immer dann, wenn Aufnahmen zulässig wären, verhältnismäßig ist. Bei der permanenten Aufzeichnung von Bildaufnahmen kommt mithin der Beachtung des

Grundsatzes der Verhältnismäßigkeit eine ganz besondere Bedeutung zu, weil der in der Aufnahme liegende Eingriff in der Aufzeichnung (Speicherung) fortdauert.

So sind etwa an die Darlegung der Erforderlichkeit der Bildaufzeichnung besondere Anforderungen zu stellen. Allein die Tatsache, dass der erfasste Bereich einen Kriminalitätsschwerpunkt bildet, wird regelmäßig nicht ausreichen, die Erforderlichkeit zu begründen. Hier wird die Struktur der vor Ort anfallenden Straftaten zu berücksichtigen sein und der vorrangige Einsatz des milderen Mittels der Bildaufnahme und einer (manuellen) Aufzeichnung im Einzelfall in Betracht kommen. Zeigt hingegen die Kriminalitätsentwicklung in einem bereits durch Bildaufnahmen überwachten Bereich, dass Fallzahlen bestimmter Delikte durch die Überwachung nicht spürbar rückläufig sind, weil die Begehung dieser Delikte mittels Übersichtsaufnahmen nur schwer zu erkennen ist und potentielle Täter dies wissen, kann der Einsatz der permanenten Bildaufzeichnung durchaus erforderlich sein, um die angestrebte Abschreckungswirkung zu erzielen.

Keinesfalls dürfen hoch auflösende Kameras Eingänge zu Wohnhäusern oder Eingangsbereiche von Arzt- oder Rechtsanwaltspraxen sowie von Presseräumlichkeiten erfassen. Gegebenenfalls muss eine Verkleinerung des überwachten Bereichs im Vergleich zu dem von - Identifizierungen nicht ermöglichenden - Übersichtsaufnahmen erfassten Areal hingenommen werden.

Schließlich sind Maßnahmen zu ergreifen, die den Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen möglichst gering halten. Das SMI schlug in diesem Zusammenhang vor, das Verfahren technisch so auszugestalten, dass keine Zugriffsmöglichkeit auf die Daten (Aufzeichnungen) besteht, es sei denn, dass sich im Nachhinein für den fraglichen Zeitraum ein polizeilich relevanter Sachverhalt herausstellt. Diesen Vorschlag sehe ich ebenso positiv wie die auf diesem Gebiet konstruktive Zusammenarbeit mit dem SMI, das den betroffenen Polizeidienststellen meine Hinweise zugeleitet und um deren Beachtung gebeten hat.

5.9.6 Videoaufzeichnungen bei Demonstrationen

Im Berichtszeitraum habe ich bei der Polizei eine Kontrolle zu der Thematik „Bildaufzeichnungen bei Demonstrationen“ durchgeführt.

Gemäß § 12 a VersammlG dürfen Bild- und Tonaufnahmen von Teilnehmern einer Demonstration nur angefertigt werden, wenn konkrete Tatsachen bzw. belegbare Anhaltspunkte für das Vorliegen einer Gefahrenlage erkennbar sind.

Die Polizei nutzt für die Beobachtung von Demonstrationen sowohl feste Standorte wie z. B. Kameras auf Hochhäusern, als auch mobile Einsatzteams, u. a. auch Hubschrauber, die die Bilder in das Lagezentrum übertragen. Dies dient der Beobachtung des Verlaufs von Veranstaltungen. Aufzeichnungen mit diesen Kameras erfolgen erst, wenn sich ein konkreter Tat- oder Gefahrenverdacht entwickelt. Auf diesen Übersichtsaufnahmen sind keine einzelnen Personen erkennbar, es wird nur das Gesamtgeschehen erfasst. Ein Heranzoomen ist technisch möglich und kann vom Lagezentrum angeordnet werden.

Die Polizei teilte hierzu mit, dass bei Demonstrationen ausschließlich auf der Grundlage des § 12 a VersammlG videografiert werde. Eine Übermittlung der Bildaufnahmen erfolge nur zwischen den beteiligten Polizeidienststellen und im Rahmen der Strafverfolgung an die Staatsanwaltschaft. Die Aufbewahrungsfrist für das Videomaterial, das als Beweismittel im Strafverfahren diene, richte sich nach der Aufbewahrungsfrist der Akte. Eine Löschung der Aufnahmen erfolgte unverzüglich, wenn nicht aus Gründen der Gefahrenabwehr oder Strafverfolgung eine Aufbewahrung notwendig sei. Das bei der Polizei im Rahmen der Kontrolle vorgefundene Bildmaterial diene ausschließlich Strafverfolgungs- und Schulungszwecken. Zu Gefahrenabwehrzwecken würden derzeit keine Bildaufzeichnungen aufbewahrt.

Gegen diese Praxis des Videografierens bzw. Beobachtens bestehen meinerseits keine Bedenken.

Allerdings habe ich den Einsatz einer „Handkamera“ gerügt. Beim Einsatz von Handkameras begleitet der jeweilige Beamte zu Fuß den Demonstrationszug und macht die Bild- und Tonaufnahmen direkt aus dieser Position. Eine Übersichtsaufnahme ist nur selten möglich. Vielmehr besteht die Gefahr, dass, wenn die Kamera dabei die ganze Zeit läuft, unzulässigerweise Nahaufnahmen von einzelnen Versammlungsteilnehmern auch außerhalb konkreter Gefahrensituationen angefertigt werden.

Der Einsatz von „Handkameras“ außerhalb der konkreten Gefahrensituation ist unzulässig. Die „Handkameras“ dürfen erst eingesetzt werden, wenn sich konkrete Anhaltspunkte ergeben, dass die Versammlung durch die Begehung von Straftaten gestört werden soll. Dies könnte z. B. der Fall sein, wenn Tumulte entstehen. Dass Personen zunächst ohne das Vorliegen von Verdachtsgründen videografiert werden, damit ggf. später, wenn es zu einer Störung gekommen ist, das Bildmaterial genutzt werden kann, um relevante Personen zu identifizieren, ist unzulässig.

Ich habe angeregt, Videoaufnahmen so zu dokumentieren, dass eine Recherche und Kontrolle jederzeit möglich ist. Meine Anregungen wurden in einer Dienstanweisung umgesetzt.

5.9.7 Vorladungen zu polizeilichen Vernehmungen

Zwei Fälle aus dem Berichtszeitraum verdeutlichen, dass die Polizei im Rahmen ihrer Ermittlungstätigkeit zur Strafverfolgung nicht immer die erforderliche Sorgfalt walten lässt, wenn sie Zeugen oder Beschuldigte zu Vernehmungen lädt.

Ein Bürger wandte sich an mich, weil es ihn verwunderte, dass er in der Vorladung zur Vernehmung als Zeuge in einer Verkehrsstrafsache gebeten worden war, sein Fahrzeug zur Vernehmung mitzubringen. Seine Verwunderung steigerte sich, als der Polizeibeamte Lichtbilder des Fahrzeugs anfertigen und Fingerabdrücke des Petenten nehmen wollte, was aufgrund der Weigerung des Petenten unterblieb. Auf Nachfrage konnte der Polizeibeamte dem Petenten nicht sagen, ob er als Zeuge oder Beschuldigter befragt wurde. Wie sich herausstellte, hatte die für die Ermittlung zuständige Polizeidirektion das Polizeirevier, das die Vernehmung durchführte, in einem Ermittlungsersuchen nicht nur um die Vernehmung des Petenten als Zeuge, sondern auch um die Fertigung von Lichtbildern des Fahrzeugs sowie eines Porträtfotos des Petenten gebeten.

In einem anderen Fall erhielt ein Petent eine Vorladung, in der ihm als Beschuldigter mitgeteilt wurde, dass beabsichtigt sei, ihn zum Tatvorwurf zu vernehmen bzw. anzuhören. Des Weiteren erschien in der Vorladung der Hinweis auf Beachtung des Beschlusses des Ermittlungsrichters, der der Vorladung beigefügt war. Dieser enthielt die Anordnung der Entnahme und Untersuchung einer Speichelprobe des Petenten, der im Vernehmungstermin freiwillig eine Speichelprobe abgab.

In beiden Fällen war der jeweiligen Ladung nicht zu entnehmen, dass in den Terminen neben der Anhörung bzw. Vernehmung weitere Maßnahmen der Verarbeitung personenbezogener Daten beabsichtigt waren. Während im ersten Fall für die Durchführung erkennungsdienstlicher Maßnahmen schon eine gesetzliche Grundlage fehlte, da der Petent offensichtlich nicht Beschuldigter war, war im zweiten Fall die Ladung zumindest missverständlich, da explizit nur die Absicht der Vernehmung bzw. Anhörung des Petenten mitgeteilt wurde. Den Betroffenen sollte deutlich gemacht werden, was sie im Vorladungstermin zu erwarten haben. Beabsichtigte - zulässige - erkennungsdienstliche Maßnahmen sind in der Vorladung anzukündigen.

Die jeweils zuständigen Polizeibehörden räumten Fehler bei der Vorbereitung und Durchführung (im ersten Fall) bzw. bei der Vorladung (im zweiten Fall) ein. Ich gewann den Eindruck, dass das Verwenden von Textbausteinen in den Vorladungen zu

einer gewissen Oberflächlichkeit in der Bearbeitung des Einzelfalles führt und dessen Eigenheiten unberücksichtigt lässt. Die dadurch bei den Betroffenen verursachte Verunsicherung hinterlässt bei diesen den vermeidbaren Eindruck fehlender Sensibilität oder gar „Geheimniskrämerei“ der Behörden im Umgang mit personenbezogenen Daten.

5.9.8 Zustellung der Ladung zur Beschuldigtenvernehmung im Ermittlungsverfahren

Aufgrund der Eingabe einer Petentin erfuhr ich Anfang 2004 von folgendem Vorgehen der sächsischen Polizei. Die erwachsene und voll geschäftsfähige Petentin sollte im Rahmen eines Ermittlungsverfahrens zur Beschuldigtenvernehmung vorgeladen werden. Die Vorladung zur Vernehmung wurde jedoch nicht an sie, sondern an den Vater ihrer gemeinsamen Kinder adressiert. Der Vater der Kinder, der eindeutig einen anderen Nachnamen als die Petentin trägt, wohnte zufällig im gleichen Mietshaus aber in einer anderen Wohnung, in einer anderen Etage. Beide Personen waren - mit einem halben Jahr Abstand - bei der Meldebehörde getrennt gemeldet.

Die Polizei ging lapidar von einer irrtümlichen Zustellung aus. Die sachbearbeitende Beamtin habe versehentlich auf einen alten Datensatz zurückgegriffen. Zudem sei kein Namens- oder Klingelschild an der Tür angebracht gewesen.

Die inhaltliche Kenntnisgabe an den Vater der gemeinsamen Kinder stellt einen Verstoß gegen das Recht auf informationelle Selbstbestimmung der Petentin dar. Die Vorladung ist demjenigen Beteiligten bekannt zu geben, für den sie bestimmt ist. Die Vorladung betraf allein die Petentin. Die Ladung hätte, wenn tatsächlich die Notwendigkeit der Zustellung über den Vater der gemeinsamen Kinder von der Polizei bestanden hätte, zumindest in einem zweiten verschlossenen Umschlag, adressiert an die Petentin, geschehen müssen.

In der Sache erfolgte in der Polizeidirektion eine Auswertung mit der zuständigen sachbearbeitenden Beamtin. Ich gehe davon aus, dass der vorliegende Vorgang ein Einzelfall war. Ich habe deshalb von einer förmlichen Beanstandung gemäß § 29 Abs. 1 SächsDSG gegenüber der Polizeidirektion absehen, da mir diese zusicherte, dass sich ein derartiges Vorgehen nicht wiederholen und meine dargestellte Vorgehensweise bei zukünftigen Zustellungen beachtet werden wird.

5.9.9 Überschießende Amtshilfe eines Polizeibeamten bei erbetener Fahrerermittlung

Gegen einen Verwandten eines Petenten hatte ein außerhalb Sachsens gelegener Landkreis bzw. das dortige Landratsamt ein Verkehrsordnungswidrigkeitenverfahren wegen

Fahrens mit überhöhter Geschwindigkeit eingeleitet. Da unklar war, ob es sich bei dem Fahrer um den Halter des Fahrzeugs handelte, schrieb der Landrat die örtlich für den Wohnort des Petenten zuständige sächsische Polizeidienststelle an und bat um eine „Identifizierung des Betroffenen durch Personenvergleich anhand des Fotos; Ermittlung des Fahrzeugführers (durch persönliche Inaugenscheinnahme); Passbildabgleich war nicht eindeutig!“.

Im Rahmen der Akteneinsicht, die der Petent erbeten hatte, stellte sich heraus, dass die um Amtshilfe ersuchte Polizeidienststelle bei der örtlichen Ausweisbehörde gespeicherte Lichtbilder des Petenten beigezogen und der ermittelnden Behörde eine richterliche Anhörung bzw. eine Fahrtenbuchauflage vorgeschlagen hatte. Auf Nachfrage des Petenten teilte die Polizeidienststelle diesem mit, dass der Lichtbildabgleich durch § 2 PAuswG legitimiert gewesen sei.

Der von der um Amtshilfe ersuchten Polizeidienststelle vorgenommene Lichtbildabgleich war datenschutzrechtlich unzulässig. Das Schreiben des Landrates an die sächsische Polizeidienststelle war als Amtshilfeersuchen zu verstehen. Die Herrschaft über die Maßnahme, zu der die Hilfe erbeten wird, und über das Verfahren im Ganzen verbleibt bei der ersuchenden Stelle. Die ersuchende Behörde ist es auch, die die von der ersuchten Stelle durchzuführende Maßnahme benennt und umgrenzt. Bittet nun die ersuchende Behörde um die Durchführung einer konkret umschriebenen Maßnahme, hat die ersuchte Stelle insoweit kein Ermessen hinsichtlich des Einsatzes bestimmter Ermittlungsmethoden; vielmehr ist sie auf die Durchführung der von der ersuchenden Behörde konkret benannten Maßnahmen beschränkt.

Ist mit der ersuchten Amtshilfehandlung die Erhebung bzw. Verarbeitung personenbezogener Daten verbunden, dient dies der Aufgabenerfüllung der ersuchten Behörde nur insoweit, als diese zur Amtshilfe verpflichtet ist und die konkret beschriebene Maßnahme durchführt. Allein dies ist Aufgabe einer um Amtshilfe ersuchten Behörde. Maßnahmen der ersuchten Stelle, die darüber hinausgehen, können nicht der Aufgabenerfüllung der ersuchten Stelle dienen, da diese nicht für das Verfahren zuständig ist und insofern keine Aufgaben erfüllt.

Vorliegend war das Amtshilfeersuchen des Landrates eindeutig. Der Fahrzeugführer sollte nach dem Wortlaut des Ersuchens gerade nicht durch einen Lichtbildabgleich, sondern durch persönliche Inaugenscheinnahme ermittelt werden.

Auf § 2 b PAuswG konnte der Rückgriff auf das bei der örtlichen Ausweisbehörde gespeicherte Lichtbild des Petenten somit nicht gestützt werden, da § 2 b Abs. 2 Nr. 2 PAuswG voraussetzt, dass die Übermittlung des Lichtbildes für die Erfüllung einer der

(um Übermittlung) ersuchenden Behörde (hier der Polizeidienststelle) obliegenden Aufgabe erforderlich sein muss.

Die zuständige Polizeidirektion bestätigte, dass der handelnde Beamte der Polizeidienststelle die Amtshilfevorschriften unzulässig ausgedehnt hatte. Zur Vermeidung künftiger Kompetenzüberschreitungen informierte die Polizeidirektion die Leiter der nachgeordneten Reviere und Inspektionen über den Anlass meiner Kontrolle und hielt zur strengen Beachtung der Verfahrensvorschriften an.

5.9.10 Taschenfahndungskarte

Durch den BfD wurde ich auf eine neue Fahndungsmaßnahme im Bereich der Bekämpfung des islamistischen Terrorismus aufmerksam gemacht. Das BMI hatte mit Schreiben vom März 2004 mitgeteilt, dass seit September 2003 für die Polizeidienststellen eine „Taschenfahndungskarte“ eingeführt worden sei, die eine Aufstellung einheitlicher Verdachtskriterien zur Optimierung der Verdachtsgewinnung beinhalte.

Vom SMI wurde mir auf meine Nachfrage hin bestätigt, dass solche Karten auch von der sächsischen Polizei genutzt werden.

Gegen den Einsatz dieser „Taschenfahndungskarten“ bestünden dann erhebliche datenschutzrechtliche Bedenken, soweit darauf eine Verarbeitung personenbezogener Daten gestützt würde. Die dort aufgeführten Kriterien, die die Zugehörigkeit einer Person zu einem islamistischen Terroristenkreis begründen sollen, können nicht die erforderliche gesetzliche Grundlage für die Durchführung einer erkennungsdienstlichen Behandlung ersetzen. Diese besondere Art der Erhebung personenbezogener Daten ist allein auf der Grundlage von § 81 b StPO und § 20 SächsPolG zulässig.

Das SMI teilte mit, dass es meine Auffassung teile. Auf der Karte sei deshalb vermerkt, dass „kein Generalverdacht“ gegen bestimmte Gruppen bestehe und Maßnahmen ausschließlich im Rahmen der rechtlichen Zulässigkeit zu veranlassen seien. Die Karten sollten lediglich als Hilfsmittel für die Verdachtsgewinnung dienen.

Zur Vermeidung von Irritationen wollte das SMI die Vertreter der Polizeidienststellen nochmals ausdrücklich auf die Rechtslage hinweisen.

5.9.11 Blitz für Kids

Die Sächsische Polizei führte wiederholt die traditionelle zweiwöchige Verkehrssicherheitsaktion „Blitz für Kids“ durch. Zu diesem Zweck wurden in der Schulanfangszeit September/Oktober landesweit verstärkt Kontrollen zu Geschwindigkeitsüberschrei-

tungen im Bereich von Grundschulen durchgeführt. Ziel der Aktion - mit dem Slogan „Kinder stoppen Temposünder“ - sollte es sein, vor allem den Schulanfängern ein gefahrloses Erreichen der Schule zu ermöglichen und die Autofahrer speziell in dieser Zeit an Tempolimits zu erinnern.

Zu Beginn der Aktionen wurden oftmals die Schüler an den durch Polizisten durchgeführten Kontrollen direkt beteiligt. So konnten und sollten sie die Personen der zu schnell fahrenden Autos erkennen und sie im direkten Kontakt bei der Verkehrskontrolle ermahnen.

Diese Vorgehensweise habe ich kritisiert. Es ist nicht zulässig, dass die Kinder bei der Auswertung der Verkehrsverstöße durch die Polizei unmittelbar beteiligt werden. Der Pranger hat keinen Platz in unserer Rechtsordnung.

Nach meiner Anregung wird die Durchführung der Verkehrsaktion jetzt wie folgt gehandhabt: Kontrolle und die Auswertung der Verstöße erfolgen allein durch die Polizei. In der ersten Woche werden die „Verkehrssünder“ durch die Polizei auf ihr Fehlverhalten hingewiesen und aufgefordert, künftig die zulässige Höchstgeschwindigkeit nicht zu überschreiten. Statt Verwarngeldern werden bei geringfügigen Verstößen Handzettel als „gelbe Karte“ ausgeteilt. Die Kinder werden so positioniert, dass eine Identifikation der Autofahrer durch die Kinder nicht möglich ist. Sie befinden sich in einiger Entfernung hinter der Kontrollstelle (50-100 m). Nach der Kontrolle ist es den Autofahrern freigestellt, ein Gespräch mit den wartenden Kindern zu führen. Hinter dem Kontrollpunkt werden auch ordnungsgemäß fahrende Personen angehalten, um ein Gespräch mit den Kindern führen zu können. Ziel des Gespräches soll es sein, dass die Kinder die ordnungsgemäß Fahrenden loben und Ihnen Handzettel „Danke“ überreichen können.

In der zweiten Woche erfahren die „Verkehrssünder“ die vorgesehenen Sanktionen in der vollen Höhe und mit allen rechtlichen Konsequenzen.

5.10 Verfassungsschutz

In diesem Jahr nicht belegt.

5.11 Landessystemkonzept/Landesnetz

In diesem Jahr nicht belegt.

5.12 Ausländerwesen

5.12.1 Merkblätter für Ausländerbehörden zur Erkennung potenzieller islamistischer Gewalttäter

Auf meine Nachfrage bestätigte mir das SMI, dass Merkblätter zur Erkennung potenzieller islamistischer Gewalttäter für den bundesweiten Einsatz bei Ausländerbehörden konzipiert worden seien, die es an die Ausländerbehörden im Freistaat weitergeleitet hatte.

In diesen Merkblättern heißt es einleitend unter anderem, dass die Mitarbeiterinnen und Mitarbeiter der Ausländerbehörden erheblich dazu beitragen könnten, Informationen zu gewinnen, die einen Hinweis auf einen möglichen Gewalttäter geben könnten. Neben verschiedenen Kriterien (Religion, Herkunftsstaat, Familienstand usw.) enthält das Merkblatt eine Liste von Maßnahmen, die „im positiven Prüffall bzw. im Zweifelsfall zu veranlassen“ seien, unter anderem die „umgehende Benachrichtigung/Einbindung der zuständigen Polizeibehörde (prüft die Einleitung eines Ermittlungsverfahrens)“.

Als problematisch angesehen habe ich, dass die Merkblätter dahingehend missverstanden werden konnten, dass sie eine Übermittlungsbefugnis oder gar -pflicht der Ausländerbehörden begründen.

Ich wies das SMI darauf hin, dass die im Ausländergesetz enthaltenen Regelungen zur Übermittlung personenbezogener Daten durch die Ausländerbehörden abschließend sind. Im Rahmen der Vorbereitung einer ausländerrechtlichen Entscheidung kann die Behörde mit einem Auskunftsersuchen an öffentliche Stellen herantreten. Grundsätzlich übermittelt dabei die Ausländerbehörde nur die für die Identifikation einer Person erforderlichen personenbezogenen Daten und erhält ggf. von der ersuchten öffentlichen Stelle weitergehende Informationen. Öffentliche Stellen sind gesetzlich verpflichtet, die zuständige Ausländerbehörde (auch ohne deren Ersuchen) zu unterrichten, wenn sie Kenntnis von einem Ausweisungsgrund erlangen. Es wäre unzulässig, würde die Ausländerbehörde im Rahmen eines Ersuchens oder gar ohne eigenes Ersuchen der Polizeibehörde mitteilen, sie habe bei einem namentlich genannten Ausländer festgestellt, dass er diese oder jene Kriterien des Merkblattes erfüllt.

Nur ausnahmsweise ist die Ausländerbehörde selbst befugt, im Rahmen der Feststellung von Gründen für die Versagung von Aufenthaltsgenehmigungen bei ihr gespeicherte personenbezogene Daten an BND, MAD und das Zollkriminalamt sowie an das LfV und das LKA zu übermitteln.

Grundlage für die Verarbeitung personenbezogener Daten kann nur eine gesetzliche Regelung sein, die Merkblätter legitimieren eine Datenübermittlung nicht.

Ich bat das SMI, die Ausländerbehörden darauf hinzuweisen, dass die Merkblätter entgegen ihrem nicht eindeutigen Wortlaut keine Pflicht zur Übermittlung personenbezogener Daten begründen, sondern allein dem Zweck dienen können, der Ausländerbehörde konkrete Kriterien, die Ausdruck kriminalistischer Erfahrung sind, zu nennen, anhand derer sie im Einzelfall prüfen kann, ob sie eine Polizeibehörde um Erkenntnismitteilung ersucht. Rechtswidrig wäre es, die Ausländerbehörde als vorgeschalteten verlängerten Arm („Horchposten“) der Polizei einzusetzen.

Das SMI wies die Regierungspräsidien und die unteren Ausländerbehörden entsprechend darauf hin, dass die Merkblätter keine Befugnis oder Pflicht zur Übermittlung von Daten begründen.

5.12.2 Noch einmal: Akteneinsicht im Visumverfahren

Bereits in 11/5.12.1 habe ich eine Ausländerbehörde kritisiert, weil sie betroffenen Ausländern bzw. deren Anwälten eine umfassende Akteneinsicht im zustimmungspflichtigen Visumverfahren verweigert hatte.

Nunmehr hatte sich eine weitere Ausländerbehörde auf den Standpunkt gestellt, dass sie gemäß § 29 VwVfG keine Akteneinsicht in die ausländerbehördliche Akte zum Visumverfahren gewähren könne, weil die Deutsche Botschaft die federführende Behörde im Visumverfahren sei und gemäß § 2 Abs. 3 Nr. 3 VwVfG das Verwaltungsverfahrensgesetz nicht für die Vertretungen des Bundes im Ausland gelte. Auch ein auf § 18 Abs. 3 Satz 1 SächsDSG gestütztes Begehren auf Einsicht in die Akte wurde seitens der Behörde versagt. Dieses Verhalten war rechtswidrig: Ein Versagungsgrund nach § 18 Abs. 5 SächsDSG lag in keinem der Fälle vor. Die Behörde argumentierte, dass die Begründung der Ausländerbehörde gegenüber der deutschen Auslandsvertretung im Fall der Versagung der Zustimmung im Visumverfahren nicht zu den auskunftspflichtigen Daten im Sinne des Datenschutzgesetzes gehöre, da sie allein die rechtliche Würdigung an Hand der gesetzlichen Vorschriften beinhalte und kein die Person des Betroffenen berührendes Datum darstelle.

Die restriktive Auslegung des § 18 Abs. 3 SächsDSG durch die Ausländerbehörde war nicht korrekt. Denn das Auskunftsrecht nach § 18 Abs. 3 Satz 1 SächsDSG gibt dem Betroffenen ein umfassendes Recht auf Einsicht in die gesamte behördliche Akte. Nach dem Volkszählungsurteil des Bundesverfassungsgerichtes ist es erforderlich, dass der Betroffene überschauen kann, welche ihn betreffende Informationen in bestimmten

Bereichen bekannt sind und er abzuschätzen vermag, auf welchem Wissen die ihn betreffenden Entscheidungen ergehen.

Dies umfasst sowohl die persönlichen Daten des Betroffenen, die in der jeweiligen Akte gespeichert sind, als auch die dazu auf Grundlage der erhobenen Daten ergangenen Entscheidungen. Dazu gehört entgegen der Ansicht der Ausländerbehörde auch die Begründung der Ausländerbehörde gegenüber der deutschen Auslandsvertretung im Falle der Versagung der Zustimmung im Visumverfahren. Diese Begründung enthält nämlich nicht eine abstrakte rechtliche Würdigung, sondern bezieht sich gerade auf den Einzelfall, nämlich auf die konkret Antrag stellende Person.

Dass es sich gleichzeitig um eine rechtliche Stellungnahme zu den einschlägigen Normen im Visumverfahren handelt, ist nicht losgelöst von den der Entscheidung zugrunde liegenden personenbezogenen Daten (Familienstand, Alter, Herkunft, etc.) zu beurteilen. Die Entscheidung der Ausländerbehörde entsteht ja gerade erst aus dem Zusammenspiel von personenbezogenen Daten des Antragstellers mit dem Gesetz und der darauf gründenden rechtlichen Würdigung. Die konkrete Entscheidung der Ausländerbehörde hat demnach einen ausdrücklichen Bezug zu den personenbezogenen Daten des Antragstellers. Somit muss sich das Akteneinsichtsrecht auch auf diese Entscheidung und deren Begründung erstrecken, um dem Betroffenen umfassende Kenntnis zu den gespeicherten Daten und den der jeweiligen Entscheidung zugrunde liegenden Überlegungen zu ermöglichen.

Die Ausländerbehörde weigerte sich trotz meiner eindringlichen Aufforderung eine umfassende Akteneinsicht zu gewähren. Vielmehr verwies sie mich darauf, dass sie eine abschließende Klärung durch das SMI unter Beteiligung des Bundes (Auswärtiges Amt) anstrebe. Sie verkennt damit auch weiterhin, dass § 18 Abs. 3 SächsDSG nicht auslegungsbedürftig ist, sondern ein umfassendes Akteneinsichtsrecht garantiert. Sollte dieser Zustand andauern, werde ich die Stadt beanstanden.

5.12.3 Besucherbücher in Asylbewerberunterkünften

Auf meine Nachfrage, ob in Sachsen in Asylbewerberunterkünften Besucherbücher geführt werden, teilte mir das SMI mit, dass in einer Vielzahl von Asylbewerberheimen die Ausweispapiere der Heimbesucher während der Besuchszeit einbehalten werden. In anderen Unterkünften hingegen wurden auch im Freistaat Besucherbücher geführt.

Eine Speicherung personenbezogener Daten in Besucherbüchern ist für die Aufgabenerfüllung der Unterbringungsbehörden nicht erforderlich und mithin unzulässig.

Für Kontrollzwecke und um sicherzustellen, dass die Besucher nach Beendigung des Besuchs das Heimgelände wieder ordnungsgemäß verlassen, ist ausreichend, dass Gäste ihren Lichtbildausweis während der Besuchszeit an der Pforte hinterlegen (solch ein Verfahren habe ich bereits als datenschutzrechtlich nicht zu beanstanden bewertet - vgl. 5/5.12). Eine Speicherung persönlicher Daten in Besucherbüchern ist für die Aufgabenerfüllung der Unterbringungsbehörden nicht erforderlich und mithin unzulässig.

In diesem Zusammenhang habe ich das SMI darauf aufmerksam gemacht, dass diese Rechtslage auch für privat geführte Asylbewerberunterkünfte gilt.

In diesen Einrichtungen werden im Rahmen einer übertragenen öffentlichen Aufgabe personenbezogene Daten im Auftrag verarbeitet (§ 7 Abs. 1 SächsDSG), so dass die für die übertragenden Behörden maßgeblichen öffentlich-rechtlichen datenschutzrechtlichen Vorschriften auch von den privaten Unterkunftsbetreibern zu beachten sind.

Das Staatsministerium sagte zu, die unteren Unterbringungsbehörden anzuweisen, zu veranlassen, dass künftig in den Asylbewerberunterkünften keine Besucherbücher mit personenbezogenen Daten mehr geführt werden.

5.13 Wahlrecht

In diesem Jahr nicht belegt.

5.14 Sonstiges

5.14.1 Auswirkungen des Urteils des Bundesverfassungsgerichtes zum großen Lauschangriff vom 3. März 2004

Das Urteil des Bundesverfassungsgerichtes vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 1084/99) hat Auswirkungen auf die Anwendung der einschlägigen Landesgesetze. Die im Urteil aufgeführten Grundrechtsgarantien, die einen entscheidenden Einfluss auf die Ausgestaltung von Strafverfolgungsmaßnahmen haben, müssen auch für entsprechende Grundrechtseingriffe im präventiven Bereich berücksichtigt werden.

Ich habe - wie die Landesbeauftragten der anderen Bundesländer auch – meine Bedenken und Überlegungen dem zuständigen SMI mitgeteilt. Die Arbeitskreise Justiz und Sicherheit veranstalteten eine ad-hoc Arbeitsgruppe, um eine einheitliche Stellungnahme zu erarbeiten. Wie sich die vom Bundesverfassungsgericht formulierten Beanstandungen im präventiven Bereich auswirken werden, bleibt abzuwarten. Da das Polizeirecht in die Zuständigkeit der Länder fällt, ist mit einer unterschiedlichen Umsetzung und Bearbeitung zu rechnen.

Hinsichtlich der sächsischen Gesetze formulierte ich gegenüber dem SMI folgende Punkte:

1. Sächsisches Polizeigesetz

§ 40 SächsPolG regelt die Erhebung von Daten in oder aus Wohnungen durch den Einsatz besonderer Mittel. Diese werden in § 36 Abs. 2 Nr. 2 SächsPolG benannt, nämlich der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und -aufzeichnungen sowie das Abhören und Aufzeichnen des gesprochenen Wortes. Gemäß § 39 Abs. 2 Satz 1 SächsPolG ist die Datenerhebung mit besonderen Mitteln unzulässig, soweit sie in ein geschütztes Vertrauensverhältnis eingreifen würde.

- Das Sächsische Polizeigesetz schützt jedoch den Kernbereich der privaten Lebensgestaltung nicht ausreichend. Insbesondere fehlen bei der Wohnraumüberwachung spezifische verfahrenssichernde Bestimmungen über den Abbruch von Überwachungsmaßnahmen, wenn in den Kernbereich privater Lebensgestaltung eingegriffen wird. Das BVerfG formuliert die Anforderungen an die Rechtmäßigkeit der Wohnraumüberwachung umso strenger, je größer das Risiko ist, dass in ihrem Rahmen Gespräche höchstpersönlichen Inhalts erfasst werden könnten. So muss die Überwachung in Situationen von vornherein unterbleiben, in denen Anhaltspunkte bestehen, dass die Menschenwürde durch die Maßnahme verletzt wird. Führt die Überwachung unerwartet zur Erhebung von absolut geschützten Informationen, muss sie abgebrochen werden und die Aufzeichnungen müssen gelöscht werden; jede Verwendung im Rahmen der Strafverfolgung - erst recht im präventiven Bereich - erhobener absolut geschützter Daten ist ausgeschlossen.

- Es fehlen Bestimmungen über ein Verwertungsverbot für Daten, die bei einer ausnahmsweise vorkommenden Verletzung des Kernbereiches erhoben worden sind. Ferner muss gesichert sein, dass Informationen aus dem unantastbaren Bereich privater Lebensgestaltung nicht zum Anknüpfungspunkt weiterer Ermittlungen werden.

- Die Anordnung des Einsatzes besonderer Mittel ist gemäß § 39 Abs. 3 Satz 1 SächsPolG zu befristen. Es gibt im Sächsischen Polizeigesetz keine Höchstfrist. Die Effektivität der richterlichen Anordnungs- und Prüfungsbefugnisse erfordert im Hinblick auf den einschneidenden Eingriff der akustischen Wohnraumüberwachung eine vorausschauende Beurteilung, die verantwortungsvoll nur für einen überschaubaren Zeitraum (Frist) vorgenommen werden kann. Zudem könnte die Maßnahme unzulässigerweise zu einer Dauermaßnahme ausarten, da eine Verlängerung mit neuer Anordnung gesetzlich möglich ist.

- Das Sächsische Polizeigesetz bestimmt, dass verdeckte Maßnahmen einer richterlichen Anordnung bedürfen (§ 36 Abs. 2 Nr. 2 SächsPolG). Bei Gefahr im Verzug und dadurch bedingter Anordnung durch die in § 39 Abs. 4 Satz 1 SächsPolG genannten Personen ist die Maßnahme binnen drei Tagen vom Amtsgericht zu bestätigen, § 39 Abs. 4 Satz 5 SächsPolG. Die richterliche Anordnung in der Strafverfolgung muss gemäß Art 13 Abs. 3 Satz 3 GG grundsätzlich durch einen mit drei Richtern besetzten Spruchkörper getroffen werden. Nur bei Gefahr im Verzug genügt nach Satz 4 die Anordnung eines einzelnen Richters; eine Anordnung der Staatsanwaltschaft oder ihrer Hilfsbeamten reicht selbst im Eilfall nicht aus. Damit soll dem besonderen Gewicht des durch Art. 13 Abs. 3 GG zugelassenen Grundrechtseingriffs Rechnung getragen werden (vgl. BT-Drs. 13/8650, S. 5). Unter Beachtung dieser verfassungsrechtlichen Grundsätze erscheint die sächsische Regelung für den präventiven Bereich als ungenügend, da in das gleiche Rechtsgut eingegriffen wird wie bei der Strafverfolgung.

Gemäß § 39 Abs. 8 Satz 1 SächsPolG sind die Betroffenen nach Abschluss der Maßnahme, nämlich den Einsatz besonderer Mittel zur Erhebung von Daten, unverzüglich zu unterrichten, sobald dies ohne Gefahr für Leben, Gesundheit oder Freiheit einer Person oder ohne Gefährdung des Zwecks der Datenerhebung erfolgen kann. Die Unterrichtung über den Einsatz eines verdeckten Ermittlers unterbleibt, soweit sie nicht ohne Gefährdung von Leib oder Leben oder der weiteren Verwendung des verdeckten Ermittlers geschehen kann, § 39 Abs. 9 Satz 2 SächsPolG. Diese letzte Alternative erscheint im Lichte des Urteils des BVerfG als nicht mehr haltbar.

Denn das Gericht führt hierzu aus: Die Grundrechtsträger haben einen Anspruch, grundsätzlich über Maßnahmen der akustischen Wohnraumüberwachung informiert zu werden. Zu benachrichtigen sind neben dem Beschuldigten die Inhaber und Bewohner einer Wohnung, in denen Abhörmaßnahmen durchgeführt worden sind. Dies gilt auch für Drittbetroffene, es sei denn, durch Recherchen über ihre Namen und Adressen wird der Eingriff in das Persönlichkeitsrecht vertieft. Unbedenklich ist es, die Benachrichtigung zurückzustellen, wenn andernfalls der Untersuchungszweck oder Leib und Leben einer Person gefährdet sind. Demgegenüber reicht die Gefährdung der - nur pauschal in Bezug genommenen - öffentlichen Sicherheit oder der Möglichkeit des weiteren Einsatzes eines nicht offen ermittelnden Beamten nicht zur Zurückstellung der Benachrichtigung.

Die oben genannte Erwägungen zu Kernbereich, Rundum-Überwachung und Verwertungsverbot gelten auch für die anderen besonderen Mittel zu Erhebung von Daten, insbesondere der längerfristigen Observation im Sinne des § 36 Abs. 2 Nr. 1 SächsPolG und dem Einsatz eines verdeckten Ermittlers im Sinne der §§ 36 Abs. 2 Nr. 3, 41 SächsPolG.

2. Gesetz zur Ausführung des Gesetzes zu Art. 10 GG im Freistaat Sachsen

§ 1 SächsAG G 10 bestimmt, dass der Staatsminister des Inneren oder seine Stellvertreter die Anordnungen treffen. Die Entscheidung zur Anordnung obliegt der Kommission, die aus einem Vorsitzenden und zwei Beisitzern besteht. Ein Richtervorbehalt ist nicht vorgesehen. Zudem muss nur der Vorsitzende die Befähigung zum Richteramt oder gar nur die erste Staatsprüfung im Sinne der §§ 5 und 6 des Deutschen Richtergesetzes oder einen nach Einigungsvertrag gleichgestellten Abschluss besitzen. Dies ist keine gleichwertige Verfahrensabsicherung wie durch einen gerichtlichen Spruchkörper. Eine entsprechende Änderung des Gesetzes ist anzustreben.

3. Sächsisches Verfassungsschutzgesetz

Nach § 5 Abs. 4 Nr. 2 SächsVSG darf eine Informationsgewinnung im Schutzbereich des Art. 13 GG nur erfolgen, wenn tatsächliche Anhaltspunkte für den Verdacht vorliegen, dass Straftaten nach § 100 c StPO oder §§ 331 bis 334 StGB die freiheitlich demokratische Grundordnung des Bundes oder eines Landes oder Leben, Gesundheit oder Freiheit einer Person oder bedeutende fremde Sach- oder Vermögenswerte gefährden. Ein Rückgriff auf die in § 100 c StPO genannten Straftaten ist nach der Rüge und Nachbesserungsaufforderung durch das Bundesverfassungsgericht bedenklich. Jedenfalls sollte das Sächsische Verfassungsschutzgesetz i. V. m. § 100 c StPO bis zur Anpassung durch den Bundesgesetzgeber nur restriktiv angewandt werden.

Im Sächsischen Verfassungsschutzgesetz fehlt wie im Sächsischen Polizeigesetz eine Vorschrift zum Abbruch der Überwachungsmaßnahmen, wenn in den absolut geschützten Kernbereich des Art. 13 GG eingegriffen wird. Es fehlt ein Verwertungsverbot für die unter Verstoß gegen den Kernbereich der Menschenwürde erlangten Kenntnisse. Insoweit wird auf die vorstehenden Ausführungen zum Polizeigesetz verwiesen.

Eine Unterrichtung über die durchgeführten Maßnahmen ist in § 5 Abs. 9 SächsVSG vorgesehen. Eine Unterrichtung muss nach Maßgabe der Entscheidung des Bundesverfassungsgerichtes auch erfolgen, wenn ein möglicher weiterer Einsatz einer für den Verfassungsschutz tätigen Person dadurch ausgeschlossen oder beschränkt wird. Der Informationsanspruch des Betroffenen wiegt insoweit höher. Auf obige Ausführungen wird verwiesen.

5.14.2 Einsicht in bzw. Auskunft aus personenbezogenen Unterlagen öffentlicher Stellen

Mehrfach kam es im Berichtszeitraum vor, dass Personen sich an mich wandten, weil ihrem Begehr auf Einsicht in zu ihnen geführten Akten öffentlicher Stellen bzw. auf Auskunft über zu ihrer Person gespeicherten Daten nicht entsprochen wurde.

Teilweise blieben entsprechende Anfragen unbeantwortet, teilweise verweigerte die öffentliche Stelle die Einsicht/Auskunft mit abwegigen Begründungen. Mehrfach wies die öffentliche Stelle darauf hin, dass nur der Schriftwechsel mit dem Betroffenen gespeichert worden sei und somit der Betroffene denselben Datenbestand in seinen Unterlagen vorfinden könne. Des Öfteren wurde die Einsicht mit dem Hinweis verwehrt, dem Betroffenen sei bereits einige Monate zuvor Akteneinsicht gewährt worden. Eine oberste Landesbehörde sah sich zu einer Entscheidung über einen Antrag auf Akteneinsicht nicht in der Lage, da der Antrag nicht begründet worden sei.

Das Auskunftsrecht als zentrales Datenschutzrecht ist notwendige Bedingung für die Transparenz staatlichen Handelns. Es ist zugleich eine Vorbedingung für die Geltendmachung der weitergehenden Rechte auf Berichtigung, Sperrung und Löschung von Daten oder des Schadenersatzanspruches. Der Anspruch des Betroffenen ergibt sich, sofern keine spezialgesetzlichen Regelungen getroffen sind, aus § 18 SächsDSG.

Nur unter den in den Absätzen fünf bis sieben dieser Norm beschriebenen Voraussetzungen unterbleibt die Erteilung einer Auskunft aus personenbezogenen Unterlagen.

Grundsätzlich besteht der Auskunftsanspruch des Betroffenen voraussetzungslos. Das Gesetz trifft insbesondere keine Aussage über eine etwaige Höchstzahl zulässiger Antragstellungen innerhalb eines bestimmten Zeitraumes oder über das Erfordernis, den Antrag auf Auskunft zu begründen. Von einer rechtsmissbräuchlichen Antragstellung - dieser Vorwurf tauchte vereinzelt auf -, die unter Umständen einer Gewährung der Akteneinsicht entgegensteht, ist allenfalls in Extremfällen auszugehen, keinesfalls aber schon dann, wenn der letzte Einsichtstermin mehrere Wochen zurückliegt.

Die Pflicht zur Begründung ihrer Entscheidung trifft allein die öffentliche Stelle, wenn diese den Antrag auf Auskunft oder Einsicht ablehnt. Die ablehnende Entscheidung ist ein belastender Verwaltungsakt, der grundsätzlich zu begründen und mit einer Rechtsmittelbelehrung zu versehen ist. In einigen der mir vorgelegten Fälle schien sich die Akteneinsicht verwehrende Stelle darüber nicht bewusst zu sein.

In sämtlichen Fällen im Berichtszeitraum wurde den Betroffenen schließlich - nach meinen Hinweisen an die jeweilige öffentliche Stelle - Akteneinsicht bzw. Auskunft gewährt oder aber die Nichtgewährung nachvollziehbar begründet.

5.14.3 Platzverweis aufgrund eines Sperrbezirkes

Ein Petent meldete sich bei mir und schilderte ein Ereignis, das ihn sehr verunsicherte: Er habe, nachdem er längere Zeit habe warten müssen, ein dringendes Bedürfnis verspürt. Da sich an dieser Stelle ein verwildertes nicht abgesperrtes Grundstück befand, verschwand er schnell „hinter den Büschen“. Als er nach dem Urinieren wieder auf die Straße trat, wurde er von zwei Mitarbeitern des Ordnungsamtes der Stadt angesprochen. Sie wiesen ihn darauf hin, dass er soeben eine Handlung begangen habe, die hier aufgrund einer Sperrbezirksverordnung der Stadt nicht geduldet werde. Der Bürger wehrte sich gegen diese Beschuldigung, mit dem Ergebnis, dass seine Personalien aufgenommen und ihm ein Platzverweis für vier Tage ausgesprochen wurde.

Der Petent wusste, dass die Straße mit dem dazugehörigen verwilderten Trümmergrundstück in den Abend- und Nachtstunden eine von Strichern frequentierte Örtlichkeit darstellte. Auf seine Nachfrage bei dem nächstgelegenen Polizeirevier wurde ihm die Existenz des Platzverweises bestätigt. Er wandte sich nunmehr an mich und wollte wissen, wo überall seine Daten gespeichert seien und an wen sie weitergeleitet wurden. Es bestand sogar der Verdacht, dass einschlägige „rosa Listen“ geführt werden.

Ich habe daraufhin beim Ordnungsamt der Stadt kontrolliert. Ein Erfolg stellte sich wegen des verzögernden Handelns des Amtsleiters erst nach mehreren Anläufen ein (siehe 12/1.4).

In der Sache stellte ich Folgendes fest: Die Stadt hat eine operative Einsatzgruppe aus zivilen Kräften, deren Aufgabengebiet die Drogenszene, die Straßenprostitution und die Stricherszene umfasst. Das Ziel der Operativgruppe ist in erster Linie die Verdrängung der oben genannten Szene mittels der in § 21 Abs. 1 und 2 SächsPolG eröffneten Maßnahmen: Platzverweis und Aufenthaltsverbot.

Fallen den Bediensteten „bekannte Personen“ oder bestimmte Handlungen auf, werden die betreffenden Personen angesprochen und auf § 4 der Städtischen Polizeiverordnung (Sperrgebiete) hingewiesen. Sollte sich der Bürger uneinsichtig zeigen, so wird unter Umständen ein Platzverweis gem. § 21 Abs. 1 SächsPolG ausgesprochen (mündlich). Dazu werden folgende Daten der Person aufgenommen: Name, Vorname, Geburtsdatum. Die Anschrift oder andere Daten werden nicht erfasst. Im Rahmen eines Platzverweises, der über einen längeren Zeitraum geht, erfolgt eine schriftliche Meldung an die örtlich zuständige Polizeidienststelle. Per Fax werden hierbei oben genannte Perso-

nalien sowie die Dauer des Platzverweises übermittelt. Das Ordnungsamt kann nach einem Platzverweis ein Ordnungswidrigkeitenverfahren einleiten. In der Sache ist dies bis zu meiner Kontrolle noch nicht geschehen.

Nach Ablauf der Frist des Platzverweises werden die Faxe in der Polizeidienststelle geschreddert. Eine Recherche zu meinem Petenten verlief in allen Datenbeständen der Polizei ergebnislos. Eine weitere Übermittlung an andere Stellen war nicht erfolgt.

Gegen die Erteilung der Platzverweise bestehen keine datenschutzrechtlichen Bedenken. Mündlich erteilte Platzverweise sind gemäß §§ 35, 37 Abs. 2 Satz 1 VwVfG i. V. m. § 1 Satz 1 SächsVwVfG Verwaltungsakte, die bei berechtigtem Interesse und unverzüglichem Verlangen des Betroffenen schriftlich zu bestätigen sind, § 37 Abs. 2 Satz 2 VwVfG. Aus diesem Grund ist es zulässig, die aufgenommenen personenbezogenen Daten (Name, Vorname, Geburtsdatum) des Betroffenen zu erheben und zu verarbeiten.

Ich habe empfohlen, dass die Dauer der Speicherung sich an der Jahresfrist des § 58 Abs. 2 VwGO orientieren sollte. Der Platzverweis, als Verwaltungsakt, ist, auch wenn er sich innerhalb von Tagen erledigt haben sollte, durch den Betroffenen mittels der Fortsetzungsfeststellungsklage überprüfbar.

Gleichzeitig ist es erforderlich, dass nach Ablauf des Platzverweises ein Zugriff der Behörde auf die Daten nicht mehr erfolgen kann, denn die Daten sind für die weitere Aufgabenerfüllung der Behörde nicht erforderlich. Aus diesem Grund sind die Daten zu sperren, § 21 Abs. 1 Nr. 2 i. V. m. § 20 Abs. 4 Nr. 1 SächsDSG, und nur im Falle eines Gerichtsverfahrens zu verwenden. Diesen Hinweis habe ich dem Ordnungsamt erteilt.

6 Finanzen

6.1 Auskunft des Finanzamtes über die Gemeinnützigkeit von Vereinen

Ein Bürger hatte wegen der Gemeinnützigkeit ortsansässige Vereine beim zuständigen Finanzamt nachgefragt und um eine Liste der Vereine gebeten. Das Finanzamt teilte ihm mit, dass aufgrund des Steuergeheimnisses und aus datenschutzrechtlichen Gründen die gewünschten Auskünfte nicht erteilt werden dürften. Er wandte sich mit der Bitte um Prüfung an mich.

Die Finanzämter haben gemäß § 30 AO das Steuergeheimnis zu wahren. Die Frage, ob ein Verein gemeinnützig und deshalb steuerlich begünstigt ist, ist eine Angabe über steuerliche Verhältnisse dieses Vereins und wird durch das Steuergeheimnis geschützt. Allerdings ist die Offenbarung der Tatsache der Gemeinnützigkeit zulässig, soweit sie der Durchführung eines Verwaltungsverfahrens, eines Rechnungsprüfungsverfahrens oder eines gerichtlichen Verfahrens in Steuersachen dient (§ 30 Abs. 4 Nr. 1 AO). Die Verhältnisse anderer dürfen auch offenbart werden, wenn diese Verhältnisse in unmittelbarer Beziehung zur Besteuerung eines Steuerpflichtigen stehen, so zum Beispiel auch bei Prüfung der Gemeinnützigkeit eines Spendenempfängers.

Regelmäßig wird sich die Anfrage eines Bürgers an das Finanzamt auf die Gemeinnützigkeit eines konkreten Vereins beschränken, zu dem bereits ein gewisses Näheverhältnis besteht und der möglicherweise selbst öffentlich für sich in Anspruch nimmt, gemeinnützig zu sein. Das Finanzamt darf in solch einem Fall mitteilen, ob der Verein gemeinnützig im Sinne der Abgabenordnung ist, die Verletzung des Steuergeheimnisses ist gemäß § 30 Abs. 4 Nr. 1 AO gerechtfertigt. Allerdings besteht auch in dieser Konstellation keine Auskunftspflicht des Finanzamtes. Erst recht ist das Finanzamt nicht verpflichtet, zur Gemeinnützigkeit einer großen Anzahl von Vereinen Stellung zu nehmen.

Als sachdienlich und dem Bürger zumutbar erscheint aus meiner Sicht der Ansatz, sich zunächst an bestimmte Vereine zu wenden und diese um Auskunft über die Gemeinnützigkeit zu bitten. Der oder die angesprochenen Vereine werden die Auskunft bereitwillig geben und gegebenenfalls ihre Einstufung als gemeinnützig nachweisen. Im Zweifelsfall kann dann eine Nachfrage beim zuständigen Finanzamt erfolgen, die sich aber - im Gegensatz zu einer umfangreichen Liste - auf einen oder wenige Vereine beschränken würde.

6.2 Vollzug der Hundesteuersatzung

Die Abteilung Gewerbe- und sonstige Steuern einer Stadtkämmerei beabsichtigte den Vollzug der Hundesteuersatzung mit den allgemeinen ordnungsdienstrechtlichen Aufgaben zu verknüpfen und dem Stadtordnungsdienst zu übertragen. Mit der Vorortkontrolle des Hundeführers (Anleinen der Hunde, Kotbeseitigung) sollte nun auch geprüft werden, ob der mitgeführte Hund steuerlich registriert ist. Dem Stadtordnungsdienst sollten über ein eigens dafür erstelltes Auskunftsprogramm in einer Datei alle bei der Stadt gemeldeten Hundehalter mit Name, Vorname, Anschrift, Kassenzeichen und Hundemarke zur Verfügung gestellt werden. Dazu habe ich mich wie folgt geäußert:

Die Hundesteuersatzung hat die Ratsversammlung dieser Stadt zu dem Zweck erlassen (die Rechtsgrundlage geschaffen), um gemäß § 2 SächsKAG die Hundesteuer einziehen zu können. Alle mit diesen im Zusammenhang stehenden Verwaltungsaufgaben können *nicht* dem Stadtordnungsdienst übertragen werden. Auch bei der Aufklärung von Ordnungswidrigkeiten nach §§ 11 und 12 Hundesteuersatzung ist er nicht beteiligt. Denn es handelt sich dabei um die Überprüfung einer eventuellen möglichen leichtfertigen Abgabenverkürzung und Abgabengefährdung nach § 6 SächsKAG, die der Abteilung Gewerbe- und sonstige Steuern unterfallen, *nicht* dem Stadtordnungsdienst.

Ferner sind auf die Hundesteuer auch die Bestimmungen der Abgabenordnung (AO) in der jeweils geltenden Fassung anzuwenden. Danach darf nur in Schadensfällen, etwa i. S. v. § 12 GefHundG, das Steuergeheimnis gemäß § 30 AO offenbart werden (das sind nicht Ordnungswidrigkeiten nach §§ 11 und 12 Hundesteuersatzung); also Auskunft über Namen und Anschrift des Hundehalters gegeben werden (vgl. § 3 Abs. 1 Nr. 1 Buchstabe c, bb SächsKAG). Die in § 30 Abs. 4 Nr. 5 AO enthaltene Offenbarungsmöglichkeit im Falle eines zwingenden öffentlichen Interesses umfasst zwar grundsätzlich auch Zwecke der Gefahrenabwehr, allerdings muss es sich dann um die Abwehr einer konkreten Gefahr für erhebliche Rechtsgüter handeln. Eine solche liegt aber bei der generell beabsichtigten Einsichtnahme in die Hundesteuerkartei (hier die Übermittlung der Datei/Liste aller Hundehalter) nicht vor, so dass diese dem Stadtordnungsdienst verwehrt ist. Darüber hinaus käme diese Datei der Erhebung von Daten auf Vorrat gleich und ist mit dem Erforderlichkeitsgrundsatz nicht vereinbar und daher unzulässig („Das Sammeln nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmten Zwecken ist mit dem Gebot der notwendigen Festlegung des Verwendungszweckes nicht vereinbar“ - BVerfGE 65, 1/46).

Eine Änderung der Hundesteuersatzung im Hinblick auf eine Datenübermittlung an den Stadtordnungsdienst würde keine Abhilfe bringen. Es bliebe bei der Verletzung des

Steuergeheimnisses. Satzungsrecht hat mit den steuergesetzlichen Bestimmungen im Einklang zu bleiben.

Eine datenschutzfreundliche Lösung besteht nach meinem Dafürhalten darin, dass Verfahren in der Weise „umzukehren“, dass der Stadtordnungsdienst mit dem Vollzug seiner ordnungsdienstrechtlichen Aufgaben alle die Hundeführer, die die vorgegebenen Normen (über Leinen- und Maulkorbpflicht, Beseitigung von Hundekot, Vorhalten der Hundemarke gemäß § 12 Abs. 1 Satz 2 Hundesteuersatzung) verletzt haben, kontrolliert. Die dabei zu erhebenden erforderlichen Angaben (Name und Anschrift des Hundehalters) können dann in den jeweiligen Fällen der fehlenden Hundemarke dem Steueramt in geeigneter Weise übermittelt werden. Die Abteilung Gewerbe- und sonstige Steuern kann dann entsprechend ihren Vorgaben nach Sächsischem Kommunalabgabengesetz und der Hundesteuersatzung tätig werden.

Die Erarbeitung eines „Auskunftsprogramms“ für den Stadtordnungsdienst war daher entbehrlich. Die regelmäßige Datenübermittlung aller gemeldeten Hundehalter nach Namen, Vornamen, Anschrift, Kassenzeichen und Hundemarke wurde nicht durchgeführt. Die Stadtverwaltung hat mir ferner schriftlich bestätigt, dass bereits übermittelte Daten und die ggf. in Papierform vorliegenden Listen nachweislich gelöscht bzw. vernichtet wurden.

6.3 Kontostammdatenabruf durch Behörden aufgrund steuer- und finanzrechtlicher Bestimmungen

Das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b AO Bestimmungen, die in das Grundrecht auf informationelle Selbstbestimmung der Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung eingreifen. Ziel der Vorschriften ist u. a. die Herstellung der Steuergerechtigkeit durch eine entsprechende Datengrundlage des Staates. Die Neuregelung erlaubt den Zugriff auf die Kontostammdaten der Bankkunden und sonstigen Verfügungsberechtigten, also auf Namensangaben, Geburtsdatum, Kontonummern und Bankdepots. Auf diese Weise erfahren die Behörden, ob ihnen die Existenz von Bankkonten vorenthalten worden ist, hingegen können damit aber noch keine Kontostände und Geldbewegungen in Erfahrung gebracht werden. Erst in einem zweiten Verfahrensschritt können Behörden auf den Kontoinhalt und die Kontobewegungen zugreifen.

Es sollen aber nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden, die Verfahren betreiben, die an einkommenssteuerrechtliche Tatbestände anknüpfen, über die Finanzbehörden auf die Daten im Wege eines automati-

sierten Abrufverfahrens Zugriff erhalten. Technisch soll nach dem Gesetz zudem dafür seitens der Kreditinstitute, die gesetzlich verpflichtet sind, die Daten bereit zu halten, Sorge getragen werden, dass der einzelne Abruf nicht bei der Datenbank verwaltenden Stelle registriert wird. Die Unüberschaubarkeit, was den Zugriff einer Vielzahl nicht näher genannter Behörden und was die unscharfen Voraussetzungen angeht, widerspricht dem Grundsatz der Normenklarheit. Die systemwidrige Heimlichkeit entspricht nicht dem Transparenzgebot und trägt nicht zur Datensicherheit bei.

Das Bundesverfassungsgericht lehnte es mit Beschluss vom 22. März 2005 (1 BvR 2357/04) zwar ab, eine einstweilige Anordnung gegen das am 1. April 2005 in Kraft getretene „Gesetz zur Förderung der Steuerehrlichkeit“ zu erlassen, dennoch ist der Rechtsstreit um die Verfassungsmäßigkeit des automatisierten Kontostammdatenabrufs noch nicht in der Hauptsache entschieden. Die Verfassungsmäßigkeit der automatischen Kontenabfrage bleibt weiterhin zweifelhaft. Ich hatte viele Anfragen der Presse und besorgter sächsischer Bürger zu der Thematik zu beantworten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer von mir mitgetragenen Entschließung gefordert, die Regelungen mit dem Ziel zu überarbeiten, dass das Recht auf informationelle Selbstbestimmung gewährleistet wird und das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens Beachtung findet (vgl. Entschließung unter 16.2.12).

Das BMF reagierte nach der z. T. mit einem großem Medieninteresse begleiteten Kritik mit einem konkretisierenden Erlass, mit dem verfügt wurde, dass Abrufe der Kontostammdaten nur anlassbezogen, zielgerichtet und nur unter Bezugnahme auf eindeutig bestimmte Personen zulässig sei. Ferner wurde in dem Erlass die Benachrichtigung der Betroffenen in verschiedenen Verfahrensstadien geregelt. Gleichwohl können interne Verwaltungsanordnungen keine unzureichenden gesetzlichen Bestimmungen ersetzen. Der Gesetzgeber ist gefragt.

Ich werde die Abrufpraxis sächsischer Behörden kontrollieren.

6.4 Befugnisse des Sächsischen Rechnungshofes zur Verarbeitung personenbezogener Daten

Mehrfach habe ich von Behörden Anfragen erhalten, inwieweit der Sächsische Rechnungshof (SRH) befugt ist, personenbezogene Daten zu verarbeiten. Mir wurde z. B. die Frage gestellt, ob die Einsichtnahme in Akten bzw. die Übersendung von Akten und Unterlagen bei Prüfvorgängen des SRH datenschutzrechtlich zulässig sei.

Die Tätigkeit des SRH ist zunächst als sächsische öffentliche Stelle im Sinne von § 2 Abs. 1 SächsDSG nicht von der datenschutzrechtlichen Aufsicht durch den Sächsischen Datenschutzbeauftragten ausgenommen (vgl. § 27 SächsDSG).

Datenübermittlungen an den SRH richten sich im Wesentlichen nach § 95 SäHO. Die Frage, ob der SRH interne Berichte und Unterlagen der Innenrevision einzelner Behörden zu erhalten befugt ist, habe ich bejaht. Der SRH kann sich bei der Verarbeitung personenbezogener Daten auf § 95 Abs. 1 SäHO stützen, wonach ihm Unterlagen, die er für erforderlich hält, vorzulegen oder zu übersenden sind. Prüfungen des SRH erstrecken sich auch auf Vorgänge der Innenrevision im Zusammenhang mit dem Verbrauch von Haushaltsmitteln. Auch die Frage einer obersten Dienstbehörde, ob dem SRH Auskünfte in Bezug auf Vor- und Zunamen von in bestimmten Organisationseinheiten tätigen Mitarbeitern gegeben werden dürfen, habe ich bejaht. Die Rechtsgrundlage für Auskünfte ist § 95 Abs. 2 SäHO. Prüfungen des SRH haben auch den Personalaufwand öffentlicher Stellen zum Inhalt und erfolgen auch mittels Organisationsuntersuchungen.

Aus § 13 Abs. 3 SächsDSG ergibt sich, dass die bei der vom SRH kontrollierten Stelle, z. B. zu Innenprüfzwecken entstandenen oder ohnehin in der Personalverwaltung vorhandenen personenbezogenen Daten auch in vom SRH eingeleiteten Prüfverfahren weiterverarbeitet werden dürfen. Bei den Prüfungen des SRH handelt es sich um ein aufsichtliches Tätigwerden im Sinne von § 13 Abs. 3 SächsDSG. Die Vorschrift erwähnt die „Rechnungsprüfung“ ausdrücklich. Im Rahmen des § 95 Abs. 1 und 2 SäHO ist der SRH auch zunächst nicht beschränkt. Weder hat die kontrollierte Stelle die Erforderlichkeit zu prüfen noch haben die Betroffenen die Einwilligung in die Datenverarbeitung des SRH zu erteilen. Der SRH entscheidet selbst über die Erforderlichkeit der Vorlage von Unterlagen bzw. die Auskunft. Anderenfalls wäre eine wirksame Finanzkontrolle im Freistaat durch den SRH nicht möglich. Das Bundesverfassungsgericht hat das Grundrecht auf informationelle Selbstbestimmung gegenüber dem grundrechtlich geschützten Interesse an einer wirksamen und leistungsfähigen Finanzkontrolle als nicht vorrangig angesehen (Heuer, Kommentar zum Haushaltsrecht, Stand Mai 2004, § 95 BHO Erl. 20 m. w. N.). Die Stellung und Unabhängigkeit des SRH wird darüber hinaus in Art. 100 Abs. 1 SächsVerf betont. Dennoch bleiben betroffene Grundrechtsträger - zumeist wird es sich um Bedienstete handeln, die durch Angaben betroffen sind - nicht ungeschützt. Der SRH erhebt für seine Prüfung erforderliche personenbezogene Daten im Rahmen eines gesetzmäßigen Verwaltungsermessens. Das bedeutet auch, dass die Verarbeitung und Erhebung von personenbezogenen Daten am Verhältnismäßigkeitsgrundsatz zu orientieren ist.

In beiden erwähnten Vorgängen war nicht erkennbar, dass die Verarbeitung der personenbezogenen Daten der Betroffenen durch den SRH nicht zum Verständnis erforderlich gewesen wäre bzw. wegen des Persönlichkeitsrechts Einzelner hätten eingeschränkt werden müssen. Anhaltspunkte hierfür wurden mir seitens der anfragenden Stellen auch nicht mitgeteilt. Der SRH hat auch die Befugnis, sensible Daten im Rahmen seiner Aufgabenerfüllung einzusehen und hierzu Daten zu verarbeiten, selbst wenn diese einer besonderen Verschwiegenheitspflicht unterliegen. Dies gilt z. B. auch für Personalunterlagen und auch Personalakten. Insofern sind Verkürzungen der Akten oder Schwärzungen ohne weitere Anhaltspunkte für ein Überwiegen von Persönlichkeitsrechten Einzelner gegenüber dem SRH nicht angebracht. Bei der Bereitstellung der Daten für den SRH ist hingegen seitens der geprüften Dienststelle auf eine datenschutzgerechte Verfahrensweise zu achten. Bei der Auskunftserteilung an den SRH ist die notwendige Vertraulichkeit herzustellen und sind die beteiligten Organisationseinheiten und Bediensteten zu minimieren. Sofern Personalakten an den SRH übersandt werden sollen, was nach § 95 Abs. 1 SäHO möglich ist, ist es Angelegenheit des SRH selbst, die Erforderlichkeit zu Prüfzwecken einzuschätzen. Regelmäßig werden aber lediglich bestimmte Aktenstücke aus Personalakten benötigt. Personalakten sollten auch grundsätzlich in der jeweiligen Dienststelle verfügbar bleiben können. Insofern sollte bei der Versendung von Personalakten und auch bei anderen besonders sensiblen Aktenbeständen bzw. Daten mit einer gebotenen Zurückhaltung verfahren werden.

Bei der Veröffentlichung des Jahresberichtes nach § 97 SäHO bzw. § 2 RHG hat der SRH darauf zu achten, dass nur zur Aufgabenerfüllung erforderliche personenbezogene Daten veröffentlicht werden und Persönlichkeitsrechte und das Grundrecht auf informationelle Selbstbestimmung Betroffener bei einer Darstellung gegenüber der Öffentlichkeit berücksichtigt werden.

6.5 Kfz-Stilllegung im unspezifischen Vollstreckungsverfahren - Einsatz der „Parkkralle“

„Finanzämter … setzen künftig Parkkralle ein / Leider gibt es viele Steuerpflichtige die ihre Steuern nicht bezahlen. Dieser Personenkreis muss künftig mit einschneidenderen Maßnahmen rechnen.“ Im Grundton dieser Pressemitteilung des SMF vom 1. Oktober 2004 wirkt die Frage nach dem Einklang mit der Rechtsordnung vielleicht unbillig. Der folgende Beitrag soll unvoreingenommen aufzeigen, dass die Zwangsstilllegung mit dem Instrumentarium des geltenden Vollstreckungsrechts ungeklärte Fragen aufwirft, während neuartige datenschutzrechtliche Auswirkungen evident werden. Er ist auch (vorläufige) Antwort auf die von Betroffenen und Interessierten an mich herangetragenen Fragen.

Fahrzeuge, die mit einem Pfandsiegel versehen im öffentlichen Verkehrsraum stehen (müssen), geben potentiell Kenntnis (über insbesondere wirtschaftliche Verhältnisse i. S. v. § 3 Abs. 1 SächsDSG) infolge der Zuordnungsmöglichkeit der hoheitlichen Maßnahme durch die das Fahrzeug wahrnehmende Öffentlichkeit auf den Kreis seiner Nutzer bzw. zum Halter. Mithin wird durch die Vollstreckungsmaßnahme eine gewisse Prangerwirkung ausgelöst, die (zumindest) nicht gesetzlicher Sinn und Zweck einer Sachpfändung sein kann. Darin liegt der datenschutzrechtliche Bezug.

Bevor sich die (subsidiäre) Frage nach der Vereinbarkeit mit dem Grundrecht auf informationelle Selbstbestimmung stellt, ist vorab zu klären, ob sich die Maßnahme überhaupt auf geltendes Pfändungsrecht stützen lässt. Denn Eingriffsverwaltung ist - unbeschadet ihrer datenschutzrechtlichen Auswirkungen - nur unter dem Vorbehalt des Gesetzes zulässig, also nur wenn die Norm, mit der sie begründet wird, nicht fehlerhaft angewendet würde.

Ein erschöpfender Überblick zum Sach- und Meinungsstand kann hier nicht geboten werden. Die Zwangsstilllegung von Kraftfahrzeugen ist faktisch auch Reaktion der öffentlichen Hand auf immer unzureichender ausfallende Beitreibungsergebnisse. Die Verwertung der Sache Kraftfahrzeug tritt dabei fast vollständig gegenüber dem Druckmittel plötzlich entzogener Mobilität zurück. Dies belegen etwa Angaben von Vollstreckungsverantwortlichen, wenn sie darauf hinweisen, es sei nicht Sinn der Maßnahme, das Fahrzeug tatsächlich zu verwerten. Die o. g. Pressemitteilung des SMF führt daher auch mit ebenso großer Offenheit aus, dass „insgesamt eine bessere Zahlungsmoral … erreicht werden [soll]“.

Nachdem die Fahrzeugsperren zunächst bei kommunalen Nutzern eingeführt wurden, sind dem Anwenderkreis inzwischen auch staatliche Stellen beigetreten; im Freistaat werden sämtliche Finanzämter zum flächendeckenden Einsatz der Fahrzeugsperre angehalten. Angefordert werden alle hierbei anfallenden Arten öffentlicher Abgaben. Das SMF weist expressis verbis (in o. g. Pressemitteilung) darauf hin, dass am Kraftfahrzeug nicht nur die säumige Kraftfahrzeugsteuer vollstreckt werden soll.

Hiervon abzugrenzen ist die gemäß § 14 Abs. 1 KraftStG auf Antrag des Finanzamts durch die Zulassungsstelle betriebene Abmeldung bzw. zwangsweise Stilllegung wegen rückständiger Kraftfahrzeugsteuern. So eine zulässigerweise durchgeführte Stilllegung kann aber in das hier beschriebene Verfahren übergehen.

Die Vollstreckungspraxis, soweit sie die meisten rechtlich relevanten Tatsachen anbelangt, hat sich mittlerweile weitgehend vereinheitlicht. Der Ablauf der Maßnahme verläuft im Wesentlichen nach folgendem Schema: „Wenn ein Fahrzeugbesitzer … auf

Mahnungen nicht reagiert, wird [Anm.: zusätzlich zum Pfandsiegel] die Parkkralle angebracht. Zahlt der Betroffene dann innerhalb von drei Werktagen seine Schulden, wird diese Sperre wieder entfernt. Überweist der Schuldner den ausstehenden Betrag nicht, wird das Fahrzeug abgeholt und anschließend zwangsversteigert.“ (Berliner Zeitung (online): „Test bestanden: Die Parkkralle wird nun in ganz Berlin eingesetzt“; 27. Februar 2004.)

Um eine gewisse Sicherheit zu erlangen, dass dem Vollstreckungsschuldner auch das Eigentum am Fahrzeug zusteht, wird regelmäßig vorab ein Halterabgleich mit Fahrzeugregisterdaten durchgeführt wird.

Zur rechtlichen Grundlage ist Folgendes zu bemerken:
„Das Beitreibungsrecht kennt als gesetzliches Eingriffsinstrument die Pfändung“ (Hagemann in: KKZ 1998, S. 57). Anders, prägnanter ausgedrückt: Ein sonstiges gesetzliches Instrumentarium neben § 286 AO 1977 bzw. § 808 ZPO gibt es hierfür nicht.[3]

Generell ist zu beachten, dass die Fahrzeugpfändung überhaupt nur dort in Betracht kommt, wo kein Pfändungsverbot greift (vgl. § 295 AO i. V. m. ZPO). Zu beachten ist insbesondere, dass die Rechtsprechung die Notwendigkeit des Kfz auch für den Arbeitsweg bejaht, soweit die Benutzung öffentlicher Verkehrsmittel nicht zumutbar ist, was bei der Praxis, zunächst die Parkkralle anzubringen, wohl häufig unbeachtet bleibt.

Zum Teil wird das Anbringen der Fahrzeugsperre als (rechtlich separierte) „Vorstufe zur Pkw-Pfändung“ - außerhalb der Pfändungshandlung(!) - betrachtet.[4] Dieser Ansicht ist mit nachvollziehbarer Argumentation widersprochen worden: „Eine isolierte Verwendung der Parkkralle - ohne Pfändung - ist gesetzlich nicht geregelt. Daher gibt es für eine solche Maßnahme keine rechtliche Legitimation.“ Denn auch über belastende „Vorstufen“ wache der Gesetzesvorbehalt (Hagemann a. a. O., 57: in einer Anmerkung, dass Gleiches auch für die Vorpfändung (§ 845 ZPO) gelte).

Eine Pfändung der „Sache“ Kraftfahrzeug kann auf genau zwei Arten bewirkt werden, entweder durch Wegnahme oder durch amtliche Kennzeichnung, i. d. R. durch Versehung mit einem Pfandsiegel. Die beiden - alternativ angelegten - Varianten ergeben sich unmittelbar aus dem Gesetzestext:

§ 286 Abs. 1 AO	entweder wird die „Sache“ aus dem „Gewahrsam“ des Schuldners in den „Besitz“ des Vollziehungsbeamten verbracht ...

[3] I. F. wird die ZPO unerwähnt gelassen; das Dargelegte gilt entsprechend.
[4] Ebd.

§ 286 Abs. 2 Satz 2 AO	... oder „andere Sachen als Geld“ bleiben „im Gewahrsam des Vollstreckungsschuldners“ und werden „durch Anlegung von Siegeln oder in sonstiger Weise ersichtlich gemacht“

Als ich bereits 1996 durch den SSG um eine Stellungnahme gebeten worden war, orientierte ich meine Stellungnahme am Gesetz. Der Gebrauch der Fahrzeugsperre zu Pfändungszwecken wurde darin als zulässige Form der Wegnahme (i. S. der Vorbereitung des alsbaldigen Abtransports) bewertet - mit der Konsequenz, dass damit eine zusätzliche Kenntlichmachung durch das Anlegen eines Pfandsiegels ausgeschlossen sei, weil das Gesetz den Einsatz beider Sachpfändungsalternativen nicht vorsehe.

Von vornherein den Einsatz der Fahrzeugsperre zugleich mit vorzusehen, erscheint insofern als Verstoß gegen den Grundsatz der Verhältnismäßigkeit.

Soweit zu übersehen ist, hat sich die Vollstreckungs-Praxis mittlerweile weitgehend festgelegt, die Fahrzeugsperre als Sicherungsmittel des im Schuldnergewahrsam verbliebenen Kfz aufzufassen. In den vorliegenden Fällen ist die Vollstreckungsstelle demzufolge (anordnend) einverstanden, dass das Fahrzeug (noch drei Werktage) im Schuldnergewahrsam verbleiben soll. Das Anlegen der Fahrzeugsperre soll danach als „andere geeignete Sicherungsmaßnahme“ i. S. v. Abschnitt 46 Abs. 6 Vollzugsanordnung gelten. Weil die dort beispielhaft erwähnte Demontage des amtlichen Kennzeichens im öffentlichen Verkehrsraum ausscheidet, wird die Fahrzeugsperre als eine für den öffentlichen Verkehrsraum geeignete Ersatzmaßnahme aufgefasst (in diesem Sinne: Tipke/Kruse - Kruse, § 286 AO Tz. 24).

Diesem Handeln zugrunde liegt die - nicht unumstrittene (in: Kölner Steuerdialog 1995, 10394) - Auffassung, dass bei der Pfändung von Kraftfahrzeugen die Befriedigung des Vollstreckungsschuldners in der Regel gefährdet sei (Abschnitt 46 Abs. 1 Satz 1 Vollzugsanordnung). Für die Schlechterstellung des Kfz-Inhabers bspw. gegenüber dem Eigentümer eines Fernsehgerätes drängt sich aber keine Erklärung auf, insbesondere vor dem Hintergrund, dass nur der zum Untergang der Sache führende Gebrauch unterbunden werden soll (vgl. Baumbach/Lauterbach/Albers/Hartmann - Hartmann ZPO, 63. Aufl., § 808 Rdnr. 21).

Eine weitere bisher nicht gänzlich eindeutig beantwortete Frage ist, ob das amtlich arretierte Fahrzeug sich überhaupt noch im Schuldnergewahrsam befindet. Das „Gewahrsam“ ist eine pfändungsrechtstypische Figur, die sich als „tatsächliche Sachhoheit“ definiert (vgl. Tipke/Kruse - Kruse AO (…), § 286, Tz. 2 ff.; Baumbach/Lauterbach/Albers/Hartmann - Hartmann ZPO, 63. Aufl., § 808 Rdnrn. 10, 15).

Den Gewahrsam beim Schuldner zu belassen, ist bekanntlich Voraussetzung für die Anbringung eines Pfandsiegels. Zu oberflächlich ist die Überlegung: „Da sogar eine Mitnahme des Fahrzeuges zulässig ist, kann dieses auch bei Ergreifung geeigneter Sicherungsmaßnahmen beim Schuldner belassen werden“ (Städteverband Schleswig-Holstein in: N Stb SH Nr. 12/1991-1/1992, Kapitel 6.11).

Wozu, wäre zu fragen, wenn es so simpel sein soll, hat dann der Gesetzgeber nicht gänzlich auf § 286 Abs. 2 Satz 2 AO verzichtet und für alle Pfändungen (die vom Beamten nach Ermessen auch als Wegnahme ausgestaltet werden dürfen) ein Pfandsiegel vorgeschrieben? Wenn Sachen nach § 286 Abs. 2 Satz 2 dem Schuldner zur Nutzung verbleiben sollen, entspricht eine Auslegung, dass sowohl Pfandsiegel als auch Sicherungsmaßnahme durchgeführt werden können, nicht dem Gesetzeswortlaut.

Die Fahrzeugpfändung wirft umstrittene, nicht abschließend geklärte Rechtsfragen auf. Durch die neuere Praxis, Fahrzeugsperre und Pfandsiegel gemeinsam anzubringen, also weder die Wegnahme zu vollziehen noch den Gebrauch zu ermöglichen, stellt sich durchaus die Frage, ob dieses Vorgehen mit der Rechtslage vereinbar ist. Bislang liegt hierzu kaum Einschlägiges und Gewichtiges vor, um von einer herrschenden Rechtsmeinung zu sprechen. Es ist den Vollstreckungsbehörden daher nur zu empfehlen, sich datenschutzrechtlich am Maßstab der Verhältnismäßigkeit zu orientieren und zum Beispiel die vorherige Sicherstellung der Fahrzeugpapiere durchzuführen. (Der Vollstreckungsbeamte sollte in diesem Fall den Kfz-Halter auf den Wegfall des Versicherungsschutzes vorsorglich hinweisen.) Derartige Maßnahmen sind datenschutzgerechter als die ansonsten häufig geübte Praxis. Selbstverständlich sind auch die Höhe der Schuld im Hinblick auf die Angemessenheit der Maßnahme und die zuvor zu klärende Frage, ob das Kraftfahrzeug des Betroffenen nicht unpfändbar ist, in die Überlegungen einzubeziehen. Da die Behörden beim Einsatz der Parkkralle wohl regelmäßig damit rechnen, dass die Sache nicht verarbeitet wird, sondern die Schuld beglichen wird, scheint das nicht immer der Fall zu sein.

7 Kultus

7.1 Kooperation von Kindergärten und Schulen

Im Oktober 2003 stellten das Kultus- und das Sozialministerium eine Vereinbarung zur engeren Kooperation von Kindertagesstätten und Schulen vor. Die Bemühungen stehen offenbar im Zusammenhang mit den politischen Diskussionen um eine gesteigerte Qualität an den Schulen bzw. einer besseren Vorbereitung der Kinder auf die Grundschule. Danach sollten unter anderem Lehrkräfte an Kindertagesstätten und Erzieher an Schulen hospitieren. Zuvor war im Ministerialblatt des Kultusministeriums eine damit im Zusammenhang stehende *Gemeinsame Vereinbarung des Sächsischen Staatsministeriums für Soziales und des Sächsischen Staatsministeriums für Kultus zur Kooperation von Kindergarten und Grundschule* (Ministerialblatt des SMK Nr. 9 vom 25. September 2003, S. 201 ff.) bekannt gemacht worden.

Die Vereinbarung verweist auf § 2 SächsKitaG und § 5 SchulG und enthält Hinweise auf einen gewissen Informationsaustausch zwischen den Einrichtungen. Auch die über die Presse hierzu veröffentlichten Meldungen ließen offen, ob auch einzelne Kinder und Eltern betreffende Angaben, insbesondere von den Kindertagesstätten oder anderen Einrichtungen an die Schulen übermittelt werden sollen. Ich habe die beiden Staatsministerien daher vorsorglich darauf hingewiesen, dass auf die schulgesetzlichen, sowie weitere landes- und bundesgesetzliche Bestimmungen und die veröffentlichte Vereinbarung kein personenbezogener Informationsaustausch gestützt werden kann. Insbesondere gilt dies für den Schulbereich. Das Schulwesen ist als Teilbereich der vollziehenden Gewalt an den Vorbehalt des Gesetzes gebunden, d. h. alle wesentlichen Regelungsgegenstände des Schulwesens bedürfen einer gesetzlichen Grundlage. Mithin dürfen auch alle Datenverarbeitungen von Schülern, Eltern und anderen Betroffenen, die in das Recht auf informationelle Selbstbestimmung eingreifen, nur auf gesetzlicher Grundlage erfolgen, § 4 Abs. 1 SächsDSG. Dabei müssen im Gesetz Inhalt, Zweck und Ausmaß der Verarbeitung personenbezogener Daten selbst geregelt sein. Derartige normenklare gesetzliche Bestimmungen, die eine Übermittlung personenbezogener Daten von den Kindertagesstätten an die Schulen (oder umgekehrt) vorsehen oder voraussetzen existieren in Sachsen nicht.

Ich habe das Staatsministerium gebeten, mir zu bestätigen, dass im Rahmen der Kooperation zwischen Kindertagesstätten und Schulen kein Austausch personenbezogener Daten erfolgt. Insbesondere sind keine gegenseitigen Hospitationen möglich, da hierbei zwangsläufig personenbezogene Daten verarbeitet werden. Das SMK hat mir daraufhin versichert: „Im Rahmen der Kooperation wird es zu keiner Verarbeitung personenbezogener Daten kommen. Hospitationen und die Teilnahme von Erziehern an Eltern-

abenden finden nur nach vorheriger Einwilligung der Eltern statt.“ Sofern hingegen Schulen vorschulische Angebote zur Erleichterung der Schuleingangsphase nach § 5 Abs. 5 SchulG anbieten, ist hiergegen nichts einzuwenden. Die damit einhergehenden Verarbeitungen personenbezogener Daten sind allerdings von denen anderer Einrichtungen strikt zu trennen. Im Übrigen werde ich darauf achten, dass eine zum Schutz der Betroffenen erforderliche informationelle Trennung zwischen Kindertagesstätten und Schulen entsprechend der ministeriellen Zusage erhalten bleibt.

7.2 Schulprojekt Regionales Schulnetzwerk für die Schulen im Südraum Leipzig

Bei einem größeren Projekt für ein Schulnetzwerk bin ich um datenschutzrechtliche Beratung gebeten worden. Das Projekt, das von kommunalen Schulträgern gemeinschaftlich betrieben und von einer Privatgesellschaft unterstützt wird, soll die Nutzung von Personal-Computern als Arbeitsmittel in Schulen fördern. Die Schüler sollen eine E-Mail-Adresse, einen Zugang im Schulnetz und zur Internetnutzung in der Schule erhalten. Grundsätzlich sind derartige Verbünde durchaus positiv zu bewerten und ich habe solche Vorhaben auch bisher konstruktiv unterstützt (vgl. auch 8/7.1.5).

Bei dem mir vorgestellten Projekt fehlte bisher vollständig ein Datenschutz- und Datensicherheitskonzept. Abstimmungen mit den Personalvertretungen und Elternräten waren zumeist noch nicht erfolgt. Es gab darüber hinaus keine Empfehlungen zu Dienstvereinbarungen und Nutzungsbedingungen bzw. -ordnungen für die einzelnen Schulen. Das mir bisher vorgestellte Vorhaben sah vor, dass das Onlineverhalten der Schüler zur Gewährung eines effektiven Kinder- und Jugendschutzes protokolliert werden soll. Aus Gründen des Jugendschutzes sollte zudem eine sog. „blacklist“ dafür Sorge tragen, dass die Schüler keine sie gefährdenden Internetseiten aufrufen können. Ich habe darauf hingewiesen, dass bereits aus Datensicherheitsgründen auch die Internetnutzung durch die Lehrer protokolliert werden muss. Systemdatenschutz kann nur durch eine lückenlose Protokollierung erfolgen. Die Aufbewahrung, Löschfristen, Zugriffsrechte und Auswertungsformalitäten der Protokolldaten waren noch nicht erkennbar festgelegt worden und sollten bei einem Schulnetz einheitlich geregelt werden.

Sofern Lehrkräfte im Rahmen des Projektes von zu Hause aus auf die Schuldaten zugreifen können und diese weiterverarbeiten sollen, sind verschiedene datenschutzrechtliche und datensicherheitstechnische Maßnahmen im Vorfeld zu treffen. Insbesondere sollten bei der eventuellen Einrichtung von Tele-Heimarbeitsplätzen die damit verbundenen umzusetzenden technischen und organisatorischen Maßnahmen daraufhin ausgerichtet werden, dass die Vertraulichkeit, Integrität und Authentizität der Daten sichergestellt ist. Ich fordere in diesem Zusammenhang, dass sich die an diesen Arbeits-

plätzen zum Einsatz kommende IT-Technik insgesamt im Eigentum der Dienststelle befindet und somit die gesamte Hardware und Software von der Dienstelle beschafft, installiert, konfiguriert und administriert wird. Auch sollten die datenschutzrechtlichen Belange dieser Arbeitsplätze durch die jeweils zuständigen Datenschutzbeauftragten überprüfbar sein.

Das Projekt werde ich weiter begleiten und in datenschutzrechtlichen Fragen beraten. Über den Fortgang des Projekts werde ich weiter berichten. Wegen der gemachten Erfahrungen empfehle ich dem zuständigen Staatsministerium, sich generell an Schulnetzvorhaben in Sachsen hilfestellend und beratend zu beteiligen.

7.3 Schulgesundheitspflege

1. Allgemeines

Bereits mehrfach habe ich in meinen Tätigkeitsberichten über Fragen im Zusammenhang mit der Datenverarbeitung im Bereich der Schulgesundheitspflege berichtet (1/7.1.2; 9/7.1.2). Nunmehr sind ein neues Schulgesetz und eine neue Schulgesundheitspflegeverordnung in Kraft getreten.

Die Schule hat einen Erziehungs- und Bildungsauftrag, keinen Auftrag aber zur Gesundheitsfürsorge. Untersuchungen haben dort stattzufinden, wo sie notwendig sind, und in einer Art und Weise, die den damit verbundenen Eingriff in die Privatsphäre minimiert. Hier handelt es sich jedoch um einen Fall staatlicher Überregulierung. Bezeichnenderweise gelten die Schulbestimmungen in Bezug auf Reihenuntersuchungen auch nur für die Schulpflichtigen, die auf staatliche Schulen gehen. Demgegenüber bleiben Eltern und Schüler, die eine nichtstaatliche Einrichtung nutzen, abgesehen von der Schulaufnahmeuntersuchung, staatlicherseits unbehelligt. Dieser Widerspruch in der gesundheitlichen Versorgung zeigt, wie fragwürdig die ausufernde Schulgesundheitspflege im Grunde genommen ist, wenn man wie selbstverständlich auf die Untersuchungen bei einem nicht geringen Teil der Schulpflichtigen verzichten kann. Die Schulgesundheitspflege sollte perspektivisch vom Kopf auf die Füße gestellt werden. Eltern könnten verpflichtet werden, die Untersuchungen ausschließlich bei niedergelassenen Ärzten nach einheitlichen Richtlinien durchführen zu lassen. Damit würden finanzielle Ressourcen geschont, Überkapazitäten bei den Gesundheitsbehörden abgebaut und nicht zuletzt überflüssige Verarbeitungen personenbezogener Daten bei staatlichen Stellen vermieden werden. Mit der eingeräumten Möglichkeit, die Reihenuntersuchungen nach § 5 Abs. 3 SchulGesPflVO durch einen Kinder- oder Hausarzt durchführen zu können, was aber für die Sorgeberechtigten kostenpflichtig sein soll, ist lediglich ein Anfang gemacht.

2. Die Beauftragung niedergelassener Kinder- und Zahnärzte durch die Gesundheitsbehörden

Nach § 26 a SchulG wird die Schulgesundheitspflege von den Behörden des öffentlichen Gesundheitsdienstes in Zusammenarbeit mit dem Schulleiter, den Lehrern, den Schülern und den Eltern wahrgenommen. Ich habe darauf hingewirkt, dass nach Absatz 6 die Eltern die Möglichkeit bekommen haben, Reihenuntersuchungen durch niedergelassene Haus- und Kinderärzte durchführen zu lassen. Darüber hinaus, auch dies habe ich dem Staatsministerium gegenüber deutlich gemacht, sehe ich keine gesetzliche Stütze für Funktionsübertragungen und die Verarbeitung personenbezogener (Gesundheits-)Daten durch Ärzte außerhalb des Gesundheitsdienstes, seien dies öffentlich- oder privatrechtlich organisierte Krankenhäuser oder niedergelassene Ärzte zum Zweck der Schulgesundheitspflege. In der Vergangenheit ist es aufgrund des Personalmangels der Gesundheitsdienste mehrfach zu „Beauftragungen“ niedergelassener Zahnärzte oder von Zahnkliniken, die nicht Teil des Gesundheitsdienstes sind, gekommen. Konnten oder wollten die Gesundheitsbehörden die Untersuchungen nicht selbst durchführen, versuchten sie dennoch Gesundheitsdaten über Dritte zu erheben. Derartige Funktionsübertragungen entgegen dem Schulgesetz waren bereits nach den alten Bestimmungen unzulässig. Die neuen Schulbestimmungen lassen diesbezüglich keinen Raum mehr für Fehlinterpretationen. Ich bin zuversichtlich, dass unzulässige Datenverarbeitungen durch von den Gesundheitsbehörden beauftragte Ärzte danach nicht mehr erfolgen. Sollten dennoch niedergelassene Mediziner, die Untersuchungen im Auftrag der Gesundheitsämter durchführen, werde ich dies zukünftig beanstanden.

3. Grenzen der Verarbeitung personenbezogener Daten durch die Gesundheitsbehörden

§ 4 Abs. 3 SchulGesPflVO legt fest, dass die Schule einen „Anamnesebogen“ des Gesundheitsamtes an die Eltern weiterzugeben hat, den diese ausfüllen sollen. Damit sollen Daten zur Krankheitsvorgeschichte des Schulkindes erhoben werden. Ich habe darum gebeten, dass der vorgesehene Erhebungsbogen der Gesundheitsbehörden vor Inkrafttreten der Schulgesundheitspflegeverordnung nach den Vorgaben des SMK zu vereinheitlichen und mit mir abzustimmen ist. Dies ist nicht erfolgt, sollte aber noch geschehen. Die auf dem Bogen enthaltenen Daten können nur solche sein, die für den Schulbesuch des Kindes von Bedeutung sind. Unzulässig ist auch eine Verarbeitung nicht erforderlicher Daten auf Einwilligungsgrundlage, da staatliche Stellen nicht berechtigt sind auf Grundlage § 4 Abs. 1 Nr. 2 SächsDSG ihren Aufgaben- und Wirkungsbereich auszudehnen. Nicht zu verarbeiten sind u. a. nachstehende Daten, wie sie in Anamnesebögen der Gesundheitsbehörden in Sachsen häufig verwendet werden:
- Geschwister des Kindes,
- Besuch einer Kindertagesstätte vor dem Schulbesuch,

- Telefonnummer der Personensorgeberechtigten,
- Daten zur Schwangerschaft der Mutter und zum Geburtsverlauf,
- die voraussetzungslose Verarbeitung von Gesundheitsdaten in Bezug auf zurückliegende Krankheiten, Unfällen, Operationen und Krankenhausaufenthalten,
- die voraussetzungslose Verarbeitung gesundheitlicher Besonderheiten (Allergien) und bei wem das Kind in ärztlicher Behandlung ist.

Derartige Daten weisen keinerlei Schulbezug auf. Lediglich erforderlich ist dagegen die Datenverarbeitung zu schulsportbefreienden Tatbeständen (z. B. Bluter-Krankheit) bzw. Krankheiten, die einen Schulbesuch aus medizinischer Sicht nicht erlauben (z. B. Sonnenlichtallergie) sowie Gesundheitsstörungen oder nicht vorhandene Fähigkeiten (z. B. Nichtschwimmer), die im Sinne von § 3 Abs. 1, Abs. 2 der Verordnung von *besonderer Bedeutung* für den Schulbesuch sind. Werden entsprechende Feststellungen gemacht, sind diese den Eltern mitzuteilen, die die Pflicht haben, für den Schulunterricht erforderliche Informationen an die Schule weiterzugeben.

Nach § 26 a Abs. 2 Nr. 8 SchulG sollen auch psychosoziale Auffälligkeiten, ansteckende und chronische Krankheiten verarbeitet werden. Ich habe die schulgesetzliche Bestimmung in dieser Fassung nicht anempfohlen. Sie ist zu unbestimmt gehalten und lässt den Gesundheitsbehörden zu viel Interpretationsspielraum. In der Praxis darf die Verarbeitung derartiger personenbezogener Daten daher nur in gravierenden Ausnahmefällen erfolgen, nämlich nur dann, wenn nach allgemeiner Lebenserfahrung ein konkreter Befund den Schulbesuch unmöglich machen, gefährden oder Mitschüler gefährden könnte. Dabei sind stets die konkreten Umstände des Einzelfalls zu betrachten. Zu berücksichtigen ist im Zusammenhang mit der vorzunehmenden Tiefe der Untersuchungen durch die Gesundheitsbehörden auch, dass es sich um eine staatliche Zwangsuntersuchung handelt, und dass die Gesundheitsbehörde an die Schulleitungen lediglich allgemeine Hinweise weiterzugeben berechtigt ist.

Die Untersuchungsergebnisse der Gesundheitsbehörden unterliegen, was die einzelnen untersuchten Schüler angeht, der ärztlichen Schweigepflicht. Dem Rechnung tragend dürfen betreffende Dokumentationen und Gesundheitsdaten einzelner Schüler nur den Eltern mitgeteilt werden, § 26 a Abs. 3 SchulG. Diese wiederum haben nach § 26 a Abs. 7 Satz 2 SchulG die Pflicht gesundheitliche Beeinträchtigungen des Schülers, die sich im Schulbetrieb auswirken können, der Schule mitzuteilen.

Auch Daten von Gesundheitsbehörden an andere Gesundheitsbehörden - z. B. beim Schulwechsel - dürfen nicht ohne weiteres weitergegeben werden, sondern auch nur mit Einwilligung der Eltern, handelt sich um eine Datenübermittlung an eine andere öffent-

liche Stelle und um von der jeweiligen Gesundheitsbehörde verarbeitete Daten, die dem Arzt-Patienten-Geheimnis unterliegen, § 6 Satz 3 SchulGesPflVO.

7.4 Evaluation des Schulunterrichts

Das neue Schulgesetz sieht in § 59 a vor, dass die Ergebnisse der Erziehungs- und Bildungsarbeit regelmäßig überprüft werden sollen. Schülerleistungen und Unterrichtsqualität sollen hierfür herangezogen werden. Eine „Evaluationsagentur“ soll die Untersuchungen durchführen.

Nur wenn daraus die Verarbeitung personenbezogener Daten wird, bin ich zuständig. Die sich ergebenden Datenverarbeitungsvorgänge sind aus der allgemein gehaltenen Vorschrift nicht absehbar. Die Gesetzesfassung entspricht nicht meinen Empfehlungen. Sie ist nicht normenklar. Auf die Bestimmung kann eigentlich eine Verarbeitung personenbezogener Daten nicht gestützt werden. Gleichwohl befürchte ich eine über die Erforderlichkeit hinausgehende Verarbeitung personenbezogener Daten. Die Arbeit der Agentur werde ich daher aufmerksam begleiten und hierüber weiter berichten.

7.5 Fotoaufnahmen von Schülern durch private Fotoateliers in Schulen

In den meisten Schulen werden privaten Fotoateliers eine allgemeine Erlaubnis zum Fotografieren von Schülern - oftmals von Schulanfängern - erteilt. Ein Vater, der gegenüber der Schule darauf hingewiesen hatte, dass nur mit seiner ausdrücklichen Erlaubnis fotografiert werden dürfe und dessen Kind dennoch aufgenommen wurde, wandte sich mit der Bitte um datenschutzrechtliche Prüfung an mich. Ich habe mich gegenüber der Schule wie folgt geäußert:

Das Fotografieren von Schülern ohne deren Einwilligung bzw. der ihrer Sorgeberechtigten verstößt gegen das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) der betroffenen Schüler. Auch wenn die Anfertigung der Bildaufnahmen als Verarbeitung der personenbezogenen Schülerdaten durch einen privaten Unternehmer, der selbst nicht dem Sächsischen Datenschutzgesetz unterliegt, erfolgt, hat doch die Schule hausrechtlich die Möglichkeit und organisatorisch die Pflicht dafür Sorge zu tragen, dass die Persönlichkeitsrechte der Kinder gewahrt bleiben und eine datenschutzgerechte personenbezogene Datenverarbeitung erfolgt, da sie als öffentliche Stelle dem privaten Unternehmer letztendlich auch die Möglichkeit eröffnet, fotografische Aufnahmen zu machen. Die Schule hat die Eltern der Kinder daher frühzeitig auf die Fotografien aufmerksam zu machen und sicherzustellen, dass eine Einwilligung in die fotografischen Aufnahmen möglich ist. Bei Grundschülern kann eine

rechtswirksame Einwilligungserklärung zum Fotografieren der Kinder nur durch die Eltern abgegeben werden, weil es diesen Schülern an der notwendigen Einsichts- und Entscheidungsfähigkeit in Bezug auf die Datenverarbeitungsvorgänge noch fehlt, und sie die Konsequenzen ihres Handelns noch nicht vollständig zu überschauen in der Lage sind. Es besteht eine allgemeine Pflicht der Schule dafür Sorge zu tragen, dass die Selbstbestimmungsrechte der Kinder, die nur die Sorgeberechtigten wahrnehmen können in der Schule gewahrt bleiben. Die Schulleitung ist nicht berechtigt, ihre Entscheidung über das Fotografieren an die Stelle der Elternentscheidung zu setzen.

Privatunternehmen, wie es z. B. auch ein Fotoatelier darstellt, haben ein einfaches geschäftliches Interesse am Fotografieren in Schulen. Von den Schulen werden ihnen dafür auch häufig die Namen der Schüler und oftmals auch die Anschriften der Eltern zur Verfügung gestellt. Die Verfahrensweise und die Bedingungen unter denen eine solche Datenübermittlung von öffentlichen Stellen an nicht-öffentliche Stellen erfolgen darf, regelt § 16 Abs. 1 SächsDSG. Derartige Datenübermittlungen sollten jedoch nach Möglichkeit vermieden werden. Sofern die Klassenlehrer hingegen die Schreiben und Informationen von Fotoateliers weiterleiten, habe ich keine Einwände.

7.6 Fotokopien aus einem Klassenbuch

Organisatoren von Klassentreffen wenden sich regelmäßig mit der Bitte um Rat und der Bitte um Unterstützung an mich, da ihren Vorstellungen von Seiten der Schulen nicht entsprochen wird. Bereits in früheren Tätigkeitsberichten habe ich mich zu diesen datenschutzrechtlichen Fragen geäußert, in 7/7.4 und 9/7.1.6. Da in Bezug auf den datenschutzgerechten Umgang mit Klassenbüchern aus früheren Schultagen erneut Fragen aufgetreten sind, greife ich das Thema wiederholend auf.

Mit der Anfrage, ob er zur Ausgestaltung einer Festzeitung anlässlich des 40. Jahrestages des Abiturs Fotokopien aus dem Klassenbuch seiner Abiturklasse anfertigen dürfe, um an bedeutsame Ereignisse zu erinnern, wandte sich ein Petent an mich. Zuvor hatte er sich erfolglos an die Schule gewandt. Aus datenschutzrechtlichen Erwägungen habe ich ebenfalls dem Überlassen des Klassenbuchs zum Anfertigen von Fotokopien nicht zugestimmt. Bei der Einsichtnahme in das Klassenbuch würde der Antragsteller nicht nur Kenntnis von den eigenen Daten, sondern auch Kenntnis über die personenbezogenen und persönlichkeitsrelevanten Daten aller seiner ehemaligen Mitschüler erlangen. Eine Übermittlung dieser Daten durch die Schule an private Dritte ist jedoch nur unter den Voraussetzungen von § 16 SächsDSG zulässig. Da die von der Schule verarbeiteten personenbezogenen Daten zu einem anderen Zweck genutzt werden sollen, ist eine Übermittlung auch nur unter den engeren Voraussetzungen des § 13 Abs. 1 bis 4 SächsDSG zulässig. Ich stehe weiterhin auf dem Standpunkt, dass es zwar zu den

Aufgaben der Schule gehört, die Organisation von Klassentreffen zu unterstützen, z. B. die Anschriften früherer Klassenkameraden nach Aktenlage in der Schule zu diesem Zweck herauszugeben (vgl. auch 9/7.1.6). Die Schule müsste hier aber aus rechtlichen Gründen - das Fotokopieren und Auswerten eines Klassenbuches für eine Jubiläumsschrift als berechtigtes Interesse unterstellt - zunächst sämtliche in den Klassenbüchern genannten Personen anschreiben (und zuvor die aktuellen Anschriften ermitteln), um ein mögliches schutzwürdiges, der Herausgabe des Klassenbuches (und der damit verbundenen Datenübermittlung) entgegenstehendes Interesse zu erkunden bzw. eine schriftliche Einwilligung zu erhalten. Das ist regelmäßig ein unzumutbarer Verwaltungsmehraufwand. Dazu ist die Schule nicht verpflichtet. Der Schulleiter der betreffenden Schule hatte sich letztendlich nach Klärung der Rechtslage bereit erklärt, dem Antragsteller wenige Seiten des Klassenbuchs, die keine personenbezogenen Daten enthalten (z. B. Titelblatt) für seine Festschrift in Kopie zu überlassen.

7.7 Internetpräsenz von Schulen

Immer häufiger erhalte ich Anfragen zur Internetpräsenz von Schulen, die hiermit Öffentlichkeitsarbeit betreiben und im Internet ihr Bildungsangebot und besonderes Profil darstellen wollen. Hierbei spielen Klassenfotos und bebilderte Erlebnisberichte aus dem Freizeitangebot der Schule eine immer größere Rolle.

Datenschutzrechtlich ist Folgendes zu beachten: Staatliche Schulen sind öffentliche Stellen gemäß § 2 Abs. 1 SächsDSG. Bereichsspezifische gesetzliche Regelungen zum Umgang mit dem Internet im Schulbereich fehlen in Sachsen. Die Angebote von Schulen sind in der Regel Mediendienste. Dann verdrängen die Vorschriften des Mediendienste-Staatsvertrag die weitgehend inhaltsgleichen Vorschriften des Teledienstegesetzes. In Bezug auf die Inhaltsdaten gilt das allgemeine Sächsische Datenschutzgesetz. Als öffentliche Stelle ist die Schule lediglich befugt, personenbezogene Daten zu verarbeiten, wenn die Verarbeitung zur gesetzlichen Aufgabenerfüllung erforderlich ist, §§ 12 ff. SächsDSG. Werden auf der Internetpräsenz einer Schule Abbildungen von Schülern, Namen von Schülern oder andere Angaben im Internet veröffentlicht, so werden damit personenbezogene Daten im Sinne von § 3 Abs. 1 SächsDSG verarbeitet. Die Verarbeitung schülerbezogener individueller Angaben im Internet wird zur Aufgabenerfüllung der Schule aber regelmäßig im Gegensatz zu auf die Schule bezogenen Informationen nicht erforderlich sein.

Ich habe aber keine Einwände, wenn die Schulen einem gewissen Informationsinteresse der Öffentlichkeit dahingehend nachkommen, wenn sie personenbezogene Daten von Schülern, z. B. Bildnisse und Namensangaben, auf Einwilligungsgrundlage im Internet verarbeiten, wie es die Bestimmungen des Mediendienst-Staatsvertrages, des Tele-

dienstegesetzes und auch des Sächsischen Datenschutzgesetzes selbst (vgl. § 4 Abs. 1 Nr. 2 SächsDSG) es ja zulassen. Auf die Formerfordernisse des § 4 Abs. 3 bis 5 SächsDSG sollte gleichwohl nicht verzichtet werden. Einzuwilligen haben bei Minderjährigen die Elternsorgeberechtigten. Bei älteren Schülern, die eine notwendige Einsichtsfähigkeit besitzen und Datenverarbeitungsvorgänge zu überblicken in der Lage sind, und dies ist etwa in einem Alter von dreizehn bis vierzehn Jahren der Fall, ist die Einwilligung der Schüler selbst erforderlich. Zusätzlich sollte man, geht man davon aus, dass sich ein Minderjähriger noch nicht selbst wie ein Volljähriger wird behaupten können, das Einwilligungserfordernis der Elternsorgeberechtigten belassen. Volljährige Schüler sind in der Lage selbständig zu entscheiden und einzuwilligen. Eine Einwilligung der Eltern entfällt in diesen Fällen.

Bei der Einwilligung ist zu beachten, dass diese nur unter der Voraussetzung der Freiwilligkeit wirksam ist, d. h., dass die Einwilligenden auf die Folgenlosigkeit der Versagung Ihrer Einwilligung hinzuweisen sind. Auch tatsächlicher Druck auf die Einwilligenden ist auszuschließen. Die Schule hat in diesem Zusammenhang sicherzustellen, dass der Schüler, dessen Einwilligungserklärung nicht vorliegt, keinem psychischen Druck ausgesetzt wird, bzw. sich schützend vor den Schüler zu stellen (Veröffentlichung eines Klassenfotos auf Wunsch der Mitschüler). Einwilligungen zur Veröffentlichung der personenbezogenen Daten sollten auch erst dann eingeholt werden, wenn die entsprechenden Bildnisse oder personenbezogenen Daten hergestellt worden sind und der Einwilligende eine Vorstellung hat, in was er konkret einwilligt.

Die personenbezogenen Daten können im Internet ohne jede Zweckbindung weltweit abgerufen, verändert oder für andere Zwecke genutzt werden, ohne das der Einzelne darauf Einfluss nehmen kann. Insofern sollte die Schule als öffentliche Stelle, unabhängig von der Einwilligungsmöglichkeit, nach strengen Maßstäben prüfen, ob und in welchem Umfang personenbezogene Daten der Schüler im Internet veröffentlicht werden sollen. Der Verzicht auf viele individuelle Informationen sollte seitens der Schulen nach dem Motto „Weniger ist mehr“ praktiziert werden. In diesem Zusammenhang sollte nicht unbeachtet bleiben, dass neben den schulischen Internetpräsentationen es zumeist auch eine große Anzahl von privaten Schüler- und Elterninitiativen gibt, die außerhalb der offiziellen Internetpräsenzen auf das schulische Leben aufmerksam machen und informieren und auf die wiederum die Schule hinweisen kann.

Da die Veröffentlichung personenbezogener Daten einzelner Schüler für die Aufgabenerfüllung der Schule insgesamt nicht erforderlich ist, müssen die Einwilligungen immer jederzeit widerruflich sein. Die Veröffentlichung im Internet ist nämlich anders zu beurteilen als eine Veröffentlichung in einer Schülerzeitung, in der personenbezogene Daten veröffentlicht werden. Die Veröffentlichung solcher Druckerzeugnisse kann nicht

mehr rückgängig gemacht werden bzw. wäre dies mit größeren Kosten verbunden. Hingegen kann die Veröffentlichung personenbezogener Daten Einzelner im Internet für die Zukunft jederzeit unterbunden werden. Dies ist zwar mit einem gewissen technischen und zeitlichen Aufwand verbunden, ist aber seitens der öffentlichen Stelle, entschließt sie sich für die Veröffentlichung personenbezogener Daten einzelner Schüler, hinzunehmen. Hier geht das Grundrecht auf informationelle Selbstbestimmung den geringfügigen Kosten und dem notwendigen zeitlichen Aufwand vor. Auch bei Veränderungen der Homepage der Schule ist die erneute Einwilligung der Betroffenen vor Veröffentlichung einzuholen, wenn wiederum personenbeziehbare oder personenbezogene Daten verarbeitet werden. Insbesondere sind Globaleinwilligungen oder pauschale Einwilligungen regelmäßig nicht ausreichend, da die einzelnen Datenverarbeitungen damit für die Betroffenen nicht absehbar und überschaubar bleiben. Die Einwilligung ist vielmehr bei der Veröffentlichung eines jeden personenbezogenen Datums einzuholen. Für die Veröffentlichung im Intranet gelten die oben stehenden Grundsätze entsprechend, auch wenn der Nutzerkreis, der auf die Daten zuzugreifen berechtigt ist, kleiner ist. In diesem Zusammenhang ist auch noch einmal darauf hinzuweisen, dass Daten im Internet oder Intranet regelmäßig leicht vervielfältigt und verändert werden können. Zu empfehlen ist, um bereits im Vorfeld missbräuchliche Nutzungen zu minimieren, insbesondere in Bezug auf Bildnisse einen Kopierschutz einzurichten. Möglich ist es auch geschlossene Benutzerkreise im Internet einzurichten, so dass die Übermittlung bestimmter personenbezogener Daten auf den Kreis der Schüler deren Angehörige und Lehrer beschränkt werden kann.

Auch Lehrer können, wie die Schüler selbst, nicht verpflichtet werden, sich z. B. an der Veröffentlichung ihrer Bildnisse im Internet zu beteiligen. Sofern zur weiteren Information, was die Schule anbelangt, personenbezogene Daten der Lehrkräfte veröffentlicht werden sollen (z. B. Kontaktdaten wie vollständige Namen, Anschriften und Rufnummern), ist dies wiederum zur Aufgabenerfüllung - sieht man vielleicht von Daten in Bezug auf die Schulleitung ab - nicht erforderlich. Die Sorgeberechtigten haben in Bezug auf die Ansprechpartner und die ihre Kinder Unterrichtenden Kenntnis bzw. können sich an die Schulleitungen wenden, so dass solche Lehrerdaten nicht im World Wide Web Verbreitung finden müssen.

7.8 Veröffentlichung von personenbezogenen Eltern- und Schülerdaten während eines Schulelternabends

Im Zusammenhang mit Schulelternabenden erreichen mich immer wieder Beschwerden. In Einzelfällen werden grundlegende Grundsätze der Amtsverschwiegenheit und des

Datenschutzes missachtet. Nach einem Vorfall dieser Art wandten sich betroffene Eltern an mich.

Im Verlauf eines Gesprächsabends in einer Schule, zu Fragen einer Sicherheitspartnerschaft gegen Gewaltbereitschaft von Schülern, hatte eine Lehrerin auf Nachfrage von Eltern personenbezogene Daten eines Schülers sowie Inhalte aus einer gegen eine Lehrerin gerichtete Dienstaufsichtsbeschwerde der Eltern des Schülers den Anwesenden bekannt gegeben. Daraufhin wandte sich die betroffene Mutter mit der Bitte um Klärung der datenschutzrechtlichen Fragestellungen an mich.

Nach dem Eingang der Stellungnahme der Schule, mit der die Offenbarung der personenbezogenen Angaben gegenüber den Anwesenden des Schulelternabends nicht gerechtfertigt werden konnte, musste ich davon ausgehen, dass die Bekanntgabe der personenbezogenen Daten des Schülers und seiner Eltern, die eine Übermittlung an private Dritte im Sinne des § 16 SächsDSG darstellt, das Grundrecht auf informationelle Selbstbestimmung der Betroffenen verletzte. Ich habe daraufhin die Schulleitung darauf hingewiesen, dass sie nur befugt ist, personenbezogene Daten im Rahmen des Erforderlichen und zur gesetzlichen Aufgabenerfüllung zu verarbeiten. Die Bekanntgabe der Daten war im Rahmen der Gesprächsrunde nicht erforderlich. Es ist auch grundsätzlich nicht datenschutzgerecht, Probleme der Lehrer und der Schule mit einzelnen Eltern und Schülern und die sich daraus ergebenden Maßnahmen in der Öffentlichkeit zu beraten. Und es ist schlichtweg auch nicht zweckmäßig. Für die Betroffenen ist eine öffentliche Erörterung regelmäßig bloßstellend bzw. verletzend. Der Elternabend, der nach meinem Kenntnisstand in seinem Verlauf eskaliert ist, wäre wohl anders verlaufen, wenn sich die Schulleitung und das Lehrpersonal datenschutzgerecht verhalten und die in Rede stehenden personenbezogenen Daten nicht bekannt gemacht hätten.

Ich habe die Schulleitung aufgefordert, derartige Datenschutzverstöße zukünftig durch vorbeugende organisatorische und personelle Maßnahmen auszuschließen, wozu insbesondere gehört, dass die Lehrerschaft der Schule über die in meinem Schreiben enthaltenen konkreten datenschutzrechtlichen Grundsätze, Bewertungen und Forderungen in Kenntnis gesetzt wird.

8 Justiz

8.1 DNA-Analyse im Strafverfahren

Die Diskussion um eine Erweiterung der DNA-Analyse im Strafverfahren beschäftigt seit Monaten Politik, Medien und Öffentlichkeit und veranlasst mich, erneut zu der Problematik Stellung zu nehmen. Die in der - in 11/16.1.13 abgedruckten - Entschließung zwischen der 65. und 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder („Bei der Erweiterung der DNA-Analyse Augenmaß bewahren“) geäußerten Bedenken behalten nach wie vor ihre Gültigkeit.

Die derzeitigen gesetzlichen Möglichkeiten des Einsatzes der DNA-Analyse und der Speicherung des DNA-Identifizierungsmusters zum Zweck der Verfolgung künftiger Straftaten haben bereits zu spektakulären Erfolgen der Ermittler geführt. Die Aufklärungsquoten im Bereich der Sexualverbrechen und Tötungsdelikte sind schon seit Jahren außerordentlich hoch. Angesichts dessen stellt sich die Frage, ob eine Ausweitung der molekulargenetischen Untersuchung und Speicherung von DNA-Identifizierungsmustern zum Zwecke künftiger Strafverfolgung überhaupt erforderlich ist. Sowohl die Untersuchung der DNA als auch die Speicherung des gewonnenen Musters sind Eingriffe in das Grundrecht des Betroffenen auf informationelle Selbstbestimmung, was manchmal in der Diskussion offensichtlich vergessen wird.

Neben der unbestritten begrüßenswerten Möglichkeit, Straftaten mit Hilfe der DNA-Analyse aufzuklären, bergen die Methode und eine zu umfangreiche Speicherung von DNA-Identifizierungsmustern auch Risiken.

Mag der das DNA-Identifizierungsmuster bildende Code heute noch keine Aussagen über genetische Dispositionen des Betroffenen zulassen, so ist angesichts des rasanten technischen Fortschritts ungewiss, besser: unwahrscheinlich, dass dies auch noch in einigen Jahren Stand der Wissenschaft sein wird. Die nicht-codierenden Teile der DNA, die für die Gewinnung des Identifizierungsmusters untersucht werden, liefern bereits heute mehr Informationen über Wahrscheinlichkeiten einzelner Krankheiten, als man vor wenigen Jahren für möglich hielt.

Im Zuge einer Ausweitung des Einsatzes der DNA-Analyse ist eine starke Erhöhung des Datenbestandes in der DNA-Analysedatei des Bundeskriminalamtes zu erwarten. Im Zusammenspiel von einem hohen Fahndungsdatenbestand und der Haltbarkeit von DNA-Material ist besteht die Gefahr, dass Spuren, die lange vor der Straftat am Tatort hinterlassen wurden, leichter und häufiger zu einem Verdacht führen, der für den Betroffenen zu einer Art Beweislastumkehr im Strafprozess führen wird, da dem Auffinden von DNA-Material am Tatort eine starke Indiz-Wirkung zukommt.

Ich sperre mich nicht gegen eine sinnvolle und angemessene Novellierung der Vorschriften zum Einsatz der DNA-Analyse im Strafverfahren.

So halte ich eine richterliche Anordnung für die molekulargenetische Untersuchung von DNA-Tatortspuren unbekannter Herkunft, die nach derzeitiger Rechtslage noch notwendig ist, für entbehrlich. Die richterliche Entscheidung ist in diesen Fällen eine verzichtbare Formalie. Von zentraler Bedeutung ist hier der Aspekt der Beschränkung der Verwendung der gewonnenen Daten auf das konkrete Verfahren bzw. bis zur Möglichkeit der Zuordnung der Spur zu einer natürlichen Person. Die weitere Verwendung (etwa eine Speicherung zum Zweck der Identifizierung in künftigen Strafverfahren) der Informationen muss dann wieder den jeweiligen Regelungen folgen und steht mithin gegebenenfalls unter Richtervorbehalt.

Eine Straftat von erheblicher Bedeutung sehe ich nicht für die Zulässigkeit der Speicherung in der zentralen DNA-Analysedatei verfassungsrechtlich zwingend als erforderliche Voraussetzung an. Entscheidend ist die Qualität der Anlasstat in Richtung einer Negativprognose, nicht ausschließlich deren Schwere. In diesem Punkt gewinnt jedoch die Rolle des Richtervorbehalts an Bedeutung. Je breiter das Spektrum möglicher Anlasstaten, desto genauer muss die Prüfung im Einzelfall erfolgen. Allein durch eine richterliche Anordnung ist eine der Bedeutung des Grundrechts auf informationelle Selbstbestimmung angemessene Prüfung der Voraussetzungen einer Speicherung gewährleistet. Zu Letzteren muss auch künftig zwingend eine Negativprognose gehören, die die zukünftige Begehung einer Straftat von erheblicher Bedeutung erwarten lässt. Die Aufgabe einer diesbezüglichen Beurteilung der Anlasstat und des Betroffenen darf keinesfalls vom Richter auf den Polizeivollzugsdienst übertragen werden.

Im Gegensatz zur pauschalen Einstufung der DNA-Analyse als erkennungsdienstliche Maßnahme sehe ich im Falle der Beibehaltung des Richtervorbehaltes für die Speicherung des DNA-Identifizierungsmusters zur künftigen Strafverfolgung nicht die Gefahr einer uferlosen Ausweitung, auch wenn die Anforderungen an die Anlasstat abgesenkt werden. Der Bedeutung des Grundrechts auf informationelle Selbstbestimmung wird mit der Einzelfallbefassung eines Richters Rechnung getragen. Im Übrigen ist es für alle Beteiligten hilfreich, wenn es bei einer so tiefgreifenden Entscheidung eine Gegenprüfung gibt.

8.2 Rasterfahndung

Nach den Terroranschlägen vom 11. September 2001 in den USA wurden bundesweit präventiv-polizeiliche Rasterfahndungen zur Enttarnung potenzieller Attentäter (sog.

Schläfer) durchgeführt. In die Bemühungen der Rasterfahndung war ich von vornherein umfassend eingebunden. Störungen im Verlauf der Fahndung konnte ich nicht feststellen; alle angefragten Stellen haben nach entsprechender Aufklärung durch das LKA ihre Pflichten erfüllt und die notwendigen Daten geliefert.

Von den ursprünglich 790.000 Datensätzen wurden nach Durchführung der Rasterung ca. 1.400 sächsische Datensätze dem BKA geliefert, die in die Verbunddatei „Schläfer“ eingestellt wurden.

Nach weiteren Rasterungen verblieb eine zweistellige Anzahl von Prüffällen, die weiteren Überprüfungen unterzogen wurden. Alle übrigen Daten waren zu diesem Zeitpunkt wieder gelöscht. In einigen dieser Prüffälle kam es zu Ermittlungs- und Strafverfahren. Die Unterlagen zu den Beschuldigten in den jeweiligen Strafverfahren wurden gemäß den „Richtlinien für die Führung kriminalpolizeilicher Sammlungen in den Polizeidienststellen des Freistaates Sachsen“ gespeichert.

Bei den übrigen Prüffällen konnte kein Straftatverdacht begründet werden. Daher wurden die Daten nach Abschluss der Ermittlungen gelöscht.

8.3 Datenerhebungen nach § 100 g StPO

Im Berichtszeitraum versuchte das LKA in zwei uns bekannt gewordenen Fällen, unzulässig auf Telefonverbindungsdaten zuzugreifen. Das LKA führte in einem Fall strafrechtliche Ermittlungen gegen den ehemaligen Bürgermeister einer Gemeinde. Das LKA forderte die Gemeinde schriftlich auf, die Telefonverbindungsdaten, die von ihrer Telefonanlage in einem bestimmten Zeitraum getätigt und dort noch gespeichert worden waren, auf „freiwilliger Basis“ dem LKA zu übermitteln. Der Justitiar der Gemeinde hatte hiergegen Bedenken und wandte sich an mich mit der Bitte um eine datenschutzrechtliche Bewertung.

Im vorliegenden Fall befand sich das LKA mit seinen Ermittlungen im strafprozessualen Bereich. Infolgedessen hatte es die Voraussetzungen des § 100 g StPO zu beachten. Dieser normiert, dass bei Straftaten von erheblicher Bedeutung diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, Auskunft über die Telekommunikationsverbindungsdaten zu erteilen haben. Die Gemeinde war hier Telekommunikationsanbieter, da über ihre Telefonanlage nicht nur dienstliche Gespräche geführt wurden, sondern den Mitarbeitern auch deren private Nutzung gestattet war. Allerdings genügte das Ersuchen des LKA an die Gemeinde den Anforderungen des § 100 h Abs. 1 Satz 3 i. V. m. 100 b Abs. 1 Satz 1, 2 und 3 StPO nicht. Diese Vorschriften legen fest, dass eine Anordnung zur Übermittlung der Daten nur durch den

Richter geschehen darf. Das Vorgehen des LKA beachtete nicht die gesetzlichen Voraussetzungen. Insbesondere blieb für eine „freiwillige“ Herausgabe der Daten seitens der Gemeinde kein Raum, denn der Gesetzgeber hat mit § 100 g StPO zwingende Voraussetzungen für eine Auskunft über Telekommunikationsverbindungsdaten geschaffen.

Die Gemeinde war daher nicht verpflichtet, die Verbindungsdaten mitzuteilen. Ein Rückgriff auf § 94 StPO - wie ihn das LKA plante - war ebenfalls nicht möglich, da § 100 g StPO insoweit lex specialis ist.

Ähnlich gelagert ist der Fall, der mir aus der Presse bekannt wurde: Nachdem im Oktober 2002 der Anschlag auf das Moskauer Theater verübt worden war, erlangte das LKA Kenntnis davon, das russische Bürger vor den Anschlägen in einem Dresdner Hotel residiert hatten und von dort zu konspirativen Wohnungen in Moskau telefonischen Kontakt hatten. Um den Sachverhalt strafrechtlich aufzuklären, trat das LKA an den Direktor des Hotels heran und verlangte eine Aufstellung aller Telefonverbindungen, die im fraglichen Zeitraum vom Hotel aus getätigt worden waren. Eine richterliche Anordnung konnte das LKA auch hier nicht vorlegen. Leider erfuhr ich von diesem Vorgang erst, nachdem der Hoteldirektor die fraglichen Verbindungsnachweise herausgegeben hatte.

Seitens des SMI wurde zugesichert, dass eine Erhebung von Telekommunikationsverbindungsdaten zukünftig nur nach den gesetzlichen Voraussetzungen erfolgen werde. Insoweit wurde zunächst von einer Beanstandung abgesehen. Ich werde diesen Sachverhalt aber im Auge behalten.

8.4 Bescheidung des Anzeigeerstatters nach Nichterhebung der öffentlichen Anklage

Ein Petent wandte sich an mich und zeigte sich darüber verwundert, dass die Staatsanwaltschaft ihm mitteilte, sie hätte ein bestimmtes Ermittlungsverfahren zuständigkeitshalber an die Staatsanwaltschaft eines anderen Bundeslandes abgegeben. Der Petent, dem die genannten Aktenzeichen unbekannt waren, wandte sich daraufhin an die Staatsanwaltschaft und erhielt die telefonische Auskunft, dass das Aktenzeichen zu dem Verfahren gegen eine Person gehöre, die ihm namentlich genannt wurde.

Im Verlauf meiner Prüfung stellte sich heraus, dass der Petent in der Vergangenheit aufgrund eigener Beobachtungen im Internet eine Anzeige gegen Unbekannt wegen Verwendung von Kennzeichen verfassungswidriger Organisationen erstattet, die Staatsan-

waltschaft nun das seinerzeit eingeleitete Ermittlungsverfahren zuständigkeitshalber abgegeben und den Anzeigeerstatter darüber informiert hatte.

Die Staatsanwaltschaft stützte die Mitteilung des Aktenzeichens und Namens des Beschuldigten an den Anzeigeerstatter auf § 171 Satz 1 StPO. Jede Strafanzeige nach § 158 Abs. 1 StPO mit dem erkennbaren Willen, die Strafverfolgung zu veranlassen, sei als Antrag auf Erhebung der öffentlichen Klage im Sinne von § 171 Satz 1 StPO anzusehen und der Anzeigeerstatter entsprechend zu bescheiden.

Ich teilte der Staatsanwaltschaft meine Zweifel an der Rechtmäßigkeit der Mitteilung des Namens und des Aktenzeichens des Beschuldigten mit, wenn ursprünglich Anzeige gegen Unbekannt erstattet wurde und der Anzeigende weder Verletzter noch sonst strafantragsbefugt war.

Erstattet der Verletzte Anzeige gegen eine bestimmte Person, so bezieht sich sein Antrag auf Erhebung der öffentlichen Klage auf diese ihm namentlich bekannte Person, die ihn aus seiner Sicht in seinen Rechten verletzt hat. Das Interesse des Verletzten an den Gründen für die Nichterhebung der Klage oder der Einstellung des Verfahrens durch die Staatsanwaltschaft ist in diesem Fall offensichtlich. Gleiches gilt für die Anzeige eines Verletzten gegen Unbekannt. Die Verletzungen des Geschädigten begründen dessen Anspruch auf Bescheidung, auch wenn er den Namen des oder der Täter nicht nennen konnte.

Ist der Anzeigende nicht verletzt, richtet sich seine Anzeige aber gegen eine von ihm benannte Person, enthält die Mitteilung des Namens des Beschuldigten im Bescheid über die Nichterhebung der Klage bzw. die Einstellung des Verfahrens für den Anzeigenden keine neuen personenbezogenen Daten desjenigen, den er ja selbst angezeigt hat.

Anders im Fall der Anzeige gegen Unbekannt, wenn der Anzeigende weder verletzt noch sonst strafantragsbefugt ist. Ein Interesse des Anzeigenden daran, den Namen der ermittelten Person, gegen die letztendlich die öffentliche Klage gar nicht erhoben bzw. deren Verfahren eingestellt wurde, zu erfahren, ist m. E. ebenso wenig ersichtlich wie eine Notwendigkeit für die Strafverfolgungsbehörden, dem Anzeigeerstatter den Namen des Beschuldigten zur Kenntnis zu geben. Die Übermittlung des Namens im Zusammenhang mit einem staatsanwaltschaftlichen Ermittlungsverfahren ist ein Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen. Dem Anzeigeerstatter, der zunächst nicht wissen konnte, welche Personen mit seinen zur Anzeige gebrachten Beobachtungen in Zusammenhang stehen könnten, wird die Identität einer Person mitgeteilt, die zumindest in den Kreis der Verdächtigen gerückt ist. Die Übermittlung

dieses Datums erfolgt, obwohl dem in der Anzeige innewohnenden Antrag auf Erhebung der öffentlichen Klage keine Folge gegeben oder nach dem Abschluss der Ermittlungen die Einstellung des Verfahrens verfügt wurde. § 171 Satz 1 StPO bietet keine gesetzliche Grundlage für die Übermittlung des Beschuldigtennamens, also für einen Eingriff in das in der Verfassung verankerte Recht auf informationelle Selbstbestimmung.

Das zwischenzeitlich informierte SMJus verwies unter Bezugnahme auf eine Stellungnahme des sächsischen Generalstaatsanwalts darauf, dass der Inhalt des Bescheids in § 171 Satz 1 StPO nicht näher geregelt, die Mitteilung des Namens des Beschuldigten an den Anzeigenden aber gerechtfertigt sei, weil ihm das Recht zur Aufsichtsbeschwerde sowie zur Gegenvorstellung zustehe. Darüber hinaus seien der Name des Beschuldigten und der Tatvorwurf erforderlich, um späteren Schriftwechsel oder Hinweise des Anzeigeerstatters einem Verfahren eindeutig zuzuordnen.

Inwiefern dem Anzeigeerstatter durch einen anonymisierten Bescheid die Möglichkeit der Aufsichtsbeschwerde bzw. Gegenvorstellung - beides gesetzlich nicht geregelte Verfahren - genommen sein könnte, ist nicht ersichtlich. Ausreichend für die eindeutige Zuordnung und Kennzeichnung eines Verfahrens ist das Aktenzeichen. Unter welchem Aktenzeichen ein Verfahren geführt wird - im Fall der Abgabe auch bei einer anderen als der zunächst tätigen Staatsanwaltschaft - kann dem Anzeigeerstatter ohne Mitteilung des Namens des Beschuldigten bekannt gegeben werden; die eindeutige Zuordnungsmöglichkeit bliebe erhalten. Eingriffe in das Recht auf informationelle Selbstbestimmung des Beschuldigten können vermieden werden, indem die Staatsanwaltschaft im Fall von Anzeigen eines nicht Verletzten gegen Unbekannt Einstellungsbescheide an den Anzeigeerstatter anonymisiert oder sich von vornherein auf die Benachrichtigung des Anzeigenden gemäß Nr. 9 RiStBV beschränkt, denn dann weiß der Anzeigeerstatter, dass seine „Anregung“ aufgegriffen und ein Ermittlungsverfahren eingeleitet wurde. Weitere Informationen aber, womöglich - wie im vorliegenden Fall - noch den Namen eines Beschuldigten, benötigt der, der Anzeige gegen Unbekannt erstattet hatte und nicht Geschädigter der Tat war, nicht.

Das SMJus teilte mir mit, dass es dem Generalstaatsanwalt des Freistaates Sachsen vorgeschlagen habe, die hier angesprochene Problematik im Rahmen der Neuprogrammierung des staatsanwaltschaftlichen Textverarbeitungssystems mit den am Entwicklerverbund beteiligten Ländern zu erörtern und sagte mir zu, mich über das Ergebnis zu unterrichten.

8.5 Berufsrechtliche Verschwiegenheitspflichten vs. Kontrollbefugnis des Sächsischen Datenschutzbeauftragten?

Im Rahmen der datenschutzrechtlichen Überprüfung einer Eingabe bat ich eine Notarin um einige Angaben zu einem ihrer Verfahren, an dem der Petent beteiligt war. In ihrem Antwortschreiben berief sich die Notarin auf § 18 BNotO und erklärte, erst dann Auskunft zu geben, wenn sämtliche Beteiligte sie von ihrer Verschwiegenheitspflicht befreit hätten. Des Weiteren verwies sie auf den Vorrang bereichsspezifischen (Bundes-)Berufsrechts vor allgemeinen (landesrechtlichen) Vorschriften.

Notare sind gemäß § 1 BNotO unabhängige Träger eines öffentlichen Amtes, die für die Beurkundung von Rechtsvorgängen und andere Aufgaben auf dem Gebiet der vorsorgenden Rechtspflege in den Ländern bestellt werden. Die Notare des Freistaates Sachsen sind öffentliche Stellen des Freistaates Sachsen im Sinne von § 2 Abs. 1 SächsDSG, sie unterstehen gemäß § 92 Nr. 3 BNotO der Aufsicht des SMJus.

Das Sächsische Datenschutzgesetz findet auf die Verarbeitung personenbezogener Daten in sächsischen Notariaten Anwendung.

Dagegen spricht nicht, dass spezialgesetzliche Vorschriften in der Bundesnotarordnung und dem Beurkundungsgesetz datenschutzrechtliche Bezüge aufweisen. Soweit diese Spezialvorschriften die Verarbeitung personenbezogener Daten regeln, gehen sie dem Sächsischen Datenschutzgesetz vor, dessen Regelungen insoweit subsidiär sind (§ 2 Abs. 4 SächsDSG).

Es ist jedoch zu berücksichtigen, dass einzelne - in verschiedenen Spezialgesetzen zu findende - Vorschriften zum Schutz personenbezogener Daten das allgemeine Datenschutzrecht nicht insgesamt, sondern eben nur insoweit verdrängen, wie sie den Schutz personenbezogener Daten regeln (§ 2 Abs. 4 SächsDSG). Ein hierfür typischer Fall ist die gesetzlich normierte Datenschutzkontrolle: Die datenschutzrechtliche Kontrolle der sächsischen Notariate (als öffentliche Stellen des Freistaates Sachsen) obliegt dem Sächsischen Datenschutzbeauftragten (§ 27 Abs. 1 SächsDSG). Die Kontrollbefugnis des Sächsischen Datenschutzbeauftragten korrespondiert der Pflicht der öffentlichen Stellen, den Sächsischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ausdrücklich beschränkt sich die Zuständigkeit des Sächsischen Datenschutzbeauftragten nicht auf die Kontrolle der Einhaltung des Sächsischen Datenschutzgesetzes; gemäß § 27 Abs. 1 SächsDSG kontrolliert er auch die Einhaltung anderer Vorschriften über den Datenschutz. Wenden öffentliche Stellen des Freistaates Sachsen in Ausübung ihrer gesetzlich übertragenen Tätigkeit Bundesrecht an und enthält das angewandte Recht Regelungen zum Schutz personenbezogener Daten, kontrolliert der

Sächsische Datenschutzbeauftragte die Einhaltung bundesrechtlicher Vorschriften über den Datenschutz. Andernfalls entstünden nicht hinnehmbare kontrollfreie Räume. Der Sächsische Datenschutzbeauftragte kontrolliert beispielsweise die Verarbeitung personenbezogener Daten in den Ausländerbehörden, die den Vorschriften des (bundeseinheitlichen) Ausländergesetzes unterliegt, ebenso wie die Einhaltung (bundeseinheitlicher) datenschutzrechtlicher Vorschriften in der Strafprozessordnung durch sächsische Staatsanwaltschaften.

Der Sächsische Datenschutzbeauftragte ist auch zur Kontrolle der Einhaltung der Datenschutzvorschrift des § 18 BNotO befugt; der Notar ist insoweit verpflichtet, Fragen zu beantworten und dem Sächsischen Datenschutzbeauftragten - auch und gerade vorgangsbezogene - Auskünfte zu erteilen. Die Kontrolle der Einhaltung des § 18 BNotO darf nicht mit dem Hinweis auf eben diese Vorschrift verhindert werden.

Dass auch die Datenverarbeitung, die besonderen Berufs- oder Amtsgeheimnissen unterliegt, durch den Sächsischen Datenschutzbeauftragten kontrolliert wird, normiert § 27 Abs. 1 S. 2 SächsDSG. Im Zuständigkeitsbereich des BfD erstreckt sich dessen Kontrolle gemäß § 24 Abs. 2 Nr. 2 BDSG auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Gemäß § 24 Abs. 6 BDSG gilt § 24 Abs. 2 BDSG entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind. Zwar verdrängen gemäß § 1 Abs. 2 Nr. 2 BDSG die Landesdatenschutzgesetze in ihrem Anwendungsbereich das Bundesdatenschutzgesetz - insofern ist die Übertragung der Kontrollbefugnis im Sächsischen Datenschutzgesetz maßgeblich -, § 24 Abs. 2 und 6 BDSG zeigen aber, dass auch der Bundesgesetzgeber die Notwendigkeit sah, Daten, die besonderen Berufs- oder Amtsgeheimnissen unterliegen, zum Zweck einer effektiven datenschutzrechtlichen Kontrolle der kontrollierenden Stelle zugänglich zu machen.

Die Argumentation, landesgesetzliche Regelungen - hier die des Sächsischen Datenschutzgesetzes - könnten bundesrechtliche Vorschriften nicht verdrängen, geht hier fehl, da es vorliegend gar nicht um die Rangordnung von Gesetzen geht, die denselben Regelungsinhalt haben. Der Grundsatz „Bundesrecht bricht Landesrecht“ (Art. 31 GG) kommt mangels tatbestandlicher Voraussetzungen hier nicht zur Anwendung.

Die Vorschrift des § 18 BNotO steht vorliegend nicht in Konkurrenz mit den die Kontrollbefugnisse des Sächsischen Datenschutzbeauftragten regelnden Vorschriften des Sächsischen Datenschutzgesetzes. Der Notar als öffentliche Stelle des Freistaates Sachsen ist gemäß § 28 Abs. 1 SächsDSG verpflichtet, den Sächsischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und Auskunft zu Fragen zu geben. Auf dieser gesetzlichen Grundlage sind für Kontrollzwecke des Datenschutzbe-

auftragten gegebenenfalls eben auch personenbezogene Daten aus einem konkreten Vorgang zu offenbaren, der Anwendungsbereich von § 18 BNotO ist insoweit nicht eröffnet. Es ist sinnwidrig, dem zur Kontrolle der Einhaltung der Verschwiegenheitspflicht Befugten eine erbetene Auskunft unter Hinweis auf eben diese Verschwiegenheitspflicht zu verweigern.

Mit diesen datenschutzrechtlichen Kontrollbefugnissen ist auch keine Absenkung des vom Notar gemäß § 18 BNotO geforderten hohen Schutzniveaus verbunden. Gemäß § 25 Abs. 6 SächsDSG sind der Sächsische Datenschutzbeauftragte und seine Mitarbeiter verpflichtet, über die ihnen bei ihrer amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit gegenüber jedermann zu wahren. Eine datenschutzrechtliche Aufsichtsbehörde, deren Kontrolltätigkeit den Schutz personenbezogener Daten gegenüber dem (spezialgesetzlich geregelten) Schutzniveau bei der kontrollierten Stelle vermindert, führte die Grundsätze des Datenschutzes ad absurdum, § 25 Abs. 6, 7 SächsDSG treffen hier die entsprechenden Vorkehrungen. Die Verschwiegenheitspflicht des Sächsischen Datenschutzbeauftragten entspricht in ihrer Qualität der Verschwiegenheitspflicht des Notars.

Nachdem auch das SMJus als oberste Aufsichtsbehörde für die sächsischen Notare davon ausgeht, dass die Verschwiegenheitspflicht des Notars nach § 18 BNotO die Kontrollbefugnisse des Sächsischen Datenschutzbeauftragten nicht einschränkt und die Notarin diese Einschätzung zur Kenntnis genommen hatte, erteilte sie schließlich die erbetenen Auskünfte.

8.6 Zustellung von Gerichtspost durch private Postdienstleister

Die mir bekannt gewordene Arbeitsweise eines durch ein sächsisches Gericht mit der Zustellung von Gerichtspost beauftragten privaten Postdienstleisters veranlasste mich, die in derartigen Konstellationen auftretenden datenschutzrechtlichen Probleme im Zusammenhang mit der Erfassung und Speicherung personenbezogener Daten im Rahmen des Zustellverfahrens gemeinsam mit dem SMJus zu erörtern.

Im Rahmen der Zustellung von Gerichtspost durch private Postdienstleister werden personenbezogene Daten verarbeitet; es liegt eine Datenverarbeitung im Auftrag gemäß § 7 SächsDSG vor. Dabei hat der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftraggeber bleibt für die Verarbeitung personenbezogener Daten verantwortlich. Diese gesetzlichen Maßgaben sind bei der Vertragsgestaltung mit privaten Postdienstleistern zu beachten.

Das SMJus wies in der Folge die Gerichtspräsidenten darauf hin, dass bei der Vergabe entsprechender Aufträge darauf zu achten sei, dass das ausgewählte Unternehmen Gewähr für die Durchführung der Maßnahmen zum Schutz personenbezogener Daten sowie für die Einhaltung der entsprechenden datenschutzrechtlichen Vorschriften bietet. Darüber hinaus bat das SMJus, derzeitige Vertragspartner der sächsischen Gerichte und Justizbehörden auf die Geltung dieser Vorschriften hinzuweisen.

8.7 Videoüberwachung im Amtsgericht

Der Präsident des Amtsgerichtes einer sächsischen Großstadt erkundigte sich, ob meinerseits Bedenken gegen die Installation einer Videoüberwachung in verschiedenen Bereichen des Amtsgerichtes bestünden.

Anlass für die Planung einer Videoüberwachung einschließlich Speicherung der aufgezeichneten Bilder seien wiederholte Beeinträchtigungen der Sicherheit der Bediensteten bzw. Vandalismuserscheinungen gewesen. Die Überwachung von Bereichen mit hohem Publikumsverkehr wie Rechtsantragsstelle, Entschädigungsstelle, Zahlstelle und Information sei erwogen worden. Die Überwachung spezieller Bereiche erscheine notwendig, um die Sicherheit der Bediensteten zu gewährleisten.

Ein Seiteneingang des Gebäudes, der als Behinderteneingang fungiere, sei ohne Videoüberwachung schlecht einzusehen; es gebe Personen, die die Situation ausnutzten, um das Gebäude betreten oder verlassen zu können, ohne den Wachtmeister oder die Information passieren zu müssen.

Der Einsatz des in Erwägung gezogenen Überwachungssystems lasse die Option zur Erweiterung auf weitere Bereiche bei Bedarf offen.

Die geplante Videoüberwachung der Bereiche mit hohem Publikumsverkehr konnte nicht meine Zustimmung finden.

Meine Bedenken erläuterte ich am Beispiel der Rechtsantragsstelle, bei der u. a. Klagen und Anträge formuliert, Erklärungen protokolliert und Beschwerden in FGG- und WEG-Verfahren sowie in Betreuungssachen entgegengenommen, also höchstpersönliche Angelegenheiten bearbeitet werden. Es wäre nun nicht unwahrscheinlich, dass ein Bürger aufgrund der Tatsache der Videoüberwachung in der Rechtsantragsstelle von seinem Vorhaben, seine Rechte mit Hilfe der Antragsstelle wahrzunehmen bzw. seine Absichten in die verfahrensrechtlich erforderliche Form zu bringen, Abstand nehmen würde.

Im Übrigen hielt ich die Maßnahme für ungeeignet, spontane Gewaltausbrüche von Besuchern - zum Großteil wird es sich nicht um geplante Aktionen handeln - zu verhindern. Besuchern eines Amtsgerichts muss ohnehin klar sein, dass sie sich in einem Gebäude aufhalten, welches durch die Präsenz zahlreicher Organe der Rechtspflege gekennzeichnet ist. Dennoch stattfindende Belästigungen wären auch durch eine Videoüberwachung nicht zu vermeiden.

Auch im Bereich des Behindertenzugangs hielt ich die Videoüberwachung nicht für erforderlich. Um den Besucherverkehr am Haupteingang zu kanalisieren und den Behinderteneingang als „Schlupfloch“ zu schließen, wäre es evtl. auch möglich, am Behinderteneingang eine Klingel zu installieren, die mit der Wachtmeisterstube oder Pforte verbunden ist. Im Bedarfsfall müsste dann ein Beamter dem Besucher öffnen.

Diese Vorgehensweise wird erfahrungsgemäß auch in anderen Gerichtsgebäuden und öffentlichen Einrichtungen praktiziert.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Lichtbildabgleich im Verkehrsordnungswidrigkeitenverfahren

Die im Berichtszeitraum festgestellte Anwendung eines Erlasses des SMI vom 18. November 1999 über die „Einsichtnahme des Polizeivollzugsdienstes und der Bußgeldbehörden in das Personalausweis- und Passregister wegen eines Bildabgleichs bei Verfahren wegen Verkehrsordnungswidrigkeiten“ durch die Verfolgungsbehörden verstößt gegen datenschutzrechtliche Grundsätze.

Der vorgenannte Erlass wurde seinerzeit im Einvernehmen mit dem Sächsischen Datenschutzbeauftragten erarbeitet, in der Anwendung zeigte sich aber, dass der Begriff des „Betroffenen“ zum Teil falsch ausgelegt wird.

So ist es gängige Praxis sächsischer Verfolgungsbehörden, auch andere Personen als den Fahrzeughalter in den Lichtbildabgleich einzubeziehen, wenn der Halter auf ein erstes Anhörungs-/Verwarnungsschreiben nicht reagiert oder von seinem Zeugnisverweigerungsrecht Gebrauch gemacht hat. Der Hinweis auf einen möglichen Lichtbildabgleich im Anhörungs-/Verwarnungsschreiben an den Halter rechtfertigt aber nicht den Lichtbildabgleich anderer Betroffener, etwa als Täter in Frage kommender Familienmitglieder, die weder angehört, noch auf einen möglichen Lichtbildabgleich hingewiesen wurden.

Pass- und Personalausweisdaten nach § 22 Abs. 2 PassG und § 2 b Abs. 2 PAuswG dürfen den Polizei- und Bußgeldstellen auf deren Ersuchen neben weiteren Voraussetzungen (u. a. Aufgabenerfüllung) nur übermittelt werden, wenn die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können.

„Betroffener“ im Sinne sowohl der genannten Vorschriften als auch des Erlasses ist nicht nur der Fahrzeughalter, gegen den in der Regel zunächst ein Ordnungswidrigkeitenverfahren eingeleitet wird, sondern jede einzelne vom Lichtbildabgleich betroffene Person.

Der Lichtbildabgleich eine Datenerhebung bei Dritten. Derartige Datenerhebungen sind gegenüber der Datenerhebung direkt beim Betroffenen grundsätzlich nachrangig. Die Subsidiarität der Datenerhebung bei Dritten findet sich im Sächsischen Datenschutzgesetz (§ 12 Abs. 4 SächsDSG) ebenso wie in den hier relevanten Vorschriften des Pass- bzw. Personalausweisgesetzes.

Entscheidend ist, dass die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden könnten (§ 22 Abs. 2 Nr. 3 PassG, § 2 b Abs. 2 Nr. 3 PAuswG).

Der Aufwand der Bußgeldstelle, nach der Auskunft der zuständigen Meldebehörde über volljährige Verwandte des Fahrzeughalters die als Täter in Betracht kommenden Personen anzuschreiben und in dieser Anhörung auf einen möglichen Lichtbildabgleich hinzuweisen, ist nicht unverhältnismäßig, denn der Bußgeldstelle liegt das anlässlich der Verkehrsordnungswidrigkeit aufgenommene Lichtbild vor, anhand dessen sie in der Lage ist, den Kreis der in Betracht kommenden Personen nach Alter und Geschlecht einzugrenzen.

Nach dieser Anhörung kann dann - soweit noch erforderlich - die Bußgeldstelle die Pass- und Personalausweisstelle um Übermittlung der Lichtbilder bzw. von Kopien derselben ersuchen; der Betroffene hatte die Möglichkeit, sich zur Sache zu äußern und weiß nun um die Möglichkeit des Lichtbildabgleichs. Bei einem Abgleich im familiären Umfeld (Ehegatte, Tochter, Sohn) hält sich der Kreis der Anzuschreibenden in engsten Grenzen, der Verfolgungsbehörde liegt das Beweisfoto vor, anhand dessen Geschlecht und ungefähres Alter erkennbar sein sollten, wenn das Beweisfoto tatsächlich Beweiskraft hat.

Eine derartige Vorgehensweise befände sich im Einklang mit den gesetzlichen Regelungen und vermiede eine „heimliche“ Datenerhebung in Form des Lichtbildabgleichs, von dem die betroffenen Personen nicht unterrichtet wurden.

Gemeinsam mit dem SMI wird derzeit eine Konkretisierung des Erlasses vorbereitet, die sowohl datenschutzrechtliche Belange der Betroffenen als auch das berechtigte Interesse der Verfolgungsbehörden an einer schnellen und mit möglichst geringem Verwaltungsaufwand verbundenen Bearbeitung der Verfahren in ausreichendem Maß berücksichtigt.

9.1.2 Telefonieren am Steuer

Der Tagespresse war im April 2004 zu entnehmen, dass infolge der Verschärfung des Ordnungswidrigkeitenrechtes telefonierende Autofahrer stärker belangt werden sollten. Der Bußgeldkatalog wurde dahingehend geändert, dass seit 1. April 2004 neben einer Geldbuße von 40 Euro auch 1 Punkt in Flensburg zu Buche schlägt. Eine Polizeidienststelle in Ostsachsen ließ in einem Interview zur geänderten Rechtslage verlauten, dass im Falle eines Ordnungswidrigkeitenverfahrens zum Beweis des Telefonates auf die

Verbindungsdaten mittels Abfrage beim Telekommunikationsanbieter zurückgegriffen werde.

Ich bat sowohl das SMI als auch den betreffenden Polizisten um eine Stellungnahme. Die Rechtslage stellt sich wie folgt dar:
Durch den § 100 g StPO wird die Möglichkeit eröffnet, bei der Strafverfolgung auf Telekommunikationsverbindungsdaten beim Netzanbieter nach richterlicher Anordnung zugreifen zu können. Als Voraussetzung wird dafür im § 100 g Abs. 1 StPO das Vorliegen einer Straftat von erheblicher Bedeutung, insbesondere - was aber nicht abschließend zu verstehen ist - eine Straftat nach dem Katalog des § 100 a Satz 1 StPO genannt.

Der in der Pressemitteilung geschilderte Fall, Telefonieren des Fahrzeugführers während der Fahrt, ist ein Verstoß gegen § 23 Abs. 1 a Satz 1 StVO. Dies ist eine Ordnungswidrigkeit im Sinne des § 24 Abs. 1 Satz 1 StVG i. V. m. § 49 Abs. 1 Nr. 22 StVO.

Für die Ahndung und Verfolgung einer Ordnungswidrigkeit ist das Gesetz über Ordnungswidrigkeiten (OWiG) anzuwenden. Dieses wiederum verweist teilweise auf die Vorschriften der Strafprozessordnung. Im § 46 Abs. 3 Satz 1 OWiG wird aber ausdrücklich klargestellt, dass im Ordnungswidrigkeitenverfahren Auskunftsersuchen über Umstände, die dem Post- und Fernmeldegeheimnis unterliegen, nicht zulässig sind. Eine Auskunft beim Netzanbieter über Telefonverbindungsdaten gem. § 100 g StPO ist im Ordnungswidrigkeitenverfahren daher nicht möglich.

Eine Maßnahme nach § 100 g StPO ist ein schwerwiegender Eingriff in die informationelle Selbstbestimmung des Einzelnen. Ein Zugriff auf die Telefonverbindungsdaten darf daher nur dann erfolgen, wenn der Verdacht einer Straftat von erheblichem Gewicht vorliegt. Für Ordnungswidrigkeiten wäre ein solcher Eingriff nicht verhältnismäßig.

Sowohl das SMI als auch die entsprechende Dienststelle versicherten, in Ordnungswidrigkeitenverfahren keine Auskünfte über Verbindungsdaten zu erheben. Infolgedessen konnte von einer Beanstandung abgesehen werden.

9.1.3 Halteranfragen privater Parkplatzbetreiber

Sowohl betroffene Bürger als auch eine Zulassungsbehörde wendeten sich im Berichtszeitraum mit der Frage an mich, ob die Übermittlung personenbezogener Daten im Rahmen einer Halterauskunft an private Parkplatzbetreiber zulässig ist.

In den mir vorgetragenen Fällen vermietete jeweils der private Parkplatzbetreiber Parkflächen zu einem bestimmten Tarif, dessen Inanspruchnahme durch das sichtbare

Hinterlegen des gelösten Parkscheins signalisiert wird. Löst der Benutzer kein Ticket, wird gemäß den Nutzungsbedingungen ein erhöhtes Nutzungsentgelt erhoben. Die Fahrzeuge, die ohne Parkschein auf dem Parkplatz abgestellt sind, werden fotografiert. Kommt der Benutzer der am Fahrzeug angebrachten Aufforderung zur Zahlung des erhöhten Nutzungsentgelts nicht nach, wendet sich der private Parkplatzbetreiber mit einer Halteranfrage an die Zulassungsbehörde.

Ich habe die Zulässigkeit der Übermittlung von Halterdaten durch die Zulassungsbehörde an private Parkplatzbetreiber bejaht.

Familienname, Vorname, Ordens- und Künstlername sowie die Anschrift als Halterdaten sind gemäß § 39 Abs. 1 StVG durch die Zulassungsbehörde unter anderem dann zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens darlegt, dass er die Daten zur Geltendmachung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr benötigt.

Das Parken auf einem privaten, allgemein zugänglichen Parkplatz ist als Teilnahme am öffentlichen Verkehr anzusehen; entscheidendes Kriterium für die Einordnung des privaten Parkplatzes als öffentlicher Verkehrsraum ist dabei die allgemeine Zugänglichkeit.

§ 39 Abs. 1 StVG verpflichtet die Zulassungsbehörde oder das Kraftfahrt-Bundesamt nicht allein im Fall gesetzlicher verkehrsbezogener Ansprüche zur Übermittlung der Halterdaten, sofern die weiteren Voraussetzungen vorliegen. Die Vorschrift spricht von „… Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr …“; auch wenn der Gesetzgeber dabei in erster Linie aus unerlaubten Handlungen abgeleitete Ansprüche im Auge hatte, lassen weder Gesetzeswortlaut noch -begründung einen Rückschluss darauf zu, dass § 39 Abs. 1 StVG eine Übermittlung ausschließlich für den Fall der Verfolgung gesetzlicher Ansprüche vorsieht. Auch der (vertragliche) Anspruch des privaten Parkplatzbetreibers ist ein Rechtsanspruch, der im Zusammenhang mit der Teilnahme am Straßenverkehr entstanden ist.

Dem Inhaber solch eines Anspruchs steht oftmals das amtliche Kennzeichen als einziger Anhaltspunkt für die Identitätsfeststellung des Anspruchsgegners zur Verfügung. Zur Verfolgung des Anspruchs ist daher eine einfache Registerauskunft notwendig; § 39 Abs. 1 StVG bietet die für eine Übermittlung personenbezogener Daten erforderliche Rechtsgrundlage. Das Gesetz unterscheidet dabei nicht zwischen verschiedenen Ansprüchen unterschiedlicher Natur. Entscheidend ist allein, dass ein Rechtsanspruch verfolgt wird, der im Zusammenhang mit der Teilnahme am Straßenverkehr steht.

9.2 Gewerberecht

9.2.1 Weitergabe von personenbezogenen Daten innerhalb einer Stadtverwaltung

Die Verwaltung einer Großen Kreisstadt wandte sich an mich mit der Frage, ob ihre Gewerbesteuerstelle auf der Grundlage des § 14 Abs. 6 GewO fallweise bzw. regelmäßig auch mittels automatisiertem Abrufverfahren (§ 14 Abs. 7 GewO) Daten vom Bereich Gewerbe der Stadtverwaltung erhalten könne. Die Gewerbesteuerstelle, die unter anderem die Bescheide für die Gewerbesteuervorauszahlung nach der Abgabenordnung erteilt, könne dann, so die Argumentation der Stadt, auf An-, Ab- und Ummeldungen von Gewerbetreibenden schneller reagieren, als wenn sie diese Informationen auf sonst üblichem Weg vom zuständigen Finanzamt erhalten würde. Könnten die Daten vom Gewerbeamt aber direkt übermittelt werden, so könnte beispielsweise verhindert werden, dass von Gewerbetreibenden unnötig steuerliche Vorauszahlungen verlangt werden. Die zur Aufgabenerfüllung der Gewerbesteuerstelle erforderlichen Daten seien konkret die Daten *Name und Anschrift des Gewerbetreibenden, angemeldete Branche, An-, Ab- oder Ummeldedatum* und *Anschrift der Betriebsstätte*. Zur Arbeitserleichterung und zeitnahen Ausführung beabsichtige man, so die Stadt, einen lesenden Zugriff auf das computergestützte Verfahren des Bereiches Gewerbe durch die Gewerbesteuerstelle im gemeindeinternen Computer-Netzwerk.

Ich beantwortete die Anfrage wie folgt: Die Gewerbeordnung sieht vor, dass vom Finanzamt den zuständigen Behörden - hier der Gewerbesteuerstelle der Stadtverwaltung - mitgeteilt wird, wenn die Steuerschuld von Unternehmen erloschen ist. Mitzuteilen sind *Name und Anschrift des Unternehmers und der Tag, am dem die Steuerpflicht endete* (§ 14 Abs. 1 a GewO). Eine regelmäßige Übermittlung von Daten vom Bereich Gewerbe an die Gewerbesteuerstelle ist auch grundsätzlich zulässig, wenn es sich wie hier - um die Weitergabe von Daten innerhalb der gesamten Verwaltungseinheit Gemeinde handelt, der die zuständige Behörde für die Entgegennahme der Gewerbeanzeige angehört (vgl. *Friauf*, Komm. z. GewO, 1998, § 14 Rdnr. 42; GewAnzVwV vom 6. Oktober 1995, SächsABl. S. 1259, Nr. 6.3.3). Allerdings beschränkt die Gewerbeordnung in § 14 Abs. 6 Satz 1 den Umfang der zulässig weiter zu gebenden Daten auf *Name, betriebliche Anschrift und angezeigte Tätigkeit*. Die Weitergabe weiterer Daten ist unter Beachtung der in § 14 Abs. 6 Satz 2 GewO genannten Voraussetzungen im vorliegenden Fall unzulässig. Dabei ist es nicht entscheidend, ob die Datenübermittlung z. B. regelmäßig per Liste mit unter Umständen zu schwärzenden einzelnen Daten - also nicht-automatisiert - oder durch einen automatisierten Abruf bzw. einen lesenden Zugriff der Gewerbesteuerstelle auf die Datei des Bereiches Gewerbe erfolgt.

Im Falle der Einführung eines automatisierten Abrufverfahrens ist nach der Gewerbeordnung unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Gewerbetreibenden zusätzlich zu prüfen, ob das automatisierte Verfahren wegen der Vielzahl der weiterzugebenden Daten oder ihrer Eilbedürftigkeit *angemessen* ist. Außerdem sind weitere datenschutz-organisatorische Regelungen wie die Protokollierung der Abrufe getroffen (§ 14 Abs. 7 GewO). In vergleichbaren mir vorgelegten Anfragen für automatisierte Datenübermittlungen in Kommunalverwaltungen habe ich unter der Voraussetzung, dass der Aufgabe und den beteiligten Stellen graduell eine gewisse Bedeutung zukommt, eine monatliche Fallzahl von 200 als erforderlich für die Angemessenheit einer automatisierten Datenübermittlung angesehen. Bei geringeren Fallmengen könnte - sofern überhaupt zweckmäßig - eine Weitergabe bestimmter Daten mit Einwilligung des Betroffenen erfolgen (§ 4 Abs. 1 Nr. 2 SächsDSG). So könnte beim Bereich Gewerbe dem Betroffenen der Vordruck einer vorbereiteten Einverständniserklärung zur Unterschrift vorgelegt werden, mit der seine Einwilligung für die Weitergabe der bezeichneten Daten an die Gewerbesteuerstelle eingeholt wird. Dabei ist der Zweck der Datenweitergabe zu beschreiben. Die Erklärung der Einwilligung darf in diesen Fällen nur freiwillig erfolgen, das heißt dem Gewerbetreibenden gegenüber ist deutlich zu machen, dass die Versagung der Einwilligung keinen Einfluss auf die Erteilung der Gewerbegenehmigung oder für ihn irgendwelche nachteilige Folgen hat. Auf die Freiwilligkeit ist auch auf dem Bogen der Einwilligungserklärung - die Einwilligung hat schriftlich zu erfolgen - hinzuweisen. Hinsichtlich der Form und des Verfahrens gelten im Übrigen § 4 Abs. 3 bis 5 SächsDSG.

10 Gesundheit und Soziales

10.1 Gesundheitswesen

10.1.1 Datenschutzrechtlicher Verstoß bei Einhaltung der 24-Stunden-Meldefrist nach dem Infektionsschutzgesetz

Ich erhielt einen Hinweis, dass das Gesundheitsamt eines Landkreises die Mitteilungspflichtigen nach § 8 Abs. 1 Nr. 2 und 3 IfSG aufgefordert hatte, Meldungen über meldepflichtige Krankheiten bzw. Nachweise von Krankheitserregern in der Zeit vom 23. Dezember 2003 bis 4. Januar 2004 per Telefax an die zuständige Rettungsleitstelle zu senden. Mitteilungspflichtige sind nach dem Infektionsschutzgesetz Leiter von Medizinaluntersuchungsämtern, sonstige private oder öffentlichen Untersuchungsstellen einschließlich der Krankenhauslaboratorien sowie Leiter von Einrichtungen der pathologisch-anatomischen Diagnostik. Das Gesundheitsamt berief sich bei dieser Verfahrensweise auf eine Mitteilung der Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen Sachsen im Ärzteblatt Sachsen Nr. 2/2001. Darin wandte sich die Behörde an die Ärzteschaft in Sachsen und informierte über „Modalitäten der Meldung von ‚Meldepflichtigen Krankheiten' und ‚Meldepflichtigen Nachweisen von Krankheitserregern' nach §§ 6 bis 10 IfSG im Freistaat Sachsen". Bestandteil dieser Information war die Aufforderung, dass, um die 24-Stunden-Frist der namentlichen Meldung an das zuständige Gesundheitsamt nach § 9 Abs. 3 IfSG in der Praxis einhalten zu können, außerhalb der normalen Dienstzeit sowie an Samstagen, Sonn- und Feiertagen, die entsprechende Meldung direkt an die Rettungsleitstellen erfolgen müsse.

Die Meldungen nach §§ 6 bis 10 IfSG enthalten regelmäßig besonders sensible Patientendaten, die dem Arztgeheimnis unterliegen und daher nur an die im Gesetz vorgesehene Stelle übermittelt werden dürfen. Wegen der klaren Regelung des § 9 Abs. 3 IfSG, wonach die Meldung an das zuständige Gesundheitsamt zu erfolgen hat, ist eine Meldung an eine Rettungsleitstelle unzulässig und datenschutzrechtlich zu beanstanden. Darüber hinaus unterliegen die Gesundheitsämter strengen gesetzlichen Auflagen zur Zweckbindung und Löschung der ihnen im Rahmen der Meldepflicht anvertrauten personenbezogenen Daten.

Ich wandte mich aus diesem Grund an das SMS als Aufsichtsbehörde mit der Bitte um Unterstützung und Stellungnahme. Das SMS, das sich meiner Auffassung anschloss, veranlasste im Rahmen der Amtsarztfortbildung die Herausgabe von Hinweisen zur datenschutzgerechten Verfahrensweise bei Meldefällen außerhalb der Dienstzeiten. Darüber hinaus wurde eine Richtigstellung zur Verfahrensweise bei Meldungen nach §§ 6 bis 10 IfSG außerhalb der offiziellen Dienstzeiten im Ärzteblatt Sachsen Nr. 9/2004 publiziert. Darin ist neben datenschutzrechtlichen Empfehlungen zum Umgang mit

Telefaxen klargestellt worden, dass eine Meldung über den Rettungsdienst ausgeschlossen ist und die Meldung auch außerhalb der offiziellen Dienstzeiten von Gesetzes wegen dem Gesundheitsamt direkt zu übermitteln ist. Das von mir beratene Gesundheitsamt des Landratsamtes korrigierte seine Verfahrensweise im Umgang mit Meldungen nach §§ 6 bis 10 IfSG außerhalb der offiziellen Dienstzeiten.

10.1.2 Stand der Einführung der elektronischen Gesundheitskarte in Sachsen

I. Einführung

Mit der geplanten Einführung der elektronischen Gesundheitskarte (eGK) wurde das bisher größte IT-Projekt in Deutschland überhaupt angestoßen. Die Karte soll nach dem Willen des Gesetzgebers flächendeckend eingeführt werden, ca. 70 Millionen Versicherte erfassen und der Kommunikation mit etwa 350.000 Ärzten, 2000 Krankenhäusern und den zahlreichen Krankenkassen in Deutschland dienen. Die über Jahrhunderte gewachsenen und bewährten Kommunikationsabläufe zwischen Patienten und Leistungserbringern in einer komplexen IT-Architektur abzubilden, ist daher auch in Bezug auf das Volumen eine gewaltige Herausforderung. Nicht nur für die IT-Branche, Gesundheitspolitiker und in Bezug auf den Ruf Deutschlands als Technologie-Standort steht viel auf dem Spiel.

Gleichwohl fehlt bei der elektronischen Gesundheitskarte jedoch eine politische Vision, eine nachvollziehbare Darstellung der Vorteile und Kosteneinsparungen im Sinne einer gesundheitspolitisch für alle wünschenswerten Lösung. Eine digitale, datenschutzgerechte, datensichere und als zentrale Informationssammlung geführte Patientenakte zum Beispiel gibt es eben nicht ohne Aufwand, nicht ohne Serverplatz und nicht zum Nulltarif. Daneben bestehen die (noch papiernen oder digitalen) Patientenakten bei den einzelnen Leistungserbringern (z. B. bei Ärzten und Krankenhäusern) weiter. Die elektronische Patientenakte, die über die eGK verarbeitet werden soll, ist jedoch eine der wesentlichen Neuerungen, an die große Erwartungen geknüpft werden. Worin soll dann aber letztendlich der Vorteil bestehen? Vielen Medizinern und Patienten erscheint die elektronische Gesundheitskarte allgemein wie eine Antwort auf eine Frage, die nie jemand gestellt hat. Sie wird als Lösungsangebot von den Bürgern nicht wahrgenommen, lediglich als nebulöse unausweichliche Neuerung im deutschen Gesundheitssystem und darunter leidet naturgemäß auch die Akzeptanz des Projekts.

Sofern die Antwort auf eine nicht gestellte Frage wenigstens messerscharf oder wenigstens einigermaßen konkret ist, kann man sich mit ihr noch irgendwie auseinandersetzen. Was die eGK angeht, liegt mir bis heute trotz vieler (politischer) Ankündigungen leider keine abschließende Lösungsarchitektur vor, die meinerseits datenschutzrechtlich und

datensicherheitstechnisch hätte beurteilt werden können. Der Grund liegt auf der Hand. Mit der elektronischen Gesundheitskarte wurde auf einfache und nachhaltige kostendämpfende Maßnahmen für die Gemeinschaft, wie sie z. B. schriftliche Informationen zur Herstellung einer Transparenz für die Patienten bei Abrechnungen medizinischer Leistungen im Bereich der gesetzlichen Krankenkassen darstellen könnten, verzichtet und ein komplexes System vorgeschrieben, dass sich dem Einzelnen von seinen gedachten Möglichkeiten und den Datenverarbeitungsvorgängen her nur schwer erschließt und insofern auch den beauftragten IT-Spezialisten entsprechende Schwierigkeiten bereitet. Das betrifft die Darstellung in datenschutzrechtlicher und -sicherheitstechnischer Hinsicht unmittelbar.

Umso bedauerlicher ist es aus meiner Sicht vor diesem Hintergrund, dass die öffentliche Diskussion auch noch aus einer gewissen technischen Sicht und mit Behauptungen über angebliche Kosteneinsparungen im Milliardenbereich beherrscht wird. Die Technik-Lastigkeit zeigt sich schon daran, dass z. B. die Idee der (zentralen) elektronischen Patientenakte (ePatientenakte) schwer mit den gesetzlichen Gegebenheiten in Einklang zu bringen ist, wonach in Deutschland die Vertraulichkeit der Gesundheitsdaten zwischen Patienten und jedem einzelnen Arzt zu wahren ist und diese nur durch eine Entbindung von der ärztlichen Schweigepflicht im Einzelfall gebrochen werden kann. Auch wirkt die Idee der ePatientenakte nicht als eine aus einer medizinischen Notwendigkeit heraus entstandene. So ist der Großteil der medizinischen Informationen über einen Menschen zumeist nur kurzzeitig valide und auch nur in einem bestimmten Zusammenhang verwertbar. Welcher Mediziner vertraut schon auf einen zwei Jahre alten Befund eines Kollegen anstatt eine erneute Untersuchung in Bezug auf den aktuellen Zustand eines Patienten anzustrengen? Schon diese vorstehenden einfachen Tatsachen limitieren den Nutzen, die Nutzung und Nutzbarkeit von Gesundheitsdatensammlungen über betroffene Patienten, die über einen gewissen Zeitraum angelegt worden sind. Hinzu kommt noch, dass die immer wieder ins Feld geführten fach- bzw. arztübergreifende Nutzungen von Gesundheitsdaten einzelner Patienten eben gerade nicht der Regelfall sind. Daher ist die bisherige Gesetzespraxis der Schweigepflichtentbindung im Einzelfall und die Übung der Arztbriefe ein geeignetes und wohl auch ausreichendes Instrumentarium, das Anliegen der Möglichkeit eines Zugriffs verschiedener Ärzte auf zentrale Sammlungen über einen Patienten hingegen aber zumeist nicht notwendig und daher auch letztendlich nicht datenschutzgerecht. Die Lösungsarchitektur des Systems und differenzierte Zugriffsberechtigungen haben insofern den rechtlichen und tatsächlichen Gegebenheiten Rechnung zu tragen und die wirklichen medizinischen Notwendigkeiten zu berücksichtigen, damit die Patientenrechte gewahrt bleiben. Dabei sind die Risiken, insbesondere bei Internet-basierten Zugängen auf zentrale Datenbestände, nicht zu unterschätzen. Eine 100-prozentige Sicherheit wird man bei Internet-basierten Sys-

temen nicht herstellen können und die Kenntnis um diese Tatsache darf den betroffenen Patienten gegenüber auch nicht unterschlagen werden. Eine vollständige Sicherheit kann gleichwohl natürlich auch nicht gefordert werden und sie gibt es auch gegenwärtig nicht beim Umgang mit Patientenakten, aber ich werde, was die sächsischen öffentlichen Stellen angeht, darauf achten, dass die Datenschutz- und Sicherheitsmaßnahmen in Bezug auf die ja letztendlich zusätzlichen Sammlungen von Patienteninformationen ein Maß behalten, dass der Sensibilität der Daten nach heutigem Stand der Technik angemessen Rechnung trägt. Kompromiss- und Übergangslösungen bin ich angesichts des Risikopotentials hingegen nicht bereit mitzutragen. Das gilt bereits für das Modellprojekt in Sachsen, das im Landkreis Löbau-Zittau in diesem Jahr beginnen soll (s. unten IV.5).

II. Die Lösungsarchitektur

Mit der Erarbeitung einer Lösungsarchitektur wurde die Fraunhofer-Gesellschaft unter Einbeziehung der bisher durch biT4health und protego.net entwickelten Lösungskonzepte beauftragt. Auf der CeBIT 2005 wurde von der Fraunhofer-Gesellschaft der Vorschlag für eine Lösungsarchitektur zur Einführung der elektronischen Gesundheitskarte („Version 1.0 der Spezifikation“)[5], auf die ich mich fortwährend in diesem Berichtsbeitrag beziehe, symbolisch an die Bundesgesundheitsministerin übergeben. Diese Lösungsarchitektur soll einen weiteren Schritt zum Aufbau der erforderlichen Telematikinfrastruktur darstellen und ist nunmehr einer Prüfung und Bewertung zu unterziehen. Die Einführung der eGK hat dabei, wie u. a. der BfD einfordert, für die Bürger transparent zu erfolgen.

Zugunsten des Projekts ist anzumerken, dass der konzeptionelle Ansatz der Lösungsarchitektur datenschutzrechtlich und technisch durchaus positiv zu bewerten ist. Einige Kapitel der Lösungsarchitektur besitzen aber derzeit immer noch Entwurfsstatus. Auch sind endgültige Abstimmungen zur Umsetzung der Anwendungen der eGK noch durchzuführen. Was die Nutzung der freiwilligen Anwendungen angeht, sind noch Details festzulegen. Tiefergehende datenschutzrechtliche Prüfungen der zu untersuchenden System-Abläufe konnten aufgrund der Komplexität noch nicht erfolgen. Eine eigens neu geschaffene Gesellschaft, die *Gematik*, der Krankenkassen und Verbände der Leistungserbringer angehören, hat nunmehr den Auftrag erhalten, Koordinierungs- und Betreiberfunktion in Bezug auf die Telematikinfrastruktur zu übernehmen. Sie soll die vorgestellte Lösungsarchitektur prüfen und technisch realisieren.

[5] Fraunhofer-Gesellschaft, ISST, IAO, SIT: Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte, Version 1.0 der Spezifikation vom 14. März 2005.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, der ich angehöre, wird die Einhaltung des Datenschutzes bei den Planungen und den anstehenden Testphasen weiterhin aufmerksam und kritisch begleiten.

III. Gesetzliche Regelungen zur eGK

Gesetzlich ist vorgesehen, ab Januar 2006 die bisherige Krankenversichertenkarte durch die eGK abzulösen. Im Sozialgesetzbuch, in § 291 a SGB V „Elektronische Gesundheitskarte“ wurden die verpflichtenden und die freiwilligen Anwendungen, die über die neue Karte realisiert werden sollen, verankert.

In der ersten Phase der Einführung ab 2006 soll die eGK vorerst die Pflichtanwendungen enthalten. Hierzu gehören:

a) Die Übermittlung ärztlicher Verordnungen in elektronischer Form (Arzneimittelverordnung, Überweisungen) sowie
b) der Berechtigungsnachweis zur Inanspruchnahme von Leistungen (Versichertenstammdaten, wie Kassenzugehörigkeit und Adresse sowie Daten, die zur Behandlung im europäischen Ausland berechtigen).

Neben den Pflichtanwendungen sind im Gesetz weitere Anwendungen auf freiwilliger Basis vorgesehen, deren Umsetzung bei der Gestaltung der Telematikinfrastruktur bereits berücksichtigt werden müssen. Zu den möglichen freiwilligen Anwendungen zählen: die Speicherung des Notfalldatensatzes, elektronischer Arztbrief, die Arzneimitteldokumentation, die elektronische Patientenakte (z. B. Befunde, Diagnosen, Therapiemaßnahmen), das Patientenfach (für sonstige Versichertendaten) und Daten über Leistungen und Kosten (Patientenquittung) der Versicherten.[6]

Die weitergehenden Anwendungen sollen zum besonderen Schutz der Patientendaten nur in Verbindung mit einem elektronischen Heilberufsausweis (HPC, Health Professional Card), zum Beispiel des behandelnden Arztes oder des Heilberuflers, der über eine qualifizierte elektronische Signatur verfügen muss, nutzbar sein. Durch Sicherungsmaßnahmen, wie das aufgedruckte Foto des Versicherten auf der Karte, soll ein Missbrauch der Versichertenkarten deutlich erschwert werden.

Durch die Einführung der eGK sollen die vorhandenen IT-Systeme der Ärzte, Apotheker, med. Einrichtungen und Krankenkassen über eine Telematikinfrastruktur vernetzt werden. Die neue eGK des Versicherten soll sowohl Datenträger als auch selbst Schlüssel des Versicherten zum Zugang zu seinen Daten und bereitgestellten Anwendungsdiensten sein. Die Karte wird daher als Chipkarte ausgestaltet, die prinzipiell zur

[6] § 291 a SGB V, in der Fassung vom 14. November 2003.

Authentifizierung, Verschlüsselung und elektronischen Signatur geeignet ist. Der Versicherte wird damit die Möglichkeit haben medizinische Daten (z. B. die Arzneimitteldokumentation) über seine Karte auf zentralen Servern speichern zu lassen und die Daten im Bedarfsfall dem Arzt oder Apotheker zugänglich zu machen.

IV. Anforderungen an die elektronische Gesundheitskarte

Der Schutz des Patientengeheimnisses muss auch in einer zunehmend IT-gestützten Medizin und bei der eGK wirksam gewährleistet sein:[7] Die Sicherheit des Systems selbst bemisst sich nach der Verlässlichkeit, der Verfügbarkeit, Integrität und Vertraulichkeit der Daten.

Kern der Überlegungen ist, dass sich die Patientenrechte durch die Einführung der elektronischen Gesundheitskarte nicht verschlechtern dürfen. Die hierfür erforderliche Beherrschbarkeit des Systems richtet sich nach der Zurechenbarkeit der Daten, Nicht-Abstreitbarkeit der Kommunikationsprozesse, Nutzungsfestlegung und Zugriffskontrolle, der Revisionsfähigkeit und Rechtssicherheit der Kommunikationsprozesse, der Durchsetzbarkeit der Betroffenenrechte (Auskunft, Berichtigung, Sperrung und Löschung), der Festlegbarkeit einer verantwortlichen Stelle für die Datenverarbeitung, Gewährleistung der freien Arztwahl, der Durchsetzbarkeit von Schadensersatzansprüchen und letztendlich auch nach der Praktikabilität für die Betroffenen (zu den grundlegenden Sicherheitsanforderungen an Medizinnetze.[8] Gerade in Bezug auf den letzten Punkt ist zu berücksichtigen, dass bestimmte Personen- und Gesellschaftsgruppen nicht durch eine zunehmend schwerer zu durchschauende Technik benachteiligt oder in der Wahrnehmung ihres Selbstbestimmungsrechts behindert werden. Werden die vorgenannten datenschutzrechtlichen Anforderungen beachtet, sollten weitergehend die IT-Struktur auch zu informationellen Vorteilen zugunsten der betroffenen Patienten genutzt werden und die Transparenz des Behandlungsgeschehens und der Datenverarbeitungswege für die Patienten erhöht werden. Nur bei der erforderlichen Transparenz für den Patienten können letztendlich die medizinische Behandlung effektiviert und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten gesenkt werden und damit für die Patienten wie auch für die Leistungserbringer Vorteile mit sich bringen.[9]

---

[7] 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Dresden, 27./28. März 2003: Entschließung - *Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung,* www.bfd.bund.de.

[8] Konferenz der Datenschutzbeauftragten des Bundes und der Länder*: Datenschutz und Telemedizin - Anforderungen an Medizinnetze* - Stand 10/02, S. 5 ff., www.bfd.bund.de.

[9] Vgl. hierzu: 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder Dresden, 27./28. März 2003: Entschließung - *Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung,* www.bfd.bund.de.

IV.1 Datenhoheit des Patienten und Freiwilligkeit

Von großer Bedeutung bei einer Speicherung von Gesundheitsdaten auf zentralen Servern ist, dass datensicherheitstechnische Belange so umgesetzt werden, dass die Patientenrechte, das Grundrecht auf informationelle Selbstbestimmung der Patienten gewahrt bleiben.

Gesetzlicher Ausgangspunkt ist § 291 a SGB V, wonach die elektronische Gesundheitskarte in Bezug auf die wesentlichen Datenverarbeitungsbereiche für die Patienten freiwillig ist. Dieses Freiwilligkeitserfordernis ist sachgerecht. Die Zusammenführung von besonders schutzwürdigen medizinischen Daten über die betroffenen Patienten ist aus Verfassungs- und Akzeptanzgründen nicht ohne Einwilligung der Betroffenen umzusetzen.[10] Dem Rechnung tragend hat der Gesetzgeber auch lediglich gewisse Versichertenstammdaten und das elektronische Rezept (eRezept) für die Patienten zur Pflicht gemacht.

IV.2 Einwilligung in die Datenverarbeitung

Das zentrale Patientenrecht, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden,[11] stellt für die technische Umsetzung eine zentrale Aufgabe dar, deren Lösung eines hohen Aufwandes bedarf. Jeder Patient, der eine Arztpraxis betritt, kann sich dafür entscheiden, dem jeweiligen Arzt alle freiwilligen Daten, nur einen Teil der Daten oder gar keine freiwilligen Daten zur Verfügung zu stellen. Auch muss der Patient die Möglichkeit haben, gegenüber einem Arzt lediglich einzelne Dokumente, z. B. seiner elektronischen Patientenakte, vorzuenthalten oder zu offenbaren. Das System darf nicht diejenigen, die ihre Daten aus den freiwilligen verarbeiteten Datenbereichen nur in Ausnahmefällen zugänglich machen wollen, benachteiligen. So kann nicht etwa die Freigabe der elektronischen Patientenakte grundsätzlich vorausgesetzt werden, wenn der Patient sie nur in bestimmten Einzelfällen nutzen will und er dann bei den Behandlungsvorgängen jeweils zur Wahrung seiner Rechte dafür Sorge tragen muss, dass die Daten von den von ihm nicht autorisierten Leistungserbringern nicht verarbeitet oder genutzt werden können (zur Gefahr der pauschalen Offenbarung von Patientendaten.[12]. Insofern ist es notwendig,

[10] Mit umfassenden und weiterführenden rechtlichen Ausführungen zur elektronischen Gesundheitskarte: Thilo Weichert, *Die elektronische Gesundheitskarte* in DuD 2004, S. 391 ff.

[11] Vgl. 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder Dresden, 27./28. März 2003: Entschließung - *Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung,* www.bfd.bund.de; 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Münster, 24.-26. Oktober 2001: Entschließung - *Datenschutzrechtliche Anforderungen an den "Arzneimittelpass" (Medikamentenchipkarte),* www.bfd.bund.de; 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder Bremen, 9./10. November 1995: Entschließung - *Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen,* www.bfd.bund.de.

[12] 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder Bremen, 9./10. November 1995: Entschließung - *Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen,* www.bfd.bund.de.

für jede einzelne freiwillige Anwendung auch eine anwendungs- oder fallbezogene Einwilligung durch den Patienten zu ermöglichen und diese auch zu dokumentieren, beispielsweise die Einwilligung zur Speicherung der medizinischen Daten einer chronischen Krankheit in der ePatientenakte.

Gegen die Einwilligungslösung, bei der die differenzierte Zustimmung des Patienten die Voraussetzung für die automatisierte Verarbeitung über die elektronische Gesundheitskarte ist, wird häufig grundsätzlich, aber zu kurz greifend eingewandt, dass die Datendokumentation damit zwangsläufig für die Leistungserbringer nicht vollständig sei.[13] Dem ist entgegenzuhalten, dass das Arzt-Patientengeheimnis notwendigerweise eine Unvollständigkeit der Datenweitergabe einschließt. Zu vergegenwärtigen ist stets, dass es sich bei den automatisiert verarbeiteten Patientendaten um Kopien handelt, denn die Dokumentationspflicht der Ärzte bleibt von der Einführung der eGK unberührt. Ärzte und Krankenhäuser haben weiterhin eigene Patientenakten zu führen. Der behandelnde Arzt verfügt letztendlich über die eigentliche vollständige Dokumentation in Bezug auf die Behandlung seines Patienten im Primärsystem seiner Praxis oder des Krankenhauses.

Inwiefern es technisch möglich, notwendig und gestattet sein soll, dass sich weitere Leistungserbringer Kopien der ePatientenakten oder der Arzneimitteldokumentation ihrer Patienten in ihre Primärsysteme in der Praxis oder im Krankenhaus zu laden - um beispielsweise die Krankengeschichte zu dokumentieren -, ist noch nicht umfassend überdacht worden. Würde eine häufige Vervielfältigung in der Praxis allerdings umgesetzt, könnten auf diese Weise schnell zahlreiche Kopien der Patientendaten entstehen, auf die der Patient auch keinen Einfluss mehr nehmen kann und dies würde die Datenhoheit des Patienten letztendlich in Frage stellen. Dies stellt ein praktisches Risiko dar, das es zu bedenken gilt.

Dass aufgrund sämtlicher vorstehender Erwägungen und wegen der Rechtslage die Erwartungen in Bezug auf die Einsparmöglichkeiten und den Nutzen der Karte selbstverständlich nicht zu hoch gesteckt werden können, sollte man insofern eigentlich voraussetzen.[14]

Ein zureichendes Konzept zur technischen und organisatorischen Umsetzung der Einwilligung bzw. der Möglichkeit der differenzierten Einwilligung in die freiwilligen Anwendungen der eGK liegt noch nicht vor. Neben der Frage der Dokumentation der

[13] Z. B. Peter Haas, Konsequenzen der Einführung der Elektronischen Gesundheitskarte für die Krankenhäuser, Tagungsband der 10. Fachtagung „Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen“, Juli 2004, Eigenverlag GMDS, S.13.

[14] Kritisch: Peter Haas, Konsequenzen der Einführung der Elektronischen Gesundheitskarte für die Krankenhäuser, Tagungsband der 10. Fachtagung „Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen“, Juli 2004, Eigenverlag GMDS, S. 15 - *am Ende.*

Einwilligung in die Nutzung einer freiwilligen Anwendung müssen auch der Widerruf und das Löschen der auf freiwilliger Grundlage verarbeiteten Daten geregelt werden. Im Detail muss auch festgelegt sein, wo die Einwilligung gespeichert wird, im Primärsystem des Arztes, auf der eGK oder auf dem Serversystem.

IV.3 Vergabe der Zugriffsrechten auf die Gesundheitsdaten

Einen weiteren Problembereich stellt die aufgrund des Selbstbestimmungsrechts des Patienten differenziert auszugestaltende Nutzungsberechtigungsarchitektur (u. a. Vergabe der Zugriffsrechte auf die Gesundheitsdaten) dar. Der Patient muss die Möglichkeit haben, bei der Einräumung der Datenverarbeitung in Bezug auf den Leistungserbringer sowohl nach einzelnen Personen als auch nach einzelnen Dokumenten zu differenzieren. Ggf. sollte auch nach einzelnen Facharztgruppen und Krankenhaus-Organisationseinheiten unterschieden werden können. Ferner muss in der technischen Umsetzung dafür Sorge getragen werden, dass die Informationsobjekte in einer Granularität, die wirklich eine datenschutzgerechte Wahrnehmung des Selbstbestimmungsrechts der Patienten gewährleistet, verarbeitet werden. Nur ein dabei vom Patienten kontrollierter und differenzierter Zugriff auf seine Gesundheitsdaten entspricht dem Sicherheitsanspruch und dem Anspruch auf Vertraulichkeit der Versicherten. Die Akzeptanz für freiwillige Anwendungen kann sicherlich erhöht werden, wenn dem Sicherheits- und Vertraulichkeitsanspruch des Bürgers im Sinne der „Datenhoheit des Patienten“ Rechnung getragen wird. In der zuletzt vorgestellten Lösungsarchitektur des Fraunhofer-Instituts sollen über eine rollenbasierte Zugangssteuerung den jeweiligen Gruppen des Gesundheitswesens nur die für diese Personen nutzbaren Dienste bereitgestellt werden. Dafür sind im Konzept so genannte virtuelle Sektorennetze für Arztpraxen, Zahnarztpraxen, Krankenhäuser, Präsenz- und Versandapotheken, eKioske und Internetzugang vorgesehen.

Zur Ausübung der Rechte der Versicherten werden „eKioske“ und auch die Anbindung der Heim-PCs von Versicherten in Betracht gezogen. Den Versicherten soll so der Zugang zu den über sie gespeicherten Daten ermöglicht werden über den sie u. a. die Berechtigungen für den Zugriff auf ihre medizinischen Dokumente festlegen oder Rezepte bei Versandapotheken bestellen können. Der eKiosk ist mit einem Kartenleser und einem Sicherheitsmodul ausgestattet und der Patient soll alleine mit seiner Karte, ohne die gleichzeitige Verwendung des Heilberufsausweises den Zugang zu seinen Daten eröffnet bekommen. Geplant ist, dass vom Karteninhaber, z. B. an einem eKiosk durch spezielle Kommandos das Sperren und Freigeben von Anwendungen vorgenommen werden kann.[15] Wie der Patient dagegen seine weiteren Zugriffsrechte orga-

[15] Fraunhofer-Gesellschaft, ISST, IAO, SIT: Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte, Version 1.0 der Spezifikation vom 14. März 2005, S. 259.

nisieren kann, ist bisher in der Lösungsarchitektur noch nicht enthalten. Weiterer Diskussionsbedarf besteht auch bei der Frage, wo die eKioske stehen sollen. Sollen sie in einer geschützten Umgebung - innerhalb eines sicheren LANs (LAN: „local area network“, die als zumeist auf ein Gebäude beschränkte Netzwerke relativ sicher sind), eines Arztes oder Apotheke - oder in anderen öffentlich zugänglichen Bereichen stehen.

Neben der Nutzung eines eKiosk soll der Patient grundsätzlich auch die Möglichkeit haben vom Heim-PC auf die Daten zuzugreifen, wobei nähere Details zur technischen Umsetzung noch offen sind. Desgleichen gibt es keine Hinweise in der Lösungsarchitektur, auf welche Anwendungen vom Heim-PC zugegriffen werden soll. Problematisch ist hierbei, dass sich der Heim-PC im Gegensatz zum eKiosk nicht in einer gesicherten Umgebung befindet. Ich gehe davon aus, dass nur die Nutzung einer gesicherten Einsatzumgebung und der geforderte Zugriff auf Daten in Verbindung mit einem Heilberufsausweis einen hinreichenden Schutz vor unerwünschter Einsichtnahme (z. B. Arbeitgeber) oder Preisgabe der Daten an Dritte gewährleisten. Wird vom gleichzeitigen Vorliegen des ärztlichen Heilberufeausweises der HPC (Healts Professional Card) abgegangen, könnte somit auf den Versicherten Druck ausgeübt werden, Unbefugten gegenüber seine Gesundheitsdaten zu offenbaren. Eine generelle Anbindung über die Heim-PCs der Versicherten mag daher zwar komfortabel sein, unterliegt aber nicht zu vertretenden Datensicherheits- und Datenschutzrisiken.

Alle Anwendungen im Rahmen der Telematikinfrastruktur der eGK basieren auf einer Kommunikationsstruktur, die auf dem Internet und Internettechnologien aufsetzen. Folgerichtig soll der Aufbau sicherer Kommunikationsverbindung zwischen eKiosk oder Leistungserbringer und den Telematik-Infrastrukturdiensten über eine verschlüsselte Verbindung (VPN: „virtual private network“) zwischen zwei Computersystemen hergestellt werden. Für die Ausführung besonders sicherheitskritischer Funktionen, beispielsweise der Vergabe von Zugriffsrechten auf die gespeicherten Patientendaten; soll die Möglichkeit der PIN-Authentifizierung des Versicherten vorgesehen werden. Inwieweit die Sicherheit der Patientendaten mit einer optional angebotenen PIN-Authentifizierung gewährleistet werden kann, ist datenschutzrechtlich noch umstritten.

Im Zusammenhang mit der Vergabe der Zugriffsrechte stellt sich letztendlich noch die Frage, welche Daten die Patienten außerhalb des elektronischen Patientenfaches (vgl. § 291 a Abs. 5 SGB V) löschen oder speichern dürfen, wie das Sperren der eGK bei Verlust oder Beschädigung und die Mitteilung der Sperrinformation bei Verlust oder Beschädigung der Karte erfolgt. Auch die grundsätzlichere Frage, wer letztlich entscheidet, welche Dokumente (Röntgenbilder, Befunde …) in das System eingespeist werden und wie lange diese Dokumente im System verbleiben sollen, ist zu beant-

worten. Sofern der Arzt oder Heilberufler diese Entscheidung allein zu treffen berechtigt sein soll, stellt dies wiederum die Datenhoheit des Patienten in Frage.

IV.4 Technische Lösung zur zentralen Datenspeicherung

Zentrale medizinische Datensammlungen sind potentiell in hohem Grade geeignet, Begehrlichkeiten bei Arbeitgebern, Kranken-, Unfall- oder Lebensversicherungen zu wecken, da zentrale Datenhaltung die Attraktivität von internen oder externen Angriffen auf das System erhöhen und gleichzeitig den Missbrauch der Patientendaten erleichtern kann. Datenschützer sind sich daher einig, dass bei der Einführung der Gesundheitskarte technisch gesehen, aus Vorsorgegründen auf Datenträgern keine lokalen Konzentrationen von Datensammlungen über den einzelnen Patienten entstehen dürfen. Die Daten sind ferner auch wirksam gegen Verlust, Zerstörung und unerlaubten Zugriff zu schützen. In der Lösung sind dafür besondere Regelungen vorzusehen, z. B. Verfahren bei Verlust oder Zerstörung der Karte oder Vertreterregelungen.

Für jeden Versicherten sollen technisch im System in einem sog. „Anwendungsordner“ vorerst nur die verpflichtenden Anwendungen - eRezept und Überweisung - angelegt werden. Alle Anwendungsdaten sollen dabei durch eine Zugangs- und Integrationsschicht (ZIS) über ein virtuelles Dateisystem verwaltet werden. Die Anwendungsdaten selbst sollen mit der eGK verschlüsselt im System gespeichert werden und sind nur wieder mit der eGK zu entschlüsseln. Über serverseitige Anwendungsdienste und die ZIS sollen die *verschlüsselten* Anwendungsdaten und die *unverschlüsselten* Verzeichnisdaten in logisch und physikalisch unabhängige Datenspeicher (ein oder mehrere Datenspeicher) abgelegt werden. Alle virtuellen Dateisysteme, die zum Versicherten angelegt sind und die er freigegeben hat, sollen unter einem sog. virtuellen „Wurzelverzeichnis“ zusammengefasst werden. Das Wurzelverzeichnis des Versicherten soll über dessen Krankenversichertennummer auffindbar sein.

Die Lösungsarchitektur lässt offen, welche Daten auf der Karte oder auf dem Server gespeichert werden sollen und auch ob ein serverbasierter Transport des eRezeptes oder ein kartenbasierter Transport erfolgen soll. Hierzu sind weitere konzeptionelle Lösungen gefordert. Erst wenn die fachlogische Lösungsarchitektur abgeschlossen ist, bin ich in der Lage, geplante Funktionen und Anwendungen der eGK datenschutzrechtlich zu beurteilen.

Hinsichtlich der Speicherung auf zentralen Servern ergeben sich neben allgemeinen Datensicherheitsaspekten durchaus auch im Zusammenhang mit der Nutzung durch andere Stellen ungewollte rechtliche Implikationen. Von einer nur auf das Patienten-Arzt/Apotheken-Verhältnis bezogenen Nutzung kann nicht mehr ohne weiteres ausge-

gangen werden. Ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht in Bezug auf die Daten, die auf der Karte gespeichert sind, besteht nicht mehr ohne weiteres.[16] Bei der Auswahl der datenverarbeitenden Stelle sollte dieser Gesichtspunkt nicht unbeachtet bleiben.

Die Integrität und Zurechenbarkeit der Daten ist durch eine qualifizierte elektronische Signatur sicherzustellen. Dabei spielt der Heilberufsausweis die entscheidende Rolle. Der Gesetzgeber hat ihn und die qualifizierte Signatur ausdrücklich vorgesehen, § 291 a Abs. 5 Satz 3 SGB V. Dabei sind sämtliche patientenbezogenen Dokumente von ihrem Urheber bzw. Verantwortlichen zu signieren. Dies kann einen in der Praxis nicht zu unterschätzenden Aufwand darstellen. Auch die weitere Pflege der Daten kann aufwendig sein, sind doch z. B. nach dem Ablauf einer gewissen Zeit Signaturen zu erneuern oder möglicherweise Datenformate anzupassen.

IV.5 Auswirkungen für den Freistaat Sachsen

Das BMGS plant, dass die eGK im Herbst 2005 in ausgewählten Regionen der Republik getestet werden kann. Im vierten Quartal des Jahres soll dann mit Kartentests in diesen Regionen begonnen werden. Der BfD hat bereits deutlich gemacht, dass bereits in der Testphase „ein Höchstmaß an Schutz und Sicherheit für die Gesundheitsdaten gewährleistet werden“ muss. Es komme darauf an, die verschiedenen technischen Lösungen für die eGK ohne Vorfestlegung auf ein bestimmtes technisches Verfahren zu testen und bei den Pilotprojekten die datenschutzfreundlichste Lösung zu finden.[17]

In Sachsen ist als Modellregion der Landkreis Löbau-Zittau vorgesehen. Bei dem Vorhaben, das auch als SaxMediCard bekannt ist, soll das hierfür von Organisationen der beteiligten Leistungserbringer geschaffene Projektbüro Rahmenbedingungen schaffen und Koordinierungsaufgaben wahrnehmen. Ich begleite das Vorhaben beratend. Die Modellregion ist ursprünglich als Projekt mit 130.000 Versicherten, 170 niedergelassenen Ärzten, 30 Apotheken und 130 sonstigen Leistungserbringern vorgesehen gewesen. Welche Größenordnungen letztendlich umgesetzt werden können, bleibt abzuwarten. Wegen der noch offenen Fragen bei der Lösungsarchitektur sind ferner auch bei dem Modellvorhaben konkrete datenschutzrechtliche Bewertungen nicht möglich.[18] Das Modellprojekt bezieht sich auf das verpflichtende eRezept und die freiwilligen Anwendungen Arzneimitteldokumentation und Notfalldaten. Die Ausgabe der Karten an

[16] Vgl. u. a. hierzu: 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder Dresden, 27./28. März 2003: Entschließung - *Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung*, www.bfd.bund.de.

[17] Pressemitteilung (10/05) des Bundesbeauftragten für Datenschutz Peter Schaar vom 14.3.2005, Bonn.

[18] Vgl. im Detail die Darstellungen unter www.gesundheitskarte-sachsen.de.

Leistungserbringer ist dabei noch in diesem Jahr und an die Versicherten Mitte des nächsten Jahres vorgesehen. Solange es sich noch um eine Testphase bzw. die Modellphase handelt, und eine Auswahl der einzubeziehenden Versicherten erfolgt, hat diese datenschutzgerecht und in Abstimmung mit mir zu erfolgen. Die Versicherten haben in datenschutzgerechter Weise einzuwilligen, insbesondere was die freiwilligen Anwendungen der eGK angeht. Der Patient ist insbesondere vor Einholung der Einwilligung in verständlicher, konkreter und umfassender Weise in Bezug auf eventuelle systembedingte Einschränkungen seiner Rechte zu informieren, § 4 Abs. 3 Satz 1 SächsDSG. Wegen der Wahrung der Selbstbestimmungsrechte sollten in einer Modellphase die Datenverarbeitungen auf Versicherte beschränkt bleiben, die auch selbst persönlich einzuwilligen in der Lage sind. Eine entsprechende Beratung zur datenschutzgerechten Verfahrensweise führe ich durch.

Zusammenfassend bleibt anzumerken, dass die bisher vorgelegten Konzepte zur Einführung der Gesundheitskarte noch eine Vielzahl von datenschutzbezogenen offenen Fragen beinhalten. Angesichts des Zeitplans - die Gesundheitskarte soll zum 1. Januar 2006 eingeführt sein - sind die nach dem Gesetz zur Schaffung der Sicherheitsinfrastruktur verantwortlichen Krankenkassen, Kammern und Berufsorganisationen unter Handlungsdruck, was aber in keinem Fall zu datenschutzrechtlichen Einbußen führen darf. Ein nachhaltiger Akzeptanz- und Vertrauensverlust auf Seiten der Patienten in Bezug auf die über die elektronische Gesundheitskarte zu verarbeitenden besonders schützenswerten Daten, die generell der ärztlichen Schweigepflicht unterliegen, ist geeignet, das Projekt ökonomisch und wegen seiner Sinnhaftigkeit in Frage zu stellen. Dies spätestens dann, wenn ein nicht unerheblicher Anteil der Patienten nicht bereit ist, die freiwilligen Möglichkeiten der Gesundheitskarte aus Selbstbestimmungsüberlegungen heraus zu nutzen. Unabhängig davon sehe ich es als meine Aufgabe an, die Bürger im Rahmen meiner gesetzlichen Unabhängigkeit über die Chancen und Risiken dieses Projektes in Sachsen aufzuklären.

10.2 Sozialwesen

10.2.1 Anforderungen an die Einwilligung in die Teilnahme an Strukturierten Behandlungsprogrammen im Falle des Unvermögens zur Vornahme der Einwilligungshandlung

Den gesetzlichen Krankenversicherungsträgern ist nach § 137 f SGB V die Möglichkeit eröffnet, Strukturierte Behandlungsprogramme, auch „Disease-Management-Programme“ oder kurz DMP genannt, einzuführen, um chronisch kranken Patienten eine bessere medizinische Versorgung zuteil werden zu lassen. Voraussetzung für die freiwillige Teilnahme durch „Einschreibung“ in ein solches Programm ist die Einwilligungserklärung des Versicherten, die sich insbesondere auf die mit der Teilnahme einher-

gehende zusätzliche Verarbeitung personenbezogener Daten bezieht (§ 137 f Abs. 3 SGB V).

Unter den in Frage kommenden Teilnehmern gibt es viele Versicherte, die aufgrund gesundheitlicher bzw. geistiger Behinderung keine Einwilligungserklärung mehr abgeben können. Eine große Krankenkasse hat sich aus diesem Grund mit der Frage an mich gewandt, ob sie selbst Anträge gemäß § 15 SGB X zur Bestellung eines Vertreters von Amts wegen beim Vormundschaftsgericht zur Einholung der erforderlichen Einwilligung in die Teilnahme an entsprechenden Behandlungsprogrammen stellen und hierzu den Geistes- bzw. Gesundheitszustand des Versicherten betreffende Sozialdaten an das Vormundschaftsgericht übermitteln dürfe, um auch diesem Personenkreis die besondere medizinische Betreuung in den Behandlungsprogrammen zukommen zu lassen (was zugleich der Krankenkasse Vorteile im sog. Risikostrukturausgleich, §§ 266 ff. SGB V, verschafft).

1. In meiner Stellungnahme habe ich zunächst angemerkt, dass es dem betroffenen Personenkreis, solange er in der Lage ist, die Einwilligungserklärung wirksam abzugeben, auch vorbehalten sein muss, über die Verwendung seiner Sozialdaten selbst bestimmen zu können. Soweit der betroffene Personenkreis aufgrund körperlicher Gebrechen oder Behinderung lediglich zur Unterschriftsleistung nicht in der Lage ist, jedoch die erforderliche Einsichtsfähigkeit für die Abgabe der Erklärung hat, ist § 67 b Abs. 2 Satz 3 SGB V zu beachten: Danach bedarf die Einwilligung der Schriftform, d. h. der eigenhändigen Unterzeichnung, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Von einer eigenhändigen Unterzeichnung ist dabei auch dann noch auszugehen, wenn der Betroffene beim Schreiben von einem Dritten unterstützt wird (Halten des Arms oder der Hand); eine bloße Unterstützung liegt so lange vor, als die Schriftzüge des Patienten von seinem Willen abhängig sind und von ihm bestimmt, also nicht vom Helfer geformt sind (vgl. Palandt-Edenhofer, Kommentar zum BGB, 61. Auflage 2002, § 2247 Rdnr. 6 zur vergleichbaren Problematik der eigenhändigen Unterschriftsleistung bei der Unterzeichnung eines Testaments).

   Soweit auch diese Anforderungen objektiv nicht eingehalten werden können, kann an die Stelle einer schriftlichen Einwilligung nur eine ebenso klar auf die konkret beabsichtigte Verarbeitung oder Nutzung der Daten bezogene und von Seiten der Krankenkasse einzuholende mündliche Erklärung treten. Die Einwilligung wird insoweit nicht unterstellt, sondern es wird nur ausnahmsweise eine andere Form als die grundsätzlich gebotene Schriftform zugelassen. Lediglich die Erklärungshandlung kann in anderer Weise als durch eigenhändige Unterschrift erfolgen. Eine stillschweigende oder gar mutmaßliche Einwilligung genügt dagegen nicht.

Das Vorliegen dieser Voraussetzung der mit der Teilnahme am Behandlungsprogramm verbundenen Verarbeitung personenbezogener Daten (vgl. § 137 f Abs. 3 Satz 2 SGB V) muss hinreichend dokumentiert sein.

2. Hiervon zu unterscheiden ist derjenige Personenkreis, der bereits aufgrund fehlender Auffassungsgabe nicht in der Lage ist, die Unterschriftsleistung zu erbringen. Bei dieser Patientengruppe fehlt es bereits an der für die Abgabe der Einwilligungserklärung erforderlichen Einsichtsfähigkeit, also der Fähigkeit, Gründe und Tragweite der Erklärung erfassen zu können. Es bleibt hier nur die Möglichkeit, dass ein Betreuer bestellt wird, der die Legitimation hat, diese Entscheidung für den Probanden zu treffen.

   Das in § 15 SGB X geregelte Verfahren zur Bestellung eines Vertreters von Amts wegen scheidet hierzu jedoch aus. Meine Überlegungen dazu sind Folgende:

   a) Folgt man der einleuchtenden Auffassung, dass der Entscheidung zur Teilnahme an Strukturierten Behandlungsprogrammen nach §§ 137 f, 137 g SGB V kein Verwaltungsverfahren zu Grunde liegt, scheidet die Anwendung von § 15 SGB X von vornherein aus, weil es sich nach der Systematik des Gesetzes um eine Vorschrift für das Verwaltungsverfahren handelt. Hinzu kommt, dass § 15 Abs. 1 SGB X eine abschließende Aufzählung der Bestellungsgründe enthält, sein Anwendungsbereich mithin nicht erweiterungsfähig ist (Kasseler Kommentar - Krasney, SGB, Stand 2003, § 15 SGB X, Rdnr. 2 m. w. N.; v. Wulffen, SGB X-Kommentar, 4. Auflage 2001, § 15 Rdnr. 7). § 15 Abs. 1 SGB X schiede dann bereits mangels tatbestandlicher Voraussetzung aus.

   b) Aber auch wenn man in der Erklärung des Versicherten, am Strukturierten Behandlungsprogramm teilnehmen zu wollen, und deren „Annahme“ durch den Sozialleistungsträger einen öffentlichen-rechtlichen Vertrag im Sinne des § 8 SGB X zu sehen hätte, schiede die Anwendbarkeit des § 15 SGB X hier nach seinem Sinn und Zweck aus:
   Die Regelung des § 15 Abs. 1 Nr. 4 SGB X soll dem Versicherten die - mangels eigener Einsichtsfähigkeit sonst nicht gegebene - Möglichkeit erhalten, erforderliche Leistungen zu erhalten bzw. sich gegen nachteilige Verwaltungsmaßnahmen zur Wehr zu setzen, z. B. mittels Einlegung von Rechtsbehelfen. Hierzu soll die Vorschrift eine beschleunigte und rechtsstaatlichen Grundsätzen entsprechenden Verfahrensdurchführung sicherstellen.

   Die Bestellung eines Vertreters von Amts wegen nach § 15 SGB X dient dagegen nicht der sozialen Fürsorge für den Betroffenen, die an sich eine Betreuungs-

anordnung gebietet; die Vorschrift stellt mithin keinen Ersatz für die Pflegschafts- oder Betreuungsregelung des BGB dar. Hier geht es jedoch weder um die Erlangung einer erforderlichen Leistung noch um die Abwehr einer belastenden Maßnahme. Denn nach eigenen Angaben der Krankenkasse führt die Nichtteilnahme an den betreffenden Programmen nicht zu einer Verschlechterung der ärztlichen Versorgungssituation des Betroffenen, vermindert also nicht die ihm zustehenden Ansprüche auf die Durchführung der Behandlung seiner Erkrankung nach den einschlägigen Vorschriften des Sozialgesetzbuches. Dem Versicherten entgeht lediglich eine besondere medizinische Betreuung und daraus folgend gegebenenfalls noch bessere Versorgung.

3. Würde der eigene Wille des Betroffenen mangels dessen Einsichtsfähigkeit durch die Willenserklärung eines auf Antrag des Sozialleistungsträgers zu bestellenden Vertreters ersetzt, führte der Sozialleistungsträger dadurch hinsichtlich der mit der Teilnahme am Strukturierten Behandlungsprogramm verbundenen zusätzlichen Verarbeitung personenbezogener Daten (§ 137 f Abs. 3 SGB V) einen Eingriff in das informationelle Selbstbestimmungsrecht des nicht mehr einwilligungsfähigen Patienten herbei. Dieser Eingriff wäre nicht von einer Rechtsgrundlage gedeckt. Denn es zählt nicht zu den gesetzlich vorgesehenen Aufgaben des Versicherungsträgers, den betreffenden Patienten zur Teilnahme an gesetzlich ja gerade als freiwillig ausgestalteten Behandlungsprogrammen zu verpflichten oder sonst zu veranlassen. Die Antragstellung stellte vielmehr eine - wenn auch in vermutlich bester Absicht erfolgende - Bevormundung des Versicherten durch den Sozialleistungsträger dar. In verfassungsrechtlicher Hinsicht findet hier das Sozialleistungsprinzip seine Grenze am informationellen Selbstbestimmungsrecht und damit an der Würde und Freiheit des betroffenen Patienten.

   Erst recht gilt dies im Hinblick darauf, dass eine entsprechende Antragstellung nach § 15 SGB X eine Übermittlung umfänglicher und höchst sensibler Sozialdaten (insbesondere hinsichtlich der zu behandelnden Erkrankung wie auch in Bezug auf die Gründe, die die mangelnde Einsichtsfähigkeit des Patienten belegen) erforderlich machte. Für diese Datenübermittlung fehlt es jedoch ebenfalls an der erforderlichen Rechtsgrundlage.

4. Schließlich: Die Krankenkasse hat ein eigenes finanzielles Interesse an der Teilnahme des Versicherten an einem entsprechenden Programm, da sie für jeden eingeschriebenen Versicherten Ansprüche (nämlich wohl dessen durchschnittliche Kosten) nach der Risikostrukturausgleichsverordnung (kurz: RSAV) geltend machen kann. § 15 Abs. 1 Nr. 4 SGB X ist jedoch auf Fälle zugeschnitten, bei denen an den von finanziellen Eigeninteressen der Behörde freien Gründen für eine Antragstellung (Abs. 1)

kein Zweifel bestehen kann. Anders ist die Kostenerstattungspflicht des vertretenen Beteiligten (§ 15 Abs. 3 Satz 2 SGB X) nicht zu rechtfertigen.

Nach Darlegung meiner Rechtsauffassung hat mir die Krankenkasse mitgeteilt, sie nehme von entsprechenden Antragsverfahren vor dem Vormundschaftsgericht Abstand.

10.2.2 Datenerhebung der Krankenkassen beim Rettungsdienst

Im Juni 2004 hat sich ein Rettungszweckverband an mich gewandt, nachdem er mehrfach von einer Krankenkasse aufgefordert worden war, Auskünfte im Zusammenhang mit durchgeführten Rettungseinsätzen zu geben. Abgefragt worden waren Angaben zum Grund der Behandlung, der Unfallart und nach Möglichkeiten zum Unfallort. Als Rechtsgrundlage wurde seitens der Krankenkasse hierfür die Vorschrift des § 294 a SGB V genannt.

Meine rechtliche Prüfung hat ergeben: Die gesetzlichen Krankenkassen sind *nicht* berechtigt, beim Rettungszweckverband (bzw. beim Rettungsdienst) Daten auf der Grundlage des § 294 a SGB V zu erheben. Für eine Übermittlung entsprechender Daten seitens des Rettungszweckverbandes an die gesetzlichen Krankenkassen kommt § 294 a SGB V als Ermächtigungsgrundlage nicht in Frage.

Begründung:
Nach § 67 a Abs. 2 Satz 2 Nr. 2 lit. a SGB X dürfen Sozialdaten durch unter § 35 Abs. 1 SGB I fallende Stellen, namentlich durch Sozialleistungsträger wie die gesetzlichen Krankenkassen, ohne Mitwirkung des Betroffenen bei anderen als den in § 35 SGB I bzw. in § 69 Abs. 2 SGB X genannten Stellen nur - sieht man von dem hier nicht in Frage kommenden lit. b der Vorschrift ab - erhoben werden, wenn eine Rechtsvorschrift die Erhebung bei ihnen zulässt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt. Was die gesetzliche Krankenversicherung betrifft, werden in den §§ 284 bis 293 SGB V (Zehntes Kapitel, 1. Abschnitt) unter den "Informationsgrundlagen" insbesondere die Datenerhebungsbefugnisse der Krankenkassen und Kassenärztlichen Vereinigungen geregelt, während in den §§ 294 bis 303 SGB V (Zehntes Kapitel, 2. Abschnitt) entsprechende Pflichten der Leistungserbringer zur Datenübermittlung bestimmt werden.
Im vorliegenden Fall handelte es sich um eine von der Krankenkasse auf *§ 294 a SGB V* gestützte, gerade die in dieser Vorschrift genannten Daten betreffende Datenerhebung. Nach der durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (BGBl. I vom 14. November 2003 S. 2190) zum 1. Januar 2004 in Kraft getretenen Vorschrift sind (nur)
- Vertragsärzte,

- ärztlich geleitete Einrichtungen und
- nach § 108 SGB V zugelassene Krankenhäuser

verpflichtet, die erforderlichen Daten, einschließlich der Angaben über Ursachen und den möglichen Verursacher, der Krankenkasse mitzuteilen, d. h. zu übermitteln, wenn Anhaltspunkte vorliegen, dass eine Krankheit Folge eines Unfalls ist oder Hinweise auf drittverursachte Gesundheitsschäden vorliegen.

Der Rettungszweckverband fällt nicht in den Anwendungsbereich dieser Vorschrift:

1. Zwar hätte man bei schlichter normtechnischer Verknüpfung des § 294 a SGB V mit § 10 Abs. 1 Satz 4 des bis zum 31. Dezember 2004 gültig gewesenen Sächsischen Rettungsdienstgesetzes (kurz: SächsRettDG), der seinerseits von einer Mitwirkung der Kassenärzte „im Rahmen des Sicherstellungsauftrags nach § 75 Abs. 1 SGB V“ gesprochen hat (die Bezugnahme auf gesetzliche Krankenversicherungen und niedergelassene Ärzte in § 28 Abs. 2 Satz 1 und 3 im neuen SächsBRKG stellt eine demgegenüber deutlich schwächere Beziehung zum SGB V her), für den Fall von einer Rechtsgrundlage für die Datenübermittlung ausgehen können, dass zufälligerweise gerade ein Kassenarzt im konkreten Rettungsdiensteinsatz tätig geworden ist. Schon die Fälle der Mitwirkung von Krankenhausärzten (§ 10 Abs. 1 Satz 3 SächsRettDG; jetzt ähnlich § 28 Abs. 2 Satz 3 und 5 SächsBRKG) wären indes hiervon nicht erfasst gewesen, jedenfalls soweit für den betreffenden Arzt nicht zugleich eine Zulassung zur ambulanten kassenärztlichen Versorgung vorgelegen hat. Hierbei dürfte es sich aber um die weit überwiegende Anzahl der bei Rettungsdiensteinsätzen tätigen Ärzte gehandelt haben und unverändert auch heute noch handeln. Keinesfalls umfasst waren und sind auch die zahlreichen Fälle, in denen ein Rettungsdienst, insbesondere in Form des Krankentransports (§ 1 Abs. 1 SächsRettDG; jetzt § 29 Abs. 1 und 2 SächsBRKG), ohne jegliche Mitwirkung eines Arztes tätig geworden ist bzw. tätig wird.

   Folglich fiele nur ein äußerst geringer Teil der vom Rettungszweckverband veranlassten Rettungseinsätze unter die Datenübermittlungsbefugnis des § 294 a SGB V - eben wegen der zufälligen Mitwirkung gerade eines Kassenarztes. Es ist in keiner Weise erkennbar, dass die Übermittlungspflicht bzw. -befugnis des § 294 a SGB V nach der Vorschrift von dieser Zufälligkeit abhängen soll. Denn Zweck der Vorschrift ist es, den Krankenkassen Informationen zur Verfolgung möglicher Regressansprüche zu übermitteln. Dieser Zweck besteht in anzuerkennender Weise unabhängig davon, ob der Rettungsdienst-Einsatz durch einen Vertragsarzt oder durch einen anderen Arzt durchgeführt wurde.

Hinzu kommt:
Die Rettungsdienste sind Leistungserbringer im Sinne des SGB V (Hauck/Noftz Rdnr. 81 zu § 2 SGB V; vgl. § 60 i. V. m. § 130 SGB V). Das Gesetz stellt in der § 294 a SGB V vorausgehenden Vorschrift eine Übermittlungspflicht für Vertragsärzte und die übrigen Leistungserbringer auf. In der § 294 a folgenden Vorschrift sieht das Gesetz eine Übermittlungspflicht genau für Vertragsärzte und ärztlich geleitete Einrichtungen vor. Daraus folgt: Das Gesetz bestimmt den Personenkreis der Übermittlungspflichtigen differenziert und mithin sehr genau. Aus der Nichterwähnung der "übrigen Leistungserbringer" in § 294 a folgt daher, dass diejenigen Erkenntnismöglichkeiten, die sich gerade durch die Tätigkeit des Rettungsdienstes (am Rettungsort) ergeben, als solche durch § 294 a nicht nutzbar gemacht werden sollen.

2. In all diesen Fällen kann auch nicht argumentiert werden, bei dem vom Rettungszweckverband veranlassten Tätigwerden handle es sich um eine „ärztlich geleitete Einrichtung“ im Sinne von § 294 a SGB V. Organe des Zweckverbands waren und sind nach § 4 SächsRettDG bzw. § 25 Abs. 2 SächsBRKG i. V. m. §§ 44, 47 Abs. 2, 15 Sächsisches Gesetz über kommunale Zusammenarbeit (kurz: SächsKomZG) die Verbandsversammlung und der Verbandsvorsitzende. Letzterer ist gemäß § 20 Abs. 1 Satz 1 SächsKomZG hauptamtlicher Beamter auf Zeit und in aller Regel kein Arzt, sondern ein in kommunalen Angelegenheiten erfahrender Bediensteter (z. B. ein Bürgermeister). Es ist zudem auch fraglich, ob bei einem Rettungszweckverband überhaupt von einer „Einrichtung“ im Sinne von § 294 a SGB V gesprochen werden kann, oder ob hiervon nur solche „Gebilde“ umfasst sind, die - ähnlich wie Krankenhäuser, Sanatorien u. ä. - eine benutzbare räumlich-sächliche Gesamtheit von Baulichkeiten umfassen müssen.

3. Nicht nur, wie jeweils miterwähnt, an diesen Gründen, sondern auch an diesem Ergebnis hat sich auch unter der Geltung des im Wesentlichen am 1. Januar 2005 in Kraft getretenen Gesetzes zur Neuordnung des Brandschutzes, Rettungsdienstes und Katastrophenschutzes im Freistaat Sachsen (GVBl. 2004, 245) nichts geändert: Nach § 28 Abs. 6 des Artikels 1 dieses Gesetzes, d. h. *des Sächsischen Gesetzes über den Brandschutz, Rettungsdienst und Katastrophenschutz - SächsBRKG*, haben die Rettungszweckverbände - nach näherer Maßgabe eines jedoch erst noch durch Rechtsverordnung (§ 26 Abs. 1 Satz 4 SächsBRKG) zu erlassenden Landesrettungsdienstplanes - zwar nun einen „Ärztlichen Leiter Rettungsdienst“ zu bestellen. Das macht den Rettungszweckverband jedoch noch nicht zu einer ärztlich geleiteten Einrichtung im Sinne von § 294 a SGB V. Dafür spricht schon die begrenzte Leitungsbefugnis dieses "Ärztlichen Leiters Rettungsdienst". Denn ausweislich des gesetzlichen Rahmens der Aufgabenzuweisung für diesen Leiter in Verbindung mit der Begrün-

dung des Gesetzentwurfs zu § 28 (LT-DS 3/9866) besteht seine Aufgabe darin, *„zu einer Qualitätsverbesserung der rettungsdienstlichen Versorgung beizutragen, indem er z. B. durchgeführte Rettungsdiensteinsätze auswertet und Verbesserungen veranlasst, sowie für die Fort- und Weiterbildung des nichtärztlichen Rettungsdienstpersonals Sorge trägt. Er kann auch zu einer wirtschaftlicheren Durchführung des Rettungsdienstes beitragen, indem er die Handlungsabläufe und die Steuerung des Einsatzes der Rettungsmittel verbessert.“*

Der ärztliche Leiter bleibt damit auf eine sehr allgemeine Mitwirkung beschränkt. Insbesondere wird ihm nicht die Zuständigkeit der Leitung einzelner Rettungseinsätze zukommen, sondern vielmehr die Rolle eines „Qualitätsmanagers“, so dass ihm Einzelfälle im Nachhinein nur zu dem Zwecke zu unterbreiten sind, dass er daraus dann Rückschlüsse für allgemeine Weisungen für eine zweckmäßige und wirtschaftliche Gestaltung vergleichbarer Einsätze ziehen kann.

Vor allem aber: Ärztlich geleitete Einrichtungen sind in § 294 a SGB V genauso wie in § 295 SGB V im technischen Sinne (Hauck/Noftz/Kranig Rdnr. 3 zu § 295 SGB V) zu verstehen als die in § 95 Abs. 1 und 4 SGB V genannte Einrichtungen, *die ermächtigt sind, an der vertragsärztlichen Versorgung teilzunehmen.* Es ist jedoch nicht erkennbar, dass der ärztliche Leiter wie auch die anderen im Rettungsdienst tätigen Ärzte im Hinblick gerade auf diese Tätigkeit eine solche Ermächtigung erhielten.

4. Angesichts dessen ist § 294 a SGB V so zu verstehen, dass er *insgesamt* keine Rechtsgrundlage für die Übermittlung der dort genannten Daten durch Rettungszweckverbände oder die in ihrem Auftrag Tätigen darstellt, auch nicht in den Fällen, in denen ein Vertragsarzt am Rettungseinsatz beteiligt ist.

Das SMI, das SMS sowie die meiner Kontrolle unterstehenden Krankenkassen haben sich vollumfänglich meiner Rechtsauffassung angeschlossen.

10.2.3 Datenschutzrechtliche Fragen im Zusammenhang mit der Verordnung häuslicher Krankenpflege

In großer Zahl erreichen mich Anfragen und Beschwerden in Fällen, in denen die gesetzliche Krankenversicherung im Hinblick auf die Verordnung häuslicher Krankenpflege Daten erheben will. Der Hintergrund ist folgender:
Gemäß § 37 SGB V erhalten Versicherte zu Hause neben der ärztlichen Behandlung häusliche Krankenpflege durch geeignete Pflegekräfte, wenn eine Krankenhausbehandlung geboten, aber nicht ausführbar ist oder wenn sie durch die häusliche Krankenpflege vermieden oder verkürzt wird. Die häusliche Krankenpflege umfasst die

erforderliche Grund- und Behandlungspflege sowie die hauswirtschaftliche Versorgung. Nach den hierzu auf der Grundlage des § 92 Abs. 1 Satz 2 Nr. 6 SGB V erlassenen „Krankenpflege-Richtlinien“ des Bundesausschusses der Ärzte und Krankenkassen in der Fassung vom 16. Februar 2000 wird häusliche Krankenpflege durch den behandelnden Arzt anhand eines vorgegebenen Formulars verordnet. Auf diesem hat der Arzt neben der verordnungsrelevanten Diagnose die Art und die Häufigkeit der jeweils konkret durchzuführenden Behandlungsmaßnahmen, also z. B. des Wechselns von Verbänden oder der Verabreichung von Medikamenten, anzugeben. Die im Vordruck beantragten Leistungen sind sodann noch von der Krankenkasse zu genehmigen.

(1) Mitarbeiter einer (meiner Datenschutzaufsicht unterstehenden) Krankenkasse waren nun dazu übergegangen, bei der Prüfung der Genehmigung nicht vom verordnenden Arzt, sondern unmittelbar vom bereits behandelnden *Pflegedienst* Auskünfte bzw. Angaben abzufordern, meist in Fällen, in denen der Arzt das Verordnungsformular unzureichend ausgefüllt hatte. Eine Vorgehensweise der Krankenkasse, die meiner Auffassung nach unzulässig ist. Denn es handelt sich hier ausschließlich um medizinische Daten, die auch ausweislich der genannten Krankenpflege-Richtlinien vom Vertragsarzt und von niemand anderem abzufordern sind. Die betreffende Krankenkasse hat mir gegenüber sehr schnell den Fehler eingeräumt und zugesagt, zukünftig entsprechende Anfragen bei den Pflegediensten zu unterlassen.

(2) Ein weiterer und zugleich zentraler Streitpunkt sind die von sog. „Pflegekräften“ der Krankenkasse durchgeführten *Hausbesuche* bei den pflegebedürftigen Versicherten.

Ich halte auch derartige Hausbesuche zum Zweck der Entscheidung über die Leistungsbewilligung für unzulässig: Die Krankenkasse ist zwar berechtigt, die ärztliche Verordnung zu prüfen, sie ist, mit anderen Worten, an die ärztliche Verordnung nicht gebunden. Denn nach § 27 Abs. 3 Bundesmantelvertrag-Ärzte bedarf es für die Leistungsbewilligung der Zustimmung der Krankenkasse zur Verordnung des Arztes (Genehmigung). Gleichwohl fehlt es meiner Auffassung nach an einer Rechtsgrundlage, die es der Krankenkasse erlaubte, beim Versicherten im Rahmen der Bewilligung häuslicher Krankenpflege - über die vom Arzt im Formular genannten Daten hinaus - zusätzliche medizinische Daten zu erheben. Dies gilt für eine Datenerhebung sowohl in schriftlicher wie auch in mündlicher Form, und diese Beschränkung darf daher auch nicht im Wege eines Hausbesuchs unterlaufen werden. Dies gilt insbesondere auch für eine gegebenenfalls im Rahmen eines solchen Hausbesuchs stattfindende Einsichtnahme in die beim Versicherten vorliegende vom Pflegedienst geführte *Pflegedokumentation*. Vor allem aber: Da die häusliche Krankenpflege von dem behandelten Arzt verordnet worden ist, hat dieser deutlich gemacht, dass er sie aus medizinischen Gründen zur Sicherung des Behandlungserfolgs für erforderlich hält. Eine Überprüfung der Verordnung hinsichtlich

dieser medizinischen Gründe darf jedoch allein durch den MDK erfolgen (vgl. Urteil des Bundessozialgerichts vom 30. März 2000, B 3 KR 23/99 R, E 86, 101 ff., Abschnitt 4 der Gründe), eine Einschaltung besonderer Pflegefachleute der Krankenkasse sieht das geltende Recht nicht vor.

(3) Die betreffende Krankenkasse hat mir nunmehr auch in diesem Punkt ausdrücklich zugestimmt, hält jedoch im Ergebnis weiterhin an der Zulässigkeit der Hausbesuche fest, und zwar mit folgender Begründung:

Ein Anspruch auf Bewilligung häuslicher Krankenpflege besteht nur, soweit nicht eine im Haushalt lebende Person den Kranken in dem erforderlichen Umfang pflegen und versorgen kann (§ 37 Abs. 3 SGB V). Es handelt sich insoweit um einen Ausschlusstatbestand, dessen (Nicht-)Vorliegen - nach Auffassung der Krankenkasse von dieser zu prüfen sein und auch von ihr selbst geprüft werden können soll, da damit keine Erhebung medizinischer Daten verbunden sei. Die Ermittlungen im Rahmen des Hausbesuchs beträfen allein die Frage, ob eine im Haushalt lebende Person in die Erbringung der Behandlungspflege mit einbezogen werden wolle oder könne.

Auch hier vertrete ich eine gegenteilige Auffassung: Die Feststellung, ob der Pflegebedürftige mit einer Person in einem Haushalt zusammenlebt, ist sicher noch eine Tatsache nichtmedizinischer Art, völlig anders verhält es sich jedoch mit der Frage, ob die Vornahme bestimmter Maßnahmen durch den Versicherten selbst möglich und zumutbar ist bzw. durch eine im Haushalt lebende Person. Dieser Entscheidung liegt zumindest auch eine medizinische Bewertung zu Grunde, da dies einerseits von der Erkrankung des Versicherten und dem damit verbundenen Pflegebedarf sowie andererseits von den Fähigkeiten, namentlich auch der körperlichen Konstitution, des im Hinblick auf seine Eignung als Pflegeperson zu beurteilenden Haushaltsangehörigen abhängt und somit anhand zu erhebender *medizinischer* Daten zu entscheiden ist (BSG a. a. O.). Dass diesem Erfordernis für die Verordnung häuslicher Krankenpflege gerade eine medizinische Bewertung zu Grunde liegt, zeigen auch die „Krankenpflege-Richtlinien“ (dort unter Nummer 11 Absatz 2), wonach die Frage, ob die verordnete Maßnahme vom Versicherten oder von einer im Haushalt lebenden Person durchgeführt werden kann, der Einschätzung des verordnenden Arztes obliegt. Und ein weiterer Punkt kommt hinzu: Die Regelung des § 37 Abs. 3 SGB V wird von der Rechtsprechung des Bundessozialgerichts aus überzeugenden Gründen gemäß § 2 Abs. 2 SGB I eng interpretiert: Danach kann die Krankenkasse die Genehmigung der Verordnung häuslicher Krankenpflege in der Regel erst dann versagen, wenn sowohl der zu Pflegende bereit ist, sich von dem (Haushalts-)Angehörigen pflegen zu lassen, als auch der in Betracht kommende (Haushalts-)Angehörige sich zur Pflege bereiterklärt hat (BSG a. a. O., unter 5 der Gründe). Eine Überprüfung des § 37 Abs. 3 SGB V durch die Krankenkasse in

Form von Hausbesuchen hat daher meiner Auffassung nach in der Regel von vornherein in den Fällen zu unterbleiben, in denen der Versicherte gegenüber der Krankenkasse auf dem Verordnungsblatt (dort Seite 2) angibt, dass er bzw. der (Haushalts-)Angehörige zu entsprechender Pflege nicht bereit ist.

(4) Auch soweit die Krankenkasse ihre Hausbesuche schließlich auch mit dem Vorhaben zu rechtfertigen versucht, den Versicherten bzw. dessen (Haushalts-)Angehörigen durch eine entsprechende Beratung und „Anleitung“ an Ort und Stelle an eine eigenständige Übernahme der Behandlungspflege heranführen zu wollen, überzeugt das nicht: Während § 37 SGB XI im Bereich der Leistungen nach SGB XI eine Beratungstätigkeit zur Optimierung der Pflege, zur Erleichterung der Pflege für Betroffene und für pflegende Angehörige vorsieht, findet sich eine entsprechende Regelung im Bereich des SGB V gerade nicht. Dabei ist zudem bedeutsam, dass hinsichtlich der Pflegeberatung nach § 37 SGB XI ausdrücklich vorgeschrieben ist, dass *nicht die Pflegekasse selbst* die Beratung durchführt. Eine Unterrichtung der Pflegekasse über die Beratungen erfolgt nur unter den Voraussetzungen des § 37 Abs. 4 SGB XI, d. h.: Mitteilungen über Erkenntnisse im Zusammenhang mit der Beratung nur durch die die Beratung durchführenden Stellen, und dies auch nur bei Einwilligung des Pflegebedürftigen.

Eine derartige Beratungsbefugnis der Krankenkasse im Bereich häuslicher Krankenpflege bedürfte daher m. E. der Aufnahme einer entsprechenden Regelung in das SGB V. Eine Erwähnung einer von der Krankenkasse zu erbringenden dahingehenden Leistung allein in den *Richtlinien* für die häusliche Krankenpflege dürfte nicht genügen. Hier besteht im Verhältnis zu den Krankenkassen noch einiger Gesprächsbedarf, insbesondere auch zu der Frage, inwieweit im Rahmen solcher Beratungsgespräche eine Beteiligung der Leistungserbringer, d. h. also der Pflegedienste, möglich ist.

10.2.4 Betreiben der Poststellen einer gesetzlichen Krankenversicherung durch Dritte?

Eine gesetzliche Krankenkasse im Freistaat bekam von einem im Bereich der Postbeförderung tätigen Unternehmen das Angebot, die Arbeit der bisher in den Dienststellen der Krankenkasse mit eigenen Bediensteten betriebenen Poststellen vollständig zu übernehmen. Und dies auch nicht etwa unter den Augen der Krankenkasse, sondern in den eigenen Geschäftsräumen des „Dienstleisters“: Dort sollte die Post geöffnet und mit Eingangsstempel versehen sowie entsprechend der Organisation der Krankenkasse sortiert und in die Sekretariate der Organisationseinheiten geliefert werden. Auch die Ausgangspost sollte das Unternehmen sammeln und zur Beförderung fertig machen. Das Unternehmen würde Einblick in die gesamte an die Krankenkasse gerichtete Post und

damit in alle nur denkbaren Gesundheitsdaten bis hin zu medizinischen Gutachten erhalten: Das Sortieren der Post ist ohne inhaltliche Kenntnisnahme nicht möglich.

Auf Bitte der betreffenden Krankenkasse habe ich das Angebot datenschutzrechtlich geprüft:

(1) Von einer solchen Auslagerung („Outsourcen“) der Poststellen einer Krankenkasse wären unzweifelhaft Sozialdaten i. S. d. § 35 Abs. 1 SGB I betroffen.

(2) Die Auslagerung der Poststellen wäre insoweit zulässig, als die Betroffenen in einen derartigen Umgang mit ihren Daten wirksam, insbesondere mit der nötigen inhaltlichen Bestimmtheit, eingewilligt hätten. Eine dahingehende schriftliche Einwilligung müsste, wohlgemerkt, bereits vor Umlenkung der betreffenden Post auf die ausgelagerte Poststelle eingeholt werden, eine nachträgliche Einholung reichte nicht aus. Die Einwilligung wäre jederzeit frei widerrufbar. Post von Personen, die eine solche Einwilligung verweigert, aus anderen Gründen noch nicht erklärt oder aber inzwischen widerrufen hätten, wäre getrennt zu behandeln. Diese Vorgehensweise musste daher bereits aus Praktikabilitätsgründen scheitern.

(3) In Übereinstimmung mit anderen Landesbeauftragten für den Datenschutz neige ich der Auffassung zu, dass es sich bei der angebotenen Auslagerung der Poststellen rechtlich um eine Auftragsdatenverarbeitung im Sinne von § 80 SGB X handelte. Eine Funktionsübertragung läge nur dann vor, wenn das Unternehmen eine gesetzliche Aufgabe der betreffenden Krankenkasse (als Leistungsträgers) übertragen bekäme. Hingegen übernimmt eine gemäß § 80 SGB X beauftragte Stelle nur Hilfsfunktionen zur Erfüllung von Aufgaben des weiterhin verantwortlichen Leistungsträgers.

Es besteht aber ja kein eigener gesetzlicher Auftrag der gesetzlichen Krankenkassen, als Leistungsträger eine Poststelle zu betreiben. Zwar kann das Betreiben einer Poststelle als unabdingbare Voraussetzung für die Erfüllung der gesetzlichen Primäraufgabe einer gesetzlichen Krankenkasse angesehen werden. Dies kann allerdings nicht dazu führen, dass die Verteilung der Postsendungen als eine der gesetzlichen Primäraufgabe der Krankenkasse gleichstehende Aufgabe und damit als möglicher Gegenstand einer Funktionsübertragung verstanden werden kann.

(4) Voraussetzung einer zulässigen Auftragsdatenverarbeitung im Sinne von § 80 SGB X ist allerdings, dass die Aufgabe des Auftragnehmers in der bloßen Datenverarbeitung (im weiteren Sinne) ohne größere eigene Entscheidungsbefugnis liegt, da nur dann der Auftragscharakter bestehen bleibt. Entscheidend ist also, inwieweit dem Auftragnehmer eigene Entscheidungsbefugnisse zugestanden werden und wie konkret der Auftrag zur Datenverarbeitung erteilt wird, hier: wie konkret das Post-Unternehmen das

Öffnen der Postsendungen, die Registrierung des Posteingangs sowie die Verteilung und das Einsammeln der Postsendungen im Rahmen des Auftrags durch verbindliche Leitlinien seitens der Krankenkasse vorgegeben würden.

(5) Die Zulässigkeit einer Auftragsdatenverarbeitung durch - wie hier - nicht-öffentliche Stellen setzt nach § 80 Abs. 5 Nr. 2 Satz 1 SGB X (Nr. 1 der Vorschrift kommt offenkundig nicht in Betracht) weiter voraus, dass die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst.

Insoweit hätte es der Krankenkasse oblegen, nachvollziehbar darzulegen, dass die Bearbeitung der Postsendungen durch das Unternehmen mit erheblichen Einsparungen verbunden wäre; dabei wären auch die nach § 80 Abs. 2 SGB X zu treffenden technischen und organisatorischen Datenschutzmaßnahmen in eine entsprechende Vergleichsberechnung einzustellen. Es ergeben sich aber noch weitere Voraussetzungen für die Zulässigkeit der Auslagerung der Poststellen in Form der Auftragsdatenverarbeitung, die in § 80 Abs. 1 und 2 SGB X detailliert genannt sind: So wäre u. a. gemäß § 80 Abs. 2 Satz 1 SGB X die Auftragserteilung auch nur zulässig, wenn der Datenschutz bei dem Unternehmen den Anforderungen genügen würde, welche für die Krankenkasse Geltung beanspruchen. Es bestehen unter den Landesbeauftragten der Länder insoweit Zweifel, ob ein privates Unternehmen in der Lage ist, den Schutz der in der hausinternen eigenen Poststelle der Krankenkasse eingehenden Sozialdaten (insbesondere z. B. auch medizinische Unterlagen) bei einer Auslagerung der Poststellen in der gleichen Weise sicherzustellen. Auch kann z. B. zumindest nicht ausgeschlossen werden, dass eine - wenn auch gegebenenfalls ungewollte - Vermengung mit der Post anderer Kunden des Post-Unternehmens erfolgt. Überdies ist zu bedenken, dass das Unternehmen bzw. ein mit ihm verbundenes Unternehmen möglicherweise am Anschriftenhandel beteiligt sind.

(6) Inwieweit es schließlich im grundsätzlichen Interesse einer gesetzlichen Krankenkasse liegen kann, wenn die Versicherten bei der Übersendung von - zum Teil höchstsensiblen! - Sozialdaten ein unbehagliches Gefühl haben, wenn diese Unterlagen nicht von ihrer Krankenkasse, sondern von einer anderen Einrichtung, zumal von einem großen Postbeförderungsunternehmen, geöffnet und zu Verteilungszwecken teilweise zur Kenntnis genommen werden, habe ich nicht zu beurteilen gehabt. Es würde aber wohl, darauf habe ich mir doch hinzuweisen erlaubt, einer aufwendigen Öffentlichkeitsarbeit seitens der Krankenkasse bedurft haben, ihren Versicherten diese Einschaltung des Postunternehmens in den Geschäftsgang zu vermitteln.

Im Ergebnis, und wohl gerade auch angesichts all dessen, hat die Krankenkasse von der erwogenen Auslagerung ihrer Poststellen Abstand genommen.

10.2.5 Biographiegespräche im Pflegeheim

Im Jahr 2003 erfuhr ich von einer Bewohnerin eines Pflegeheimes, dass das Heim biographische Angaben über seine Bewohner zusammenstellte: An Hand eines von einem Fachverlag vertriebenen umfangreichen Vordruckes, der die Bezeichnung „Biographiegespräch“ trug, wurden den Betroffenen von den Pflegekräften Fragen zu allen Lebensabschnitten gestellt, und zwar durchaus zum Teil auch sehr persönliche, ja intime: Benimmregeln und Witze aus dem Elternhaus, Name des Kuscheltieres, Idole der Jugend, Liebeserlebnisse, auch die Frage, was dem Betroffenen als Erwachsenen heilig gewesen ist, welche politischen oder religiösen Überzeugungen er gehabt hat, welche Reiseziele, welche Ängste, auch wie es im Alter um die Gesundheit des Lebenspartners gestanden hat, und vieles andere mehr.

Entsprechend den Antworten wurden von den Pflegekräften Eintragungen in den Erhebungsbögen vorgenommen. In manchen Fällen wurden diese „Biographiegespräche“ wohl auch schon mit Bewerbern um einen Heimplatz vor deren Einzug in das Pflegeheim geführt.

(1) Solche Datensammlungen greifen in das Recht des Heimbewohners auf informationelle Selbstbestimmung ein. Soweit - wie mir berichtet wurde - sich die Träger der Heime durch öffentliche Stellen, nämlich durch die Pflegekassen bzw. deren Medizinischen Dienst (den MDK) sowie die Heimaufsicht, zu diesen Datenerhebungen veranlasst sehen, gilt: Öffentliche Stellen dürfen ihrer Aufsicht unterliegende Private nicht zur Verarbeitung personenbezogener Daten anhalten, wenn sie nicht gesetzlich dazu ausdrücklich ermächtigt sind oder wenn diese Verarbeitung nicht unzweifelhaft privatrechtlich rechtmäßig ist. Das folgt aus der Grundrechtsbindung der öffentlichen Gewalt (Art. 1 Abs. 3 GG) bzw. der Gesetzesbindung der vollziehenden Gewalt (Art. 20 Abs. 3 GG). Das SGB XI enthält eine solche Rechtsgrundlage aber nicht, und auch an einer zivilrechtlichen Erlaubnis fehlt es.

(2) Die Datenerhebung ist insbesondere für die Erfüllung der in § 75 Abs. 1 SGB XI für vollstationäre Einrichtungen festgehaltenen Dokumentationspflicht des Leistungserbringers nicht erforderlich. Es steht außer Frage, dass die Erbringung von Pflegeleistungen - gerade auch zum Schutz der Heimbewohner - überprüfbar sein muss. Dazu sind die Pflegeleistungen des Leistungserbringers zu dokumentieren und unterliegen sie der Überprüfung durch die Pflegekasse bzw. - bei Anhaltspunkten für unzureichende Pflegeleistungen - durch den MDK. Eine derart detaillierte Beschreibung der Persönlichkeit der zu pflegenden Person, wie dies der betreffende Fragebogen vorsah, ist für die Prüfung von Pflegeleistungen weder geeignet noch erforderlich und überdies unverhältnismäßig. Dies wurde mir auch von einer meiner Aufsicht unterliegenden Kranken-

kasse bestätigt, wonach seitens der Pflegekassen von den Heimen nicht verlangt wird, dass sie Datensammlungen anhand des betreffenden Fragebogens oder anhand ähnlicher Vordrucke anlegen.

(3) Es ist auch nicht erkennbar, dass die Erhebung der betreffenden Daten der Erfüllung des Heimvertrages seitens des Heimes im Sinne von § 28 Abs. 1 Nr. 1 BDSG dienlich sein könnte, wenn es nicht der unzweifelhafte und selbstbestimmte, konkret geäußerte Wunsch des Heimbewohners ist, dass im Heim eine solche Dokumentation über ihn angelegt wird. Das gilt auch im Hinblick auf den gut nachvollziehbaren Gesichtspunkt, dass man vor dem Eintritt einer Demenzerkrankung noch etwas über die Lebensgeschichte der betreffenden Person wissen möchte, um später besser für sie sorgen zu können. An die Feststellung der Selbstbestimmtheit des Wunsches sind dabei hohe Anforderungen zu stellen. Von Freiwilligkeit kann bei der Befragung hilfsbedürftiger Personen, um die es hier geht, ganz allgemein nicht ohne weiteres die Rede sein, da der betreffende Personenkreis von den befragenden Personen in starkem Maße abhängig ist. So wurde mir damals in glaubhafter Weise berichtet, dass - statt auf die Freiwilligkeit hinzuweisen - den Heimbewohnern erklärt worden sei, das Heim werde geschlossen, wenn nicht alle den Fragenkatalog beantworteten!

(4) Richtig ist: Das Pflegepersonal sollte Gespräche mit dem Heimbewohner ermöglichen, wenn der Gepflegte dies wünscht. Solche, auf der Grundlage eines gegebenenfalls erst nach längerer Zeit entstandenen Vertrauensverhältnisses zwischen Pfleger und Gepflegten geführten Gespräche unterscheiden sich jedoch ganz wesentlich von Interviews, wie sie anhand des Fragebogens durchgeführt werden sollten. Wer in einem Pflegeheim lebt, ist in besonderem Maße auf die Hilfe und Fürsorge anderer, insbesondere des Pflegepersonals, angewiesen. Aber auch wer auf Pflegeleistungen angewiesen ist, hat das Recht auf Achtung seiner Intimsphäre. „Biografiegespräche“ unter Einsatz von Fragebögen der hier verwendeten Art sind nichts anderes als Befragungen und Ausfragungen. Sie stellen einen Akt der Entmündigung und einen nicht zu rechtfertigenden Eingriff in das Persönlichkeitsrecht des betroffenen Heimbewohners dar.

(5) Erfreulicherweise kommt nach Mitteilung des SMS der entsprechende Fragebogen nicht mehr zum Einsatz, auf die Einführung eines landesweit einheitlichen Biographieformulars wurde indes verzichtet. Nach Angaben des SMS soll lediglich die Orientierungshilfe des Landespflegeausschusses zum Thema Pflegeplanung und Pflegedokumentation um eine Unterrichtung der Heimträger über die Verwendung eines Biographieblattes (das über die nach § 13 Abs. 1 Nr. 4 HeimG vorgeschriebene Datenerhebung hinaus weitere erfragte biographische Daten enthält) dahingehend ergänzt worden sein, dass den Heimträgern empfohlen werde, im Informationsschreiben an die Bewerber um

einen Heimplatz darauf hinzuweisen, dass diese Datenerhebung freiwillig sei und keinen Einfluss auf den Abschluss des Heimvertrages habe.

Ich habe dem SMS, dem beim SMS angesiedelten Landespflegeausschuss sowie den für Heimaufsicht zuständigen Stellen mitgeteilt, dass ich derartige Empfehlungen nicht für ausreichend erachte, insbesondere was die für die Einwilligung erforderliche vorherige umfassende und verständliche Aufklärung des Heim*bewohners* angeht. Auch ist meiner Auffassung nach seitens der Heimträger sicherzustellen, dass sich die Datenerhebung jeweils nach den Besonderheiten des einzelnen Pflegefalles auszurichten hat.

Eine Antwort auf diese Kritik habe ich bisher nicht erhalten. Auch ist mir bislang trotz meiner Aufforderung die genannte Orientierungshilfe (alter und neuer Fassung) nicht übermittelt worden.

10.2.6 Krankenkassen-Werbung unter Verwendung personenbezogener Daten - an Schulen und überhaupt

Mit meiner vergleichsweise restriktiven Rechtsauffassung zur Verarbeitung personenbezogener Daten durch die gesetzlichen Krankenversicherungen *zu Werbezwecken* bin ich im Jahre 2002, wie in 11/10.2.2 dargestellt, vom Bundessozialgericht vollauf bestätigt worden. In Reaktion auf dessen Entscheidung vom November 2002 hat der Bundesgesetzgeber eine begrenzte Erlaubnis für derartige Verarbeitungen personenbezogener Daten in das SGB V eingefügt: Keineswegs - so zeigt sich - der Freibrief, als den die eine oder andere gesetzliche Krankenversicherung die Neuregelung verstanden wissen möchte:

Aufgrund der Eingabe der Eltern einer betroffenen Schülerin erfuhr ich, dass eine große gesetzliche Krankenversicherung durch als „Schulberater“ bezeichnete Bedienstete an sächsischen Schulen, und zwar schon seit einigen Jahren (!), „praxisorientiertes Berufsstarter- und Bewerbertraining“ durchführt. Von der Gestaltung von Bewerbungsunterlagen bis zu rhetorischen Hilfestellungen für das Vorstellungsgespräch werden die Schüler dabei von den Mitarbeitern der Krankenkasse geschult - während eigentlich Deutsch, Gemeinschaftskunde oder Geschichte auf dem Stundenplan stehen. Schließlich kommt noch ein (vermutlich bundesweit verwendeter) Fragebogen „Checkpoint Gesundheit & Beruf“ zum Einsatz, welcher - dieser Eindruck wird den Schülern gegenüber erweckt - als Entscheidungshilfe bei der Berufswahl nützlich sein soll. Hierzu werden neben dem Namen, dem Geburtsdatum und der Anschrift auch das voraussichtliche Ende der Schulzeit, der voraussichtliche Schulabschluss und die Krankenkassenmitgliedschaft erfragt. Auf dem Fragebogen befindet sich unter anderem der Hinweis, dass die Preisgabe der Daten freiwillig sei.

Grundsätzlich ist zu solchen Aktivitäten einer Krankenkasse zu sagen: Hilfe bei der Berufswahl zählt ganz eindeutig nicht zu den (gesetzlich vorgesehenen) Aufgaben einer gesetzlichen Krankenversicherung. Insbesondere auch der in § 14 SGB I ausgestaltete Beratungsanspruch umfasst nicht die Befugnis zur Erhebung personenbezogener Daten von Personen, mit welchen ein sozialversicherungsrechtliches Verhältnis eben gerade noch nicht besteht.

Im Grunde geht es der Krankenkasse aber auch gar nicht um Hilfestellungen bei der anstehenden Berufswahl, sondern nur darum, die zukünftigen Berufsanfänger für eine Mitgliedschaft in ebendieser Krankenkasse zu gewinnen.

Eine derartige Vorgehensweise bei der Mitgliederwerbung ist meiner Auffassung nach unzulässig, da es hier an der notwendigen Datenerhebungsbefugnis der Krankenkasse fehlt:

(1) Unverändert (vgl. hierzu schon 11/10.2.2) enthält die Datenerhebungs- und Speicherungsbefugnis des § 284 Abs. 1 Satz 1 Nr. 1 SGB V keine Erlaubnis, für Zwecke der Mitglieder*werbung personenbezogene Daten zu erheben.* Die Werbung von Mitgliedern fällt nämlich auch nicht unter die mit Gesetz vom 14. November 2003 vorgenommene Ergänzung des Tatbestandes der Vorschrift um die Wörter „einschließlich der für die Anbahnung eines Versicherungsverhältnis erforderlichen Daten“: Nach der eindeutigen Gesetzesbegründung (BT-Drs. 15/1525, 8. September 2003, S. 142 lSp. zu Nr. 159) soll dies lediglich den Zeitabschnitt zwischen der Beitrittsabsichtserklärung des wechselbereiten Versicherten und dessen ‚Kündigung’ seiner Mitgliedschaft gegenüber seiner bisherigen Krankenkasse betreffen.

Dem entspricht auch der Wortlaut: „Anbahnung“ eines Rechtsverhältnisses ist ein der Begründung des Rechtsverhältnisses (hier: Versicherungsverhältnis, Mitgliedschaft) naher Abschnitt der Herbeiführung eines Rechtsverhältnisses (zivilrechtlich gesprochen: Es ist schon ein vorvertragliches Schuldverhältnis entstanden - also der Anwendungsbereich der sog. c.i.c.). Zum selben Ergebnis führt außerdem auch die systematische Auslegung: Mit derselben Änderung des SGB V (durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung) hat der Gesetzgeber nämlich den § 284 SGB V um einen eigenen Absatz 4 ergänzt, der die Verarbeitung personenbezogener Daten zu Zwecken der „Gewinnung von Mitgliedern“ in näher bestimmten Grenzen erlaubt: Genau dieser § 284 Abs. 4 SGB V ist die Regelung für die Verarbeitung personenbezogener Daten durch die Krankenkassen zu Werbezwecken. Es ist gerade diese Vorschrift, die den Krankenkassen die Möglichkeit eröffnet, personenbezogene Werbung zu betreiben (so auch ganz deutlich die Gesetzesbegründung a. a. O. S. 143 lSp.).

(2) Nach dieser Befugnis zur Verarbeitung personenbezogener Daten zu Zwecken der Mitgliederwerbung in § 284 *Abs. 4* SGB V dürfen nur Daten verwendet werden, die aus *allgemein zugänglichen* Quellen entnommen werden können. Wenn die Krankenkasse wie hier an Schüler während des Schulunterrichts herantritt, ist dies ersichtlich nicht der Fall: Es handelt sich um einen seitens einer Behörde (einer anderen öffentlichen Stelle) exklusiv verschafften Zugang zu den Betroffenen, die dann persönlich ihre Daten preisgeben.

(3) Diese Regelung des § 284 Abs. 4 SGB V ist, was die Erlaubnis für Krankenkassen betrifft, personenbezogene Daten zu Werbezwecken zu verarbeiten, abschließend: Trotz des Umstandes, dass die Krankenkassen infolge der Einführung des Kassenwahlrechtes (§ 173 SGB V) verstärkt im Wettbewerb um Mitglieder stehen, hat der Gesetzgeber sich im Hinblick auf die genannte Entscheidung des BSG, wonach Mitgliederwerbung nicht zu den Aufgaben der gesetzlichen Krankenversicherung gehört, für welche die Krankenkassen personenbezogene Daten erheben dürfen, dennoch klar dafür entschieden, zur Gewinnung neuer Mitglieder lediglich die Verwendung von Daten zuzulassen, die aus allgemein zugänglichen Quellen entnommen werden können (vgl. auch dazu die ausführliche Gesetzesbegründung a. a. O. S. 143 lSp.). Die Vorschrift erlaubt ganz bestimmte Aktivitäten dieser Art („wird … zugelassen“, Gesetzesbegründung a. a. O.) - mehr nicht. Es handelt sich um eine durch die begrenzte Eingriffsbefugnis zugleich zum Ausdruck gebrachte (ebenso begrenzte) Aufgabenzuweisung.

Aus diesem Grund lässt sich entgegen der von der Krankenkasse vertretenen Auffassung die von ihr vorgenommene Datenerhebung auch nicht, und zwar auch nicht teilweise, darauf stützen, dass sie freiwillig, also mit Einwilligung des Betroffenen erfolgt sei.

Die Erhebung personenbezogener Daten zum Zwecke der Mitgliedergewinnung ist schon deswegen nicht aufgrund bloßer Einwilligung zulässig (anders wohl die genannte Gesetzesbegründung a. a. O.), weil § 67 a Abs. 1 Satz 1 SGB X dies für die Datenerhebung im Unterschied zur (weiteren) Verarbeitung von Sozialdaten und deren Nutzung gemäß § 67 b Abs. 1 Satz 1 SGB X gar nicht als Erlaubnistatbestand vorsieht, wie auch das Bundessozialgericht in der genannten Entscheidung hervorgehoben hat (im Einzelnen 11/10.2.2, S. 113, drittletzter Absatz).

Hinzu kommt ein vom Wortlaut der genannten Vorschriften des SGB X unabhängiger Gesichtspunkt: Kraft des verfassungsrechtlichen Grundsatzes des *Vorbehaltes des Gesetzes* dürfen Träger öffentlicher Gewalt nicht flächendeckend, in großem Stil Aufgaben oder vermeintliche Aufgaben mit Hilfe einer lediglich durch Einwilligung der Betroffenen gerechtfertigten Verarbeitung personenbezogener Daten erledigen. Anders

ausgedrückt: Die Träger öffentlicher Gewalt - und zu diesen gehören die gesetzlichen Krankenkassen als Körperschaften des öffentlichen Rechtes nun einmal immer noch - 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.

(Diesen Gesichtspunkt haben die Datenschutzbeauftragten des Bundes und der Länder zum Beispiel auch im Hinblick auf die vom Bundessozialgericht am 23. Juli 2002 entschiedene Frage [näher dazu 11/10.2.1] geltend gemacht, inwieweit Krankenkassen berechtigt sind, Einsicht in Behandlungsunterlagen von Krankenhäusern oder Ärzten zu nehmen. Das Einholen einer Einwilligung in die Übersendung den Krankenkassen nicht zustehender Unterlagen wäre als eine Umgehung der vom Gesetzgeber getroffenen Regelung anzusehen, nämlich als Überschreitung der in dieser begrenzten Befugniszuweisung zugleich für das Handeln der Krankenkasse gesetzten Grenze. Diese Rechtsauffassung muss auch für die Fälle der Mitgliederwerbung auf Einwilligungsgrundlage gelten.)

(4) Überdies hat in vielen Fällen gar keine für sich genommen ausreichende Einwilligung vorgelegen. Denn die Krankenkasse hat bei minderjährigen Schülern nicht zusätzlich die Einwilligung der Eltern (Sorgeberechtigten) eingeholt. Sie hat das damit zu rechtfertigen versucht, dass nach Vollendung des 15. Lebensjahres die Einwilligung des betroffenen Minderjährigen ausreiche.

Dies trifft nicht zu: Die Grundrechtsmündigkeit beseitigt den Minderjährigenschutz nicht. Dementsprechend ist nach der Rechtsprechung des Bundesgerichtshofes (Urt. v. 16. November 1971 - VI ZR 76/70, NJW 1972, 335, 337 rSp. und Urt. v. 2. Juli 1974 - VI ZR 121/73, NJW 1974, 1947, 1950; zustimmend Jauernig-Teichmann Rdnr. 54 zu § 823 BGB) davon auszugehen, dass ab Vollendung des 14. Lebensjahres bei einem Eingriff in Rechte bzw. Rechtsgüter wie das Persönlichkeitsrecht Minderjähriger die Einwilligung der Erziehungsberechtigten nicht ausreicht, sondern *daneben* auch diejenige des Betroffenen selbst erforderlich ist. Aber es müssen eben *beide* Einwilligungen vorliegen, auch die der Sorgeberechtigten.

Das in Abweichung vom Bürgerlichen Recht nach § 36 SGB I nichtgeschäftsfähigen Personen mit Vollendung des 15. Lebensjahres eingeräumte Recht, Sozialleistungen zu beantragen, wirkt sich auf die Voraussetzungen einer rechtswirksamen Einwilligung in den Eingriff in absolute Rechte nicht aus.

Schließlich war die Einwilligungserklärung als Kleingedrucktes im Gesamtvordruck recht versteckt angebracht worden. Wenn man § 67 b Abs. 2 Satz 4 SGB X nicht heranziehen will, war das ein Verstoß gegen § 4 Abs. 4 Satz 2 SächsDSG, also das Gebot, die Erklärung der Einwilligung in die Verarbeitung personenbezogener Daten im äußeren Erscheinungsbild der Erklärung hervorzuheben, wenn diese zusammen mit anderen Erklärungen schriftlich erteilt wird.

Das SMK teilt erfreulicherweise meine Rechtsauffassung. Es gilt, dafür zu sorgen, dass dies an den Schulen auch so umgesetzt wird. Zu meinen Aufgaben dabei gehört es selbstverständlich, dazu beizutragen, dass alle gesetzlichen Krankenversicherungen - da sich diese natürlich, wie ich verstehe, den Zwängen einer Konkurrenzsituation ausgesetzt sehen - *gleich* behandelt werden.

10.2.7 Unbefugte Weitergabe medizinischer Daten aus Strukturierten Behandlungsprogrammen: Verfahren der Auftragsdatenverarbeitung

Zu den Neuerungen in der gesetzlichen Krankenversicherung gehört die Einführung sog. *Strukturierter Behandlungsprogramme* für chronische Krankheiten (§§ 137 f, 137 g SGB V) mit starker Steuerung durch die Krankenkassen und Vergütung der zusätzlichen Leistungen (namentlich auch Dokumentationsleistungen!) der Ärzte. Es ist den Versicherten freigestellt, sich in ein solches Programm einzuschreiben und insbesondere auch in die dabei stattfindende Verarbeitung ihrer medizinischen Daten einzuwilligen (§ 137 f Abs. 3 SGB V; vgl. oben Abschnitt 10.2.1). Damit sich für eine ein solches Behandlungsprogramm betreibende Krankenkasse kein Kostennachteil gegenüber anderen gesetzlichen Krankenversicherungen ergibt, ist die genaue Anzahl der Versicherten, die an einem Strukturierten Behandlungsprogramm („Chronikerprogramm“) teilnehmen, im sog. Risikostrukturausgleich als vorteilhaft zu berücksichtigen (vgl. §§ 267 Abs. 2 Satz 4, 266 Abs. 4 Satz 2, 137 f Abs. 3 SGB V). Das bedeutet: Es ist finanziell für die Krankenkasse wichtig, dass ihr jeder Versicherte, der am Strukturierten Behandlungsprogramm teilnimmt, auch bekannt ist und beim Risikostrukturausgleich mitgezählt werden kann.

Zu der für eine als ordnungsgemäß anzuerkennende Teilnahme an einem Strukturierten Behandlungsprogramm vorgeschriebenen umfangreichen Verarbeitung von Behandlungsdaten (§ 266 Abs. 7 Satz 1 Nr. 3 SGB V, § 28 Abs. 1 Nr. 1 Risikostrukturausgleichsverordnung [RSAV]) gehört vor allem auch eine Übermittlung an die Krankenkassen (§ 28 Abs. 2 und 3 RSAV), wofür in Sachsen, wie wohl auch in der Regel in den anderen Bundesländern, gemäß § 28 Abs. 2 Satz 1 Nr. 1 RSAV auf Empfängerseite eine *Arbeitsgemeinschaft* der gesetzlichen Krankenkassen *im Sinne von § 219 SGB V* gebildet worden ist. Diese Arbeitsgemeinschaft hat die Aufgabe, die von den beteiligten

Ärzten erhobenen Daten zu pseudonymisieren (§ 28 f Abs. 2 Satz 1 Nr. 1 RSAV), sie pseudonymisiert an die Kassenärztliche Vereinigung bzw. eine von Mitgliedern der Arbeitsgemeinschaft gebildete gemeinsame Einrichtung zu übermitteln (Nr. 4) und sie in bestimmten Fällen zu depseudonymisieren (Nr. 5).

In Sachsen, das mit der sog. Diabetesvereinbarung (mit der ich seinerzeit intensiv beschäftigt gewesen bin) schon einen Vorläufer der Strukturierten Behandlungsprogramme (auch „Desease Management Programme“ genannt) gehabt hat, haben sich, soweit bekannt, schon rund 300.000 Zuckerkranke in das entsprechende Programm eingeschrieben. Zusammen mit sieben weiteren Bundesländern hat die in Sachsen gebildete Arbeitsgemeinschaft die gesamte Verarbeitung der personenbezogenen Daten einem Privatunternehmen (als sogenannter Datenstelle) übertragen. Das ist aus Kostengründen geschehen, aber im Hinblick auf das Gebot des § 80 Abs. 5 Satz 2 SGB X, wonach der überwiegende Teil der Speicherung des gesamten Datenbestandes beim Auftraggeber verbleiben muss, problematisch (ist nicht die *Arbeitsgemeinschaft* selbst der Auftraggeber?). Die Datenschutzbeauftragten haben sich mit ihren darauf gestützten Bedenken jedoch nicht durchsetzen können. Prompt - so ist man versucht zu sagen - ist es insoweit zu einem erheblichen Datenschutzverstoß gekommen: Das von der genannten Ländergruppe (nach EU-weiter Ausschreibung beauftragte, hauptsächlich in Bayern tätige Unternehmen hat die von ihm zu bearbeitenden Daten, nämlich Dateien mit Abbildungen handschriftlich ausgefüllter ärztlicher Dokumentationsbögen sowie Dateien mit digital eingelesenen ärztlichen Dokumentationsbögen, vertragswidrig an eine vietnamesische Tochtergesellschaft übermittelt, wobei hinsichtlich des Zweckes und des genauen Personenbezuges nicht alles im einzelnen hat aufgeklärt werden können. Herausgekommen ist das nur, weil ein ausgeschiedener Mitarbeiter des Unternehmens Aufsichtsbehörden unterrichtet hat.

Der Vorgang ist unter Beteiligung des Hessischen Datenschutzbeauftragten intensiv geprüft worden. Da es an den gebotenen Protokollierungen zum Teil gefehlt hat, haben sich die Vorgänge nur sehr beschränkt aufklären lassen.

Letztlich haben sich auch die Datenschutzbeauftragten damit abfinden müssen, dass die Krankenkassen sich gezwungen gesehen haben, mit den bisherigen Auftragnehmer weiter, wenn auch nunmehr mit dichtesten Kontrollen seitens der Auftraggeber, zusammenzuarbeiten. Denn die anderen in Frage kommenden Anbieter haben sich, so ist erklärt worden, ebenfalls schon als überfordert herausgestellt. Außerdem scheuen die Krankenkassen Neuverhandlungen über die Vergabe solcher Leistungen, da die Auftragnehmer erheblich höhere Preise als bisher verlangen müssten, weil sich die Arbeiten an den Dokumentationsbögen als viel aufwändiger herausgestellt haben, als ursprünglich erwartet worden ist.

Weil also schnelle Ausweichlösungen nicht zur Verfügung gestanden haben, da man weder schnell ein eigenes Rechenzentrum hätte aufbauen noch auf dem freien Markt auf Anhieb Kapazitäten hätte finden können, die die Aufgabe aus dem Stand heraus hätten bearbeiten können, ist nichts anderes übrig geblieben, als mit dem bisherigen Auftragnehmer, nur jetzt mit intensiveren Kontrollen, weiterzumachen.

Es ist daher nicht zu einer Kündigung des Werkvertrages, aber immerhin zu einer Beendigung von Unterauftragnehmerverhältnissen, personellem Wechsel in der Leitungsebene, zu Abmahnungen, zu neuen Organisationsstrukturen und zur Veranlassung staatsanwaltschaftlicher Ermittlungen gekommen.

Fazit: Die immer weiter gestiegene Komplexität der gesetzlichen Regelungen der gesetzlichen Krankenversicherung, die sich insbesondere in der immer aufwendigeren vorgeschriebenen Verarbeitung personenbezogener Daten auswirkt, hat an die Grenzen der Leistungsfähigkeit in verwaltungstechnischer und datenverarbeitungstechnischer Hinsicht geführt, so dass Sanktionierungen von Fehlverhalten nur noch sehr eingeschränkt möglich sind. Dazu ist der Auftraggeber viel zu sehr vom Auftragnehmer abhängig! Keine günstigen Bedingungen für den Datenschutz.

10.2.8 Einsichtnahme des Sächsischen Rechnungshofes in Prüfberichte des Sächsischen Landesprüfungsamtes für Sozialversicherung

Gemäß § 87 SGB IV unterliegen die Träger der Sozialversicherung staatlicher Rechtsaufsicht, die Unfallverhütung durch die gesetzliche Unfallversicherung, insbesondere die Berufsgenossenschaften, unterliegt auch staatlicher Fachaufsicht. Länderzuständigkeit besteht insoweit gemäß § 90 Abs. 2 SGB IV für die Aufsicht über diejenigen Sozialversicherungsträger, deren Zuständigkeitsbereich sich nicht über das Gebiet eines Landes hinaus erstreckt, also die sogenannten landesunmittelbaren Versicherungsträger (mit Erweiterung in Absatz 3 für Sozialversicherungsträger, deren Zuständigkeitsbereich sich über das Gebiet von nicht mehr als drei Ländern hinaus erstreckt). Landesrecht bestimmt, wer die für die Sozialversicherung zuständige oberste Verwaltungsbehörde ist. Gemäß § 4 Abs. 1 SächsAGSGB ist dies das Sächsische Staatsministerium für Soziales [Gesundheit, Jugend, Familie]. Als für die Sozialversicherung zuständige oberste Verwaltungsbehörde des Landes hat dieses Staatsministerium gemäß § 274 SGB V außerdem die Geschäfts-, Rechnungs- und Betriebsführung der ihrer Aufsicht unterstehenden Krankenkassen - das sind in Sachsen die AOK Sachsen und die IKK Sachsen - zu prüfen. Gemäß § 274 Abs. 1 Satz 4 und 5 SGB V ist der gesamte Geschäftsbetrieb auf seine Gesetzmäßigkeit und Wirtschaftlichkeit hin zu prüfen und haben die zu prüfenden Stellen, zu denen neben den Krankenversicherungen auch Verbände der Krankenkassen und die jeweilige kassenärztliche Vereinigung gehören,

auf Verlangen alle Unterlagen vorzulegen und alle Auskünfte zu erteilen, die zur Durchführung der Prüfung erforderlich sind.

Zuständig in Sachsen ist dafür gemäß § 5 Abs. 1 SächsAGSGB das im SMS eingerichtete *Landesprüfungsamt für Sozialversicherung*.

Der SRH wiederum ist gemäß § 88 Abs. 1 Satz 1 SäHO befugt, *die gesamte Haushalts- und Wirtschaftsführung* auch des *Landesprüfungsamtes für Sozialversicherung* zu prüfen. Gemäß § 90 SäHO erstreckt sich diese Prüfung insbesondere darauf, ob die geprüfte Stelle wirtschaftlich und sparsam verfährt, ob sie ihre Aufgabe mit weniger Aufwand oder effektiver erfüllen kann, ob die Haushaltsvorschriften eingehalten worden sind und das Rechnungswesen ordnungsgemäß ist.

Das wirft auch datenschutzrechtliche Fragen auf, konkret nämlich die, inwieweit das Landesprüfungsamt dem SRH Einsicht in seine unter anderem auch personenbezogene Daten von Versicherten bzw. Patienten enthaltenden Prüfberichte gewähren darf:

1. Aus Gründen einer effektiven Finanzkontrolle umfasst das Prüfungsrecht der Rechnungshöfe grundsätzlich auch die Vorlage von Unterlagen mit personenbezogenen Daten. Das Sozialgeheimnis steht den Prüf- und Erhebungsrechten des SRH nicht grundsätzlich entgegen. Gleiches gilt für das Steuergeheimnis (Nebel in: Piduch, Bundeshaushaltsrecht 2. Auflage § 95 Rdnr. 2) wie auch für die ärztliche Schweigepflicht bei öffentlichen Krankenanstalten (BVerwG, Urt. v. 11. Mai 1989, NJW 1989, 2961, 2962; BVerfG, Beschluss vom 29. April 1996, NJW 1997, 1633, 1634).

2. Die dafür wegen §§ 67 b Abs. 1 Satz 1, 67 d Abs. 1 SGB X i. V. m. § 35 Abs. 1 Satz 4, letzter Fall, SGB I i. V. m. § 67 c Abs. 3 SGB X erforderliche gesetzliche Übermittlungserlaubnis ist § 69 Abs. 5 SGB X zu entnehmen. Danach ist *die Übermittlung von Sozialdaten zulässig für die Erfüllung der gesetzlichen Aufgaben der Rechnungshöfe (und der anderen Stellen, auf die § 67 c Abs. 3 Satz 1 SGB X Anwendung findet).* Die Vorschrift vermeidet eine Einengung auf das „Erforderliche“. Damit wird zum einen dem Umstand Rechnung getragen, dass das Prüfungsrecht des SRH grundsätzlich nicht bereits durch die Prüfungsbefugnisse oder allgemeine Aufsichtsbefugnisse anderer Rechtsträger eingeschränkt oder ausgeschlossen ist. Die Prüfung durch den SRH ist vielmehr als eigenständiges Kontrollinstrument neben der Aufsicht durch die Exekutive konzipiert, der SRH wird insoweit als unabhängiges, auf Verfassungsauftrag beruhendes Organ staatlicher Finanzkontrolle aus eigenem Recht tätig (Urteil des BayVGH vom 16. Februar 1995, Az.: 9 B 94.778 - juris). Die Aufsicht und die Rechnungsprüfung betreffend die gesetzlichen Krankenkassen, die, wie schon erläutert, nach § 274 SGB V i. V. m. § 5 Abs. 1 und 2 SächsAGSGB dem

Landesprüfungsamt übertragen ist, stellt für sich allein insoweit keine Spezialvorschrift dar, die das Prüfungsrecht des SRH verdrängen könnte (vgl. BayVGH a. a. O.). Zum anderen scheint das Abstellen auf die bloße *Dienlichkeit* für die Aufgabenerfüllung - statt der strengen Erforderlichkeit - dem Rechnungshof in Übereinstimmung mit bisher ergangenen Gerichtsentscheidungen die Beurteilung überlassen zu sollen, welche Unterlagen bzw. Daten er für seine Kontrolltätigkeit konkret benötigt.

3. Die gesetzliche Aufgabe des SRH hinsichtlich der Prüfung der Haushalts- und Wirtschaftsführung des Landesprüfungsamtes ist allerdings durch § 112 Abs. 1 Satz 1 Nr. 2 SäHO dahingehend begrenzt, dass eine Prüfung der Haushalts- und Wirtschaftsführung der landesunmittelbaren Träger der gesetzlichen Krankenversicherung ausgeschlossen ist.

   Daraus folgt: Die Prüfung der Haushalts- und Wirtschaftsführung des Landesprüfungsamtes durch den SRH darf nicht so weit gehen, dass sie sich als Prüfung der Haushalts- und Wirtschaftsführung der gesetzlichen Krankenkassen auswirkt, die vom Landesprüfungsamt geprüft werden. Die Kontrolle des SRH umfasst, wie dargelegt, nicht die vollständige Rechts- und Zweckmäßigkeit des Handelns der seiner Kontrollzuständigkeit unterliegenden Behörde, also nicht die sachliche Richtigkeit von deren Aufgabenerledigung.

   Aufgrund dessen ist schwer nachvollziehbar, für welche Zwecke der SRH Einblick in die Prüfberichte benötigen könnte. Jedenfalls aber kann ausgeschlossen werden, dass ihm dabei auch zweckmäßigerweise Kenntnisse von Einzelvorgängen aus den geprüften Krankenkassen zu Gebote stehen sollten, damit er seine Aufgaben erfüllen kann.

4. Ergebnis ist daher: Das Landesprüfungsamt ist nicht befugt, dem SRH Sozialdaten zu übermitteln.

   Soweit der SRH Anspruch auf Einblick in Prüfberichte des Landesprüfungsamtes haben sollte, müssten Passagen, die in personenbezogener Weise Einzelfälle betreffen, ausgenommen werden (Einblick nur in teilgeschwärzte Ablichtungen).

   Sozialversicherungsträger als solche haben, dies sei vorsorglich angemerkt, kein Recht auf informationelle Selbstbestimmung (allenfalls Betriebsgeheimnisse). Daten, die sich auf sie als solche beziehen, sind keine Sozialdaten im Sinne von §§ 67 ff. SGB X (vgl. § 67 Abs. 1 Satz 1 SGB X).

10.2.9 Übermittlung von Angaben zum Mietvertrag eines Wohngeldempfängers auf Ersuchen der Sozialhilfebehörde im Hinblick auf einen Antragsteller, der mit dem familienangehörigen Wohngeldempfänger in einer Haushaltsgemeinschaft lebt

Die Sozialhilfebehörde einer Großstadt wollte von der Wohngeldbehörde (derselben Großstadt) wissen, wie hoch der von einer bestimmten Wohngeldempfängerin nach dem Mietvertrag zu zahlende Mietzins sei, weil sich die volljährige Tochter der Wohngeldempfängerin, die mit ihrer Mutter einen gemeinsamen Haushalt führte und daher in einer „Wohn- und Wirtschaftsgemeinschaft“ nach § 4 Abs. 2 WoGG lebte, nach Stellung eines Antrages auf Sozialhilfe geweigert hatte, der Sozialhilfebehörde den Mietvertrag der Mutter vorzulegen.

Die Wohngeldbehörde hat mir erläutert, dass für den Anspruch auf Wohngeld das Einkommen beider als Familienmitglieder in Haushaltsgemeinschaft (vgl. § 4 Abs. 2 Satz 1 WoGG) lebenden Personen zu berücksichtigen und dass für die Berechnung der Sozialhilfe für einen Angehörigen der Wohn- und Wirtschaftsgemeinschaft die Miet-Belastung pro rata, das heißt nach Köpfen verteilt, zu Grunde zu legen ist, so dass die Sozialhilfebehörde in der Tat zur Berechnung des Sozialhilfeanspruches der Tochter wissen muss, wie hoch die für diese sozialhilferechtlich anzusetzende Mietbelastung ist (unabhängig vom genauen zivilrechtlichen Innenverhältnis zwischen der Mutter als Hauptmieterin und der Tochter).

Zu recht ist die Behörde bei ihrer Anfrage davon ausgegangen, dass die Wohngeldbehörde gemäß § 67 d Abs. 2 SGB X die Hauptverantwortung für die Zulässigkeit der Übermittlung tragen würde. Auch mit ihrer Überlegung, dass maßgebliche Übermittlungserlaubnis nur § 69 Abs. 1 Nr. 1, 3. Fall SGB X sein könnte, also die Übermittlung für die Zwecke der Erfüllung einer gesetzlichen Aufgabe des datenempfangenden Sozialleistungsträgers, hat die Behörde meiner Auffassung nach recht gehabt. Für die Anwendung dieser Vorschrift spielt es nach dem Gesetzeswortlaut keine Rolle, wenn wie im vorliegenden Falle um Übermittlung von Daten für ein Verwaltungsverfahren ersucht wird, in dem Antragsteller eine andere Person ist als in demjenigen Verfahren, innerhalb dessen die ersuchte Behörde das betreffende Datum (Mietzinsverpflichtung) gespeichert hat. Abgesehen davon ist das Datum der Mietzinsverpflichtung der Mutter mittelbar (latent) auch ein Datum der Tochter, und zwar sowohl im Wohngeldverfahren - weil die Tochter mittelbar (quasi) auch Empfängerin von Wohngeld ist, insofern ihre Einkünfte und die Tatsache, dass sie als Familienangehörige Mitnutzerin der Wohnung ist, bei der Berechnung des Wohngeldanspruches zu berücksichtigen sind - als auch im Sozialhilfeverfahren, weil dort, wie oben angegeben, diese im Außenverhältnis zum Vermieter nur die Hauptmieterin (Mutter) betreffende

Angabe sozialhilferechtlich auch ein auf die Tochter bezogenes Datum ist, weil sich die Höhe der Mietzinsverpflichtung auf deren Sozialhilfeanspruch auswirkt.

§ 69 Abs. 1 Nr. 1 SGB X setzt, sinnvollerweise, nicht voraus, dass der Betroffene bei der um Übermittlung ersuchten und bei der ersuchenden Stelle in derselben Weise am jeweiligen Verwaltungsverfahren beteiligt, also in beiden Fällen Antragsteller ist.

Außerhalb der Verantwortung der um Übermittlung ersuchten Stelle liegt die - gleichwohl aber bei Betrachtung des Gesamtvorganges zu prüfende - Frage, ob die Sozialhilfebehörde befugt ist, abweichend von § 67 a Abs. 2 Satz 1 SGB X das betreffende Sozialdatum statt bei der Betroffenen (in erster Linie in diesem Verfahren also der Tochter) bei einer dritten Stelle, also ohne Mitwirkung des Betroffenen zu erheben. Einschlägige Erlaubnisvorschrift ist § 67 Abs. 2 Satz 2 Nr. 1 SGB X. Voraussetzungen sind neben der bereits geklärten Übermittlungsbefugnis der Wohngeldstelle der unverhältnismäßige Aufwand einer Erhebung beim Betroffenen (Buchst. b) und das Fehlen von Anhaltspunkten dafür, dass durch die Übermittlung überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt würden. Der hier vorliegende Fall der Weigerung der Antragstellerin, in diesem Punkt ihre Angaben vollständig zu machen (und erst recht zu belegen), wird in den Kommentierungen zu § 67 a Abs. 2 Satz 2 Nr. 1 Buchst. a (und Buchst. b) SGB X üblicherweise nicht erwähnt, im Unterschied zu dem Fall, dass Angaben des Betroffen wegen Anhaltspunkten für Ihre Unrichtigkeit überprüft oder die unbeabsichtigte Lückenhaftigkeit oder Ungenauigkeit der Angaben behoben werden sollen (vgl. Hauck/Haines Rdnr. 82, von Wulffen Rdnr. 8 und 10 sowie Kassler Kommentar - Scholz Rdnr. 28-32, jeweils zu § 67 a SGB X). Das liegt vermutlich daran, dass im Falle dieser Weigerung gemäß § 66 SGB I der Sozialleistungsträger dem Antragsteller, der seine Mitwirkungspflicht gemäß § 60 Abs. 1 innerhalb der durch § 65 SGB I gesteckten Grenzen nicht erfüllt, schlicht die Leistung verweigern kann. Die Frage, warum die Sozialhilfebehörde in diesem Fall nicht diesen Weg hat gehen, sondern stattdessen Angaben zur Höhe der Mietzinsverpflichtungen der Mutter hat besorgen wollen, hat die Wohngeldstelle als um Übermittlung ersuchte Stelle nicht zu kümmern brauchen. Zwar ist der hier in der Weigerung zum Ausdruck gekommene Wille der Betroffenen bei der Frage, ob überwiegende schutzwürdige Interessen ihrer Person nicht beeinträchtigt werden, zu berücksichtigen (von Wulffen Rdnr. 8 zu § 67 a SGB X); es sind jedoch keine Anhaltspunkte dafür zu erkennen gewesen, dass tatsächlich schützwürdige überwiegende Interessen der betroffenen Tochter durch die Einholung der Angaben über die Mietzinsverpflichtung der Mutter beeinträchtigt sein könnten. Nichtsdestoweniger hat sich die Frage gestellt, warum die Sozialhilfebehörde nicht schlicht die Leistung versagt hat.

Im Hinblick auf immer wieder anzutreffende dahingehende Vorstellungen vieler Behörden: Ein Sozialleistungsträger, dem ein Antragsteller für die Entscheidung über seinen Antrag notwendige Daten zur Verfügung gestellt hat - wie hier im Falle die Mutter der Wohngeldbehörde ihren Mietvertrag vorgelegt hat -, verarbeitet die betreffenden Daten nicht aufgrund einer Einwilligung des Antragstellers (im Sinne von § 67 b Abs. 2 SGB X), sondern der Antragsteller hat diese Daten gemäß § 67 a Abs. 3 Satz 3 SGB X freiwillig zur Erfüllung der Mitwirkungslast (nach § 65 Abs. 1 SGB I „Mitwirkungspflichten“) zur Verfügung gestellt. Eine Übermittlung an einen anderen Sozialleistungsträger gemäß § 69 Abs. 1 Nr. 1 SGB X (oder auch auf anderer gesetzlicher Grundlage) ist also nicht davon abhängig, ob eine Einwilligung gerade auch in die Übermittlung an andere Sozialleistungsträger vorliegt.

10.2.10 Erstattung von Strafanzeigen durch die Sozialhilfebehörde; Begriff des „Sozialdatums“

Eine Sozialhilfeempfängerin hatte in einem Brief an das Sozialamt einer sächsischen Großstadt u. a. mitgeteilt, dass ihr Lebenspartner Waffen besitze und auch Betrügereien über das Internet begehe.

Dem städtischen Datenschutzbeauftragten, der sich daraufhin im Hinblick auf die Frage, ob das Sozialamt Polizei oder Staatsanwaltschaft informieren dürfte bzw. musste, an mich gewandt hat, habe ich geantwortet, dass zunächst zu prüfen sei, inwieweit die - vorrangigen - Spezialvorschriften des Sozialgesetzbuches maßgeblich seien. Denn gemäß §§ 67 d Abs. 1, 67 b Abs. 1 Satz 1 SGB X dürfen *Sozialdaten* außer im Fall der Einwilligung des Betroffenen nur übermittelt werden, wenn dies durch die §§ 68 ff. SGB X oder eine andere Vorschrift des Sozialgesetzbuches erlaubt ist. Mit anderen Worten: Die Befugnis zur Weitergabe von *Sozialdaten* richtet sich ausschließlich nach Sozialgesetzbuch. (Dabei erkennt das Sozialgesetzbuch in § 71 SGB X die dort abschließend genannten, nach anderen Gesetzen bestehenden Übermittlungs*pflichten* ausdrücklich und in dem Sinne an, dass es entsprechende Übermittlungserlaubnisse ausspricht. Bei den sonstigen Übermittlungsvorschriften der §§ 67 d ff. SGB X spricht das Gesetz lediglich von Übermittlungs*befugnissen*.)

Voraussetzung für die Anwendbarkeit des SGB war dabei zunächst, dass es sich bei den von der Sozialhilfeempfängerin in ihrem Brief gemachten Angaben überhaupt um Sozialdaten handelte, also Daten, für die das Sozialgeheimnis, mithin die besonderen Datenschutzregelungen des Sozialgesetzbuches, insbesondere §§ 67 ff. SGB X, gelten: Der Begriff des Sozialdatums wird in § 67 Abs. 1 SGB X bestimmt als Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, die von einem Sozialleistungsträger im Hinblick auf seine Aufgaben nach dem

Sozialgesetzbuch erhoben, verarbeitet oder genutzt wird. Das sog. Sozialgeheimnis, also die besonderen Datenschutzvorschriften des Sozialgesetzbuches, erfasst danach nur solche Informationen (Daten), die der Sozialleistungsträger mit dem nötigen "fachlichen Bezug" (Hauck/Haines Rdnr. 23 zu § 67 SGB X), d. h. "nicht nur im Zusammenhang" mit seiner Aufgabenwahrnehmung (Kasseler Komm. - Scholz Rdnr. 24 zu § 67 SGB X), sondern zwecks Erfüllung von Aufgaben verarbeitet (sc. im weiteren Sinne), die sich unmittelbar aus dem Sozialgesetzbuch (als vorgeschrieben oder zugelassen, vgl. § 30 Abs. 1 SGB IV) ergeben (Kasseler Komm. a. a. O., Hauck/Haines a. a. O.).

Soweit die von der Sozialhilfeempfängerin gemachten Angaben danach keinen fachlichen Bezug zur Entscheidung der Behörde über die Gewährung oder Rückforderung von Sozialhilfeleistungen gehabt haben, hat sich die Erlaubtheit der Übermittlung von Daten an Polizei oder Staatsanwaltschaft nach allgemeinem Datenschutzrecht, d. h. nach Sächsischen Datenschutzgesetz, bestimmt. Die zweckändernde Übermittlung an die Staatsanwaltschaft bzw. Polizei wäre nach § 13 Abs. 2 Nr. 3 SächsDSG (insoweit unverändert gegenüber § 12 Abs. 2 Nr. 3 SächsDSG a. F.) zulässig gewesen.

Wenn sich die betrügerische Verschaffung von Einnahmen durch den Lebenspartner der Briefabsenderin möglicherweise auf die Gewährung von Sozialhilfe an diese oder auch an den Lebenspartner ausgewirkt hat - was ich angenommen habe -, dann hat es sich bei den näheren Angaben zu dieser 'selbständigen' und zu Einnahmen führenden Tätigkeit, soweit diese bei der Sozialhilfebehörde gespeichert und genutzt werden, um Sozialdaten im Rechtssinne gehandelt. Der Waffenbesitz hat nach Sozialrecht vom Antragsteller bzw. Leistungsempfänger anzugebende Vermögenswerte betreffen können. Damit ist eine Übermittlungsbefugnis nach § 69 Abs. 1 Nr. 2 i. V. m. Nr. 1 SGB X in Betracht gekommen: *Die Übermittlung von Sozialdaten ist danach zulässig, soweit sie erforderlich ist für die Durchführung eines mit der Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem Sozialgesetzbuch zusammenhängenden gerichtlichen Verfahrens, einschließlich eines Strafverfahrens,* wobei unter letzteres auch schon das staatsanwaltschaftliche Ermittlungsverfahren fällt (str., Nachweise bei Scholz a. a. O. § 69 Rdnr. 8; überzeugend jedoch die positive Auffassung des LG Stuttgart, Beschluss vom 11. Mai 1993, NStZ 1993, 552 ff.; es läuft für das praktische Ergebnis auf dasselbe hinaus, wenn eine Übermittlung an die Staatsanwaltschaft oder die Polizei als stattdessen grundsätzlich nach § 69 Abs. 1 Nr. 1 SGB X zulässig angesehen wird, wie von Scholz a. a. O. Rdnr. 6 und von Hauck/Haines Rdnr. 23, jeweils zu § 69 SGB X).

Im Hinblick auf die Voraussetzung des *Zusammenhanges* des gerichtlichen Verfahrens mit der Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch reicht auch hier jede Aufgabe aus, die im Sinne von § 30 Abs. 1 SGB IV gesetzlich vorgeschrieben oder zugelassen ist (v. Wulffen/Roos § 69 Rdnr. 13). Sie muss nicht ausdrücklich im

Gesetz als "Aufgabe" benannt sein. Zu den gesetzlichen Aufgaben eines Sozialhilfeträgers zählt vielmehr auch eine Strafanzeige, soweit diese Maßnahme zur Wahrung der Einhaltung der für die Sozialleistungen geltenden Vorschriften, insbesondere zum Schutz gegen Missbrauch von Sozialleistungen (v. Wulffen/Roos a. a. O. Rdnr. 26) und insoweit zur Verhütung weiterer Schädigungen der Solidargemeinschaft erforderlich ist. Denn zu den Aufgaben der Sozialleistungsträger gehört es ja vor allem auch zu überprüfen, ob die Voraussetzungen für die Leistungsgewährung vorliegen oder ob Zahlungen zu Unrecht erfolgt sind oder gegebenenfalls erfolgten (vgl. v. Wulffen/Roos Rdnr. 13 zu § 69 SGB X). Es geht also um Straftaten zu Lasten der in § 35 SGB I genannten Stellen (Hauck/Haines Rdnr. 23 zu § 69 SGB X).

Als Straftat zu Lasten des Sozialhilfeträgers ist ausschließlich in Betracht gekommen, dass die Sozialhilfeempfängerin sich möglicherweise dadurch unberechtigt Sozialhilfeleistungen verschafft hatte, dass sie die - wenn auch illegalen - Einkünfte ihres Lebenspartners aus ‚selbstständiger', wenn auch möglicherweise betrügerischer ‚Tätigkeit' bis zu ihrem Brief verschwiegen hatte.

Für die Übermittlung von Sozialdaten im Interesse der Verfolgung von Straftaten, die demgegenüber nicht zum Nachteil eines Sozialleistungsträgers, sondern zum Nachteil Dritter verübt werden, ist § 73 SGB X die maßgebliche Vorschrift. Die Voraussetzungen des Absatzes 1 dürften dabei durch die (angeblichen) Betrügereien und den (angeblichen) Waffenbesitz nicht erfüllt gewesen sein. Absatz 2 der Vorschrift hat von der Rechtsfolge her die in Frage stehende Übermittlung nicht erlaubt. Überdies wäre die Übermittlung gemäß Absatz 3 der Vorschrift nur aufgrund einer Entscheidung des zuständigen Ermittlungsrichters (§ 162 StPO) zulässig gewesen.

Zusammenfassend war festzuhalten:
Soweit die Daten für Entscheidungen über die Gewährung oder Rückforderung von Sozialhilfe benötigt wurden, durften sie für eine Strafanzeige gegen die Briefschreiberin übermittelt werden. Andernfalls fehlte es zwar an der nötigen Befugnis zur Speicherung (§ 67 d SGB X), eine Übermittlung an die Strafverfolgungsbehörde zwecks Strafanzeige war jedoch zulässig.

10.2.11 Übersendung von Sozialhilfeakten im Rahmen der Kostenerstattung zwischen Trägern der Sozialhilfe

In bestimmten Fällen, die nunmehr in §§ 106 ff. SGB XII durch Vorschriften geregelt sind, die zum 1. Januar 2005 die bis dahin gültig gewesene Regelung im Bundessozialhilfegesetz (dort §§ 103 ff.) abgelöst haben, ist im Verhältnis zwischen beteiligten Trägern der Sozialhilfe eine Kostenerstattung für bereits gewährte Leistungen vorge-

sehen. Im Jahr 2003 ist es in diesem Zusammenhang zum Streit zwischen zwei Sozialämtern gekommen, als nämlich das wegen Umzugs des Sozialhilfeempfängers (dem Grunde nach) zur Kostenerstattung verpflichtete Sozialamt einer sächsischen Großstadt das (dem Grunde nach) erstattungsberechtigte Sozialamt in Schleswig-Holstein auf dessen Kosterstattungsverlangen hin zwecks Überprüfung der Höhe der geltend gemachten Forderung um Übersendung der betreffenden Sozialhilfeakte gebeten hat, die andere Seite jedoch dieser Aufforderung - nach Rücksprache mit dem dortigen Datenschutzbeauftragten - nicht hat Folge leisten wollen. (Erstattungsanspruch nach § 107 BSHG; inzwischen ist diese Vorschrift ersatzlos gestrichen worden, weil man gemeint hat, für den nach Einführung des SGB II [„Hartz IV“] in der Sozialhilfe verbleibenden stark verkleinerten Personenkreis darauf verzichten zu können.)

Ich habe das Begehren des sächsischen Sozialleistungsträgers für datenschutzrechtlich zulässig gehalten:
§ 69 Abs. 1 Nr. 1 SGB X erlaubt die Übermittlung solcher Daten, die für die Erfüllung der gesetzlichen Aufgaben des Empfängers erforderlich sind. Auf Grund seiner Pflicht zu einer den Grundsätzen der Wirtschaftlichkeit und Sparsamkeit entsprechenden Haushaltsführung obliegt dem erstattungspflichtigen Sozialleistungsträger eine eigenständige Prüfung der Aufwendungen, deren Erstattung verlangt wird. Deswegen bedarf die Geltendmachung einer Erstattungsforderung einer detaillierten Aufschlüsselung der dem Hilfeempfänger gewährten Hilfen (so auch VG Dresden Beschl. v. 4. Februar 1999 - 6 K 3484/96). Denn nur auf diese Art und Weise ist dem erstattungspflichtigen Sozialhilfeträger eine Überprüfung der gewährten Leistungen auf ihre Gesetzmäßigkeit i. S. d. § 110 SGB XII (ehemals § 111 Abs. 1 BSHG) möglich. Nach dieser Vorschrift sind „aufgewendete Kosten [nur] zu erstatten, soweit die Leistung diesem Gesetz entspricht“. Das heißt: Der leistungsgewährende Träger muss sich auch in Fällen, in denen ihn selbst wegen seines Erstattungsanspruchs letztlich keine Kostenlast trifft, im Rahmen des geltenden Rechts halten; es soll verhindert werden, dass der kostenerstattungspflichtige Träger Aufwendungen des leistungsgewährenden Sozialhilfeträgers erstatten muss, die dieser unter Verletzung der gesetzlichen Regelungen im SGB XII (ehemals BSHG) erbracht hat (vgl. allgemein zu diesem Interessenwahrungsgrundsatz die Ausführungen bei Schellhorn, BSHG-Komm., 16. Auflage 2002, § 111 Rdnr. 4 ff., die auch für die nunmehr geltenden Regelungen im SGB XII ihre Gültigkeit behalten).

Dies hat zur Folge, dass jede einzelne Sozialhilfeleistung durch den erstattungspflichtigen Leistungsträger daraufhin zu überprüfen ist, ob sie (ganz oder teilweise) zu Unrecht gewährt worden ist. Um den erstattungspflichtigen Sozialleistungsträger in die Lage zu versetzen, die Gründe nachvollziehen zu können, die den erstattungsberechtigten Träger zu seiner Entscheidung veranlasst haben, hat dieser seinerseits die Um-

stände, die den geltend gemachten Anspruch begründen, darzulegen und gegebenenfalls in ausreichendem Maße nachzuweisen. Den erstattungsberechtigten Leistungsträger trifft mithin eine Darlegungs- und Beweispflicht (vgl. VG Augsburg, Urteil v. 16. Juni 1998, Az.: Au 3 K 97.968, VwRR BY Nr. 2/99 S. 69 ff.), oder richtiger gesagt eine entsprechende -last.

Der Prüfungspflicht des erstattungspflichtigen Sozialamts steht auch ein gegebenenfalls von ihm abgegebenes Anerkenntnis nicht entgegen, soweit dieses lediglich die Erstattungspflicht dem Grunde nach umfasst. Auch dann verbleibt es hinsichtlich der geltend gemachten Höhe der zu erstattenden Leistungen bei einer vollumfänglichen Prüfungspflicht des erstattungspflichtigen Leistungsträgers.

Einer entsprechenden Prüfungspflicht steht insbesondere auch nicht entgegen, dass es sich bei dem Kostenerstattungsberechtigten ebenfalls um einen Sozialleistungsträger handelt. Insbesondere gibt es meines Erachtens keinen Grundsatz, wonach bei der Kostenerstattung zwischen Leistungsträgern ein weniger strenger Prüfungsmaßstab anzulegen ist. Wie bereits dargelegt, hat der erstattungspflichtige Leistungsträger nicht nur ein Überprüfungsrecht, sondern eine Überprüfungspflicht. Aus diesem Grund kann ich - wie auch einige meiner Kollegen - den insoweit anderslautenden Ausführungen meines Schleswig-Holsteinischen Kollegen in seinen Hinweisen vom 11. November 1998 (Amtsbl. Schl.-H. 1998, S. 965) nicht folgen.

Das Begehren der Aktenübersendung des sächsischen Sozialhilfeträgers ist daher meiner Auffassung nach bei Beachtung folgender Gesichtspunkte keinen datenschutzrechtlichen Bedenken begegnet:

(a) Zur Erfüllung der gesetzlichen Aufgabe des (erstattungspflichtigen) Sozialleistungsträgers im Sinne des § 69 Abs. 1 Nr. 1 SGB X, hier also der Prüfungspflicht im Hinblick auf den Kostenerstattungsanspruch, sind - zumindest dann, wenn der erstattungspflichtige Leistungsträger hierfür Gründe darlegt - *sämtliche* Akten(teile) vorzulegen, die die Voraussetzungen des geltend gemachten Kostenerstattungsanspruchs betreffen, also einen Bezug zu den zu erstattenden Kosten haben.

Die Aktenübersendung ist insoweit erforderlich im Sinne des § 69 Abs. 1 Nr. 1 SGB X, da der betreffende Sozialhilfeträger seine Prüfungspflicht nur ordnungsgemäß erfüllen kann, soweit er selbst anhand der Akten die Tatsachen und Erwägungen nachvollziehen kann, die den erstattungsberechtigten Träger zu seiner Entscheidung veranlasst haben.

(b) Hinsichtlich des Umfangs der vorzulegenden Akten gilt: Es kommt nicht auf den formellen, äußeren Zusammenhang, sondern auf den Inhalt der Unterlagen an, d. h. darauf, ob der Inhalt konkreten Bezug zu den geltend gemachten Kosten hat. Negativ

abgegrenzt bedeutet dies: Von der Vorlagepflicht ausgenommen sind nur diejenigen Verwaltungsvorgänge und damit Aktenteile, die unter keinerlei möglichem rechtlichen Gesichtspunkt einen Bezug zu den geltend gemachten Kosten haben.

Der Dissens mit meinem Schleswig-Holsteinischen Kollegen ist nicht ausgeräumt worden (vgl. dessen TB für 2004 unter 4.6.2 „Misstrauen unter Sozialämtern“). In der Praxis wird ein abgestuftes Austauschen substantiierter Informationen seitens der erstattungsberechtigten und ebensolcher Einwände der erstattungspflichtigen Stelle in den meisten Fällen schon unterhalb der Schwelle der vollständigen Aktenübersendung zum Erfolg führen können.

10.2.12 Warengutscheine für Sozialhilfeempfänger

Im Jahr 2003 wurde ich auf die Praxis des Sozialamts einer sächsischen Großstadt aufmerksam gemacht, einmalige Leistungen nach dem Bundessozialhilfegesetz in der Weise in Form von Warengutscheinen zu gewähren, dass auf den betreffenden Gutscheinen nicht nur der Gegenstand der bewilligten Leistung (ob Haushaltsgerät oder Möbelstück) angegeben, sondern neben dem Namen und der Anschrift des Hilfeempfängers auch die vollständige Bezeichnung und Anschrift des ausreichenden Sozialamts vermerkt war. Eine Vorgehensweise des Sozialamts, die Betroffene - für mich durchaus nachvollziehbar - als Herabwürdigung empfanden, mussten sie sich doch in den Geschäften und damit in aller Öffentlichkeit als Sozialhilfeempfänger zu erkennen geben.

Datenschutzrechtlich handelte es sich um die Preisgabe von durch § 35 Abs. 1 SGB I geschützten Sozialdaten. Die mit der notwendigen Aushändigung des Warengutscheins durch den Hilfeempfänger an den Verkäufer verbundene Bekanntgabe von Sozialdaten durch die Sozialhilfebehörde stellte eine Datenübermittlung im Sinne des § 67 Abs. 6 Nr. 3 SGB X dar. Eine solche ist gemäß § 69 Abs. 1 Nr. 1, 1. Fall SGB X zulässig, soweit sie für die Erfüllung der Zwecke erforderlich ist, für die die Daten erhoben worden sind. Diese Zweckbindung war vorliegend nicht verletzt: Die im Warengutschein enthaltenen Sozialdaten sind zur (Entscheidung über die) Erbringung von Leistungen nach dem Bundessozialhilfegesetz erhoben und gespeichert worden, und die Veranlassung der Vorlage des Warengutscheins im Geschäft diente gerade der Leistungserbringung - also demselben Zweck. Die entscheidende Frage war allerdings, inwieweit es zur Erfüllung des Zwecks tatsächlich erforderlich war, dass der Hilfeempfänger einen Warengutschein statt Geld bekommen und dass der Warengutschein den Namen und die Anschrift des Empfängers enthalten hat, die Nummer des Gutscheins und das Aktenzeichen der Behörde dagegen nicht ausreichen sollte.

Grundsätzlich wird von der Rechtsprechung der Verwaltungsgerichte (BVerwG, Entscheidung vom 14. März 1991 - 5 C 70/86, NJW 1991, 2305, ferner VGH Baden-Württemberg, Urt. v. 23. Juni 1998, FEVS 49, 168, OVG Lüneburg, Beschluss vom 22. April 1997, FEVS 48, 121) die mit der Leistung von Sozialhilfe in Gestalt der Ausreichung von Warengutscheinen verbundene Übermittlung personenbezogener Daten nicht für unzulässig gehalten, weil anerkannt werden muss, dass es Fälle gibt, in denen es erforderlich ist, sicherzustellen, dass die Sozialhilfeempfänger die ihnen zur Verfügung gestellten Mittel tatsächlich für die Ausstattungsgegenstände einsetzen, für deren Anschaffung sie bestimmt sind. Auch Rabattvergünstigungen, die die Sozialhilfeträger erwirken können, stellen einen anerkannten Grund dafür dar, im Rahmen der in Gestalt einmaliger Beihilfen erbrachten Sozialhilfe von Warengutscheinen Gebrauch zu machen. Dabei ist jedoch die konkrete Ausgestaltung auf ihre Erforderlichkeit hin zu überprüfen: Die Erforderlichkeit der Datenübermittlung setzt zunächst voraus, dass die Ausstellung des Warengutscheines dem materiellen Sozialhilferecht entspricht (das ein der Würde des Menschen entsprechendes Leben ermöglichen soll, § 1 Abs. 2 Satz 1 BSHG, § 1 Satz 1 SGB XII). Dass das bei dem mir konkret vorgelegten Vorgang der Fall war, hatte das Sächsische OVG bereits rechtskräftig entschieden und auch überzeugend dargelegt. Bei der Prüfung, ob auch das Sozialgeheimnis, also § 35 Abs. 1 SGB I eingehalten worden war, war zu berücksichtigen, dass das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist. Der Einzelne muss im überwiegenden Allgemeininteresse Einschränkungen dieses Rechtes hinnehmen. Für die Ausübung des pflichtgemäßen Ermessens bei der Entscheidung über die Art und Weise der Leistung von Sozialhilfe bei einmaliger Beihilfe zum Lebensunterhalt, bedeutet dies, dass dem Recht auf informationelle Selbstbestimmung gegenüber anderen abwägungsrelevanten Gesichtspunkten nicht von vornherein der Vorrang zukommt. Vielmehr tritt bei Vorliegen eines überwiegenden Allgemeininteresses und der Auswahl eines Mittels, das für den angestrebten Zweck geeignet und erforderlich ist, das Recht auf informationelle Selbstbestimmung zurück.

Im Hinblick darauf sind insbesondere folgende Überlegungen anzustellen:
Werden für die Ausgabe von Warengutscheinen Gründe der sparsamen Verwendung öffentlicher Haushaltsmittel geltend gemacht (der Träger der Sozialhilfe ist gemäß § 72 Abs. 2 SächsGemO verpflichtet, die Haushaltswirtschaft sparsam und wirtschaftlich zu führen), könnte dem entgegenstehen, dass der Hilfeempfänger die beantragten Leistungen gleich günstig oder günstiger selber beschaffen kann. Der Träger der Sozialhilfe muss also dem Hilfeempfänger die Möglichkeit geben, Unterlagen für einen Kostenvergleich vorzulegen.

Aber auch dann, wenn die Ausgabe von Warengutscheinen zur Einsparung öffentlicher Mittel führt, stellt sich die Frage, ob die Leistungen nicht auch unter Weglassung des Namens und der Anschrift des Hilfeempfängers erbracht werden könnte, so dass der Gutschein lediglich eine Nummer und das Aktenzeichen der Sozialhilfebehörde trüge. Wird die Kaufsache, was bei größeren Haushaltsgegenständen regelmäßig der Fall sein dürfte, von dem Geschäft beim Erwerber angeliefert, macht das die Kenntnis des Namens und der Anschrift des Hilfeempfängers erforderlich. Das gleiche gilt, wenn das Geschäft die Identität der im Warengutschein genannten und der im Geschäft auftretenden Person überprüft, indem es sich z. B. den Personalausweis des Käufers vorlegen lässt. Andernfalls ist kein Grund zu Erkennen, den Namen und die Anschrift des Hilfeempfängers zu nennen.

Im konkreten Fall hat der Sozialhilfeträger sich nicht mit Erfolg auf die Pflicht zur sparsamen Verwendung öffentlicher Haushaltsmittel und auf die möglicherweise erforderliche Anlieferung gekaufter Gegenstände beim Käufer berufen und damit den mit der Ausreichung des betreffenden Warengutscheins verbundenen Eingriff in das Recht des Sozialleistungsempfängers auf informationelle Selbstbestimmung auch nicht rechtfertigen können. Schließlich hat das Sozialamt das dann auch eingeräumt und versprochen, zukünftig auf die Angabe von Name und Anschrift des Sozialhilfeempfängers verzichten und statt dessen ein anonymisiertes Zuordnungskriterium, z. B ein Aktenzeichen, verwenden zu wollen.

Da auf Grund der zum 1. Januar 2005 in Kraft getretenen Regelungen des SGB XII und des SGB II einmalige Leistungen nur noch in Ausnahmefällen in Betracht kommen, da diese nunmehr bereits weitgehend im Regelsatz nach SGB XII bzw. in der Regelleistung nach SGB II berücksichtigt sind, dürfte sich die Problematik - zumindest derzeit - wesentlich entschärft haben.

10.2.13 Teilnahme von Praktikanten eines Jugendamts an Beratungsgesprächen

Darf der Praktikant eines Jugendamts an Beratungsgesprächen, z. B. als Protokollant, teilnehmen, und das vor allem ohne Zustimmung der anderen Gesprächsteilnehmer? Ein Petent sah durch die so praktizierte Verfahrensweise eines Jugendamts sein Recht auf informationelle Selbstbestimmung verletzt.

Ich konnte seine Bedenken nicht teilen, und zwar aus folgenden Gründen:
Nach § 6 Abs. 1 SächsDSG, dessen Anwendung durch die Datenschutzvorschriften des Sozialgesetzbuches nicht ausgeschlossen ist, ist es allen bei der Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen des Freistaates Sachsen beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu ver-

wenden. Über diese Pflicht, das Datengeheimnis zu wahren, sind die Personen nach § 6 Abs. 2 SächsDSG zu unterrichten und hierauf sowie auf die Einhaltung sonstiger Vorschriften über den Datenschutz schriftlich zu verpflichten. Von § 6 SächsDSG werden sämtliche Personen erfasst, deren Aufgabengebiet sie mit personenbezogenen Daten regelmäßig in Berührung bringt. Hierbei kommt es entscheidend auf die Möglichkeit des Datenzugangs an. Damit wird deutlich, dass sämtliche Personen, deren Beschäftigungsverhältnis ihnen faktisch Zugang zu personenbezogenen Informationen ermöglicht, eine persönlich zu erfüllende Rechtspflicht trifft. In welchem Umfang diese Tätigkeiten anfallen oder andere Tätigkeiten für das Beschäftigungsverhältnis bestimmend sind, ist unerheblich. Unerheblich ist auch die Rechtsgrundlage, auf der die Beschäftigung beruht, so dass auch Praktikanten gleichermaßen betroffen sind (Gola/Schomerus, Kommentar zum BDSG, 7. Auflage 2002, § 5 Rdnr. 8). Hinsichtlich der in § 6 Abs. 2 SächsDSG festgelegten Unterrichtungspflicht reicht ein bloßer Hinweis auf die zu beachtenden Vorschriften nicht aus. Vielmehr ist eine umfassende Einführung in die Probleme des Datenschutzes und seine Auswirkungen auf die Tätigkeit am konkreten Arbeitsplatz sowie eine Einweisung in die erforderlichen Schutz- und Sicherungsverfahren nötig.

Hinweis: Für die Verpflichtung auf das Datengeheimnis sollten die von § 2 SächsDSG erfassten Behörden - hierzu zählen selbstverständlich auch die Jugendämter - die von mir erarbeiteten Muster verwenden (veröffentlicht unter www.datenschutz.sachsen.de, Datenschutz und Recht).

Die Teilnahme eines Praktikanten an Beratungsgesprächen zu Ausbildungszwecken begegnet daher bei vorheriger ordnungsgemäßer Verpflichtung des Praktikanten auf das Datengeheimnis auch mit Rücksicht auf das Persönlichkeitsrecht des Einzelnen, den Kreis der Beratungsteilnehmer möglichst eng begrenzt zu halten, keinen datenschutzrechtlichen Bedenken. Die Teilnahme eines Praktikanten zu Ausbildungszwecken bedarf dabei nicht der vorherigen Zustimmung der übrigen Gesprächsteilnehmer, die Entscheidung über die Teilnahme eines Praktikanten an entsprechenden Beratungen obliegt vielmehr allein der Entscheidung der ausbildenden Dienststelle.

Meine Prüfung ergab, dass, soweit erkennbar, die Praktikanten und Auszubildenden des betreffenden Jugendamts ordnungsgemäß auf das Datengeheimnis verpflichtet werden.

Anders ist die Rechtslage, wenn es sich um bloße Betriebspraktika von Schülern allgemeinbildender Schulen handelt, siehe 4/5.9.12.

10.2.14 Hausaufgabenkontrolle durch Hortnerinnen

Ein Vater wandte sich an mich, weil er mit Folgendem nicht einverstanden war: Erzieherinnen eines Schulhorts, den auch sein Kind besuchte, waren dazu übergegangen, die von den Schulkindern während der nachmittäglichen Hortbetreuung gefertigten Hausaufgaben nicht nur abzuzeichnen, sondern in den Schulheften auch zu vermerken, inwieweit es sich um eine eigene Leistung des Kindes handelte oder ob es Hilfe benötigt hatte. Auch die Bearbeitungsdauer wurde festgehalten. Auf diese Weise wurden Zusatzinformationen über die Hortkinder gesammelt, die der Grundschule, die die Kinder besuchten, nach Einschätzung des Vaters durchaus willkommen waren.

Die mit der Eintragung der Bearbeitungsvermerke in das jeweilige Schulheft zwangsläufig verbundene und ja auch gewollte Bekanntgabe dieser personenbezogenen Daten an den Lehrer stellte datenschutzrechtlich eine Datenübermittlung (§ 67 Abs. 6 Satz 2 Nr. 3 SGB X i. V. m. § 61 Abs. 1 Satz 1 SGB VIII) dar, für die es an der nötigen Erlaubnis (§ 67 d Abs. 1 SGB X i. V. m. § 61 Abs. 1 Satz 1 SGB VIII) fehlte. Denn gemäß § 67 d Abs. 1 SGB X ist die Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt. Die beschriebene Datenübermittlung an die Lehrer ließ sich nicht auf eine dieser Vorschriften stützen, insbesondere auch nicht auf die des § 69 SGB X. Danach ist eine Übermittlung von Sozialdaten zulässig, soweit sie erforderlich ist für die Erfüllung einer *im Sozialgesetzbuch bestimmten gesetzlichen Aufgabe* der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden. Hier jedoch war die Übermittlung für die Erfüllung einer gesetzlich vorgesehenen Aufgabe der Kindertagesstätte nicht erforderlich, und die Schule ist keine in § 35 SGB I genannte Stelle und hat keine im Sozialgesetzbuch bestimmten Aufgaben. Überdies: Ein Lehrer hat sich selbst ein eigenes Bild von den Leistungen des Schülers zu machen - ohne die zusätzlichen Informationen Dritter wie z. B. einer Hortbetreuerin, zumal dann, wenn er diese Informationen nur für einen Teil der Schüler erhält, eben diejenigen, die den Hort besuchen. Die Ungleichbehandlung ist ja offensichtlich: Bei Schülern, die nicht den Hort besuchen, verfügt der Lehrer nicht über solche Zusatzinformationen, die in die Leistungsbeurteilung einfließen könnten, obwohl sie möglicherweise bei der Erledigung ihrer Hausaufgaben ebenfalls Hilfe in Anspruch genommen haben, nämlich die ihrer Eltern, Großeltern oder älterer Geschwister. Mit anderen Worten: Die Leistungen eines Schülers, der bei der Erledigung seiner Aufgaben die Hilfe einer Betreuerin in Anspruch genommen hat, werden möglicherweise anders beurteilt als die Leistungen eines Schülers, der seine Aufgaben mit Hilfe seiner Eltern oder Geschwister angefertigt hat - gleiche Leistungen werden so möglicherweise ungleich bewertet, ohne dass hierfür ein sachlicher Grund vorliegt. Auch der Aufgabenzuweisung der § 22 Abs. 2 SGB VIII, § 2 Abs. 1 bis 3

SächsKitaG schließlich ist nicht die Aufgabe des Hortes zu entnehmen, die betreffenden Daten festzuhalten und an die Schule zu übermitteln.

Unerheblich ist dabei, in welcher Trägerschaft der Schulhort betrieben wird, d. h. ob es sich um einen vom Träger der öffentlichen Jugendhilfe selbst oder um einen von einem freien Jugendhilfeträger betriebenen Hort handelt: Zwar sind die Träger der freien Jugendhilfe keine Normadressaten der §§ 61 ff. SGB VIII, jedoch sind sie aus ihrer vertraglichen Beziehung mit dem Leistungsempfänger gehalten, den Datenschutz mindestens in dem Maße zu sichern, wie dies ansonsten Pflicht des Sozialleistungsträgers selbst wäre (Wiesner/Mörsberger, SGB VIII, Anhang § 61, Rdnr. 61) - also gemäß § 61 Abs. 1 Satz 1 SGB VIII nach Maßgabe des § 35 SGB I und der §§ 67 ff. SGB X. Auf diese Weise erfüllen die Träger der öffentlichen Jugendhilfe ihre nach § 61 Abs. 4 SGB VIII bestehende Pflicht, sicherzustellen, dass bei den Trägern der freien Jugendhilfe der Schutz von Sozialdaten in entsprechender Weise wie bei ihnen selbst gewährleistet wird.

Ich habe meine Einwände dagegen zurückgestellt, dass die Vermerke von Hortnerinnen über die Bearbeitung von Hausaufgaben in den Schulheften dann gemacht werden, wenn die Eltern des Kindes hierin eingewilligt haben. Zu missbilligen war jedoch im Anschluss daran die lange Zeit, bzw. die vielen Versuche, die das zuständige Jugendamt für die Erarbeitung der hierzu erforderlichen § 67 b Abs. 2 SGB X genügenden Einwilligungserklärung benötigt hat, nämlich nicht weniger als 16 (!!) Monate - und dies trotz aktiver Mithilfe meinerseits in Form konkreter Formulierungsvorschläge. Meine Mahnungen haben das betreffende Jugendamt offenbar erst beeindruckt, als ich sie mit einer Beanstandungsandrohung verbunden habe. Das Verlangen nach Umsetzung meiner Hinweise und Anregungen muss beim Jugendamt offenbar Widerwillen oder Überforderung ausgelöst haben.

10.2.15 Unberechtigte Geltendmachung des Auskunftsanspruches des Unterhaltsberechtigten durch das Jugendamt

Einen Fall von Aufgaben- und Zuständigkeitsüberschreitung und damit zwangsläufig verbundener (vgl. ganz allgemein dazu jetzt richtungweisend BVerwG, Urteil vom 9. März 2005, 6 C 3/04!) unzulässiger Verarbeitung personenbezogener Daten habe ich bei einem Jugendamt feststellen müssen: Nachdem es von einer Kindesmutter um Hilfe bei der Geltendmachung des Unterhaltsanspruches ihrer minderjährigen Tochter gebeten worden war, hatte sich das Jugendamt an den privaten Arbeitgeber des Kindesvaters gewandt und um Auskunft über dessen Arbeitseinkommen gebeten, nachdem es zuvor den Kindesvater selbst mehrmals erfolglos zur Auskunftserteilung aufgefordert hatte. Wunschgemäß hatte der Arbeitgeber - gegen den Willen des Kindesvaters - dem

Jugendamt die erbetenen Auskünfte erteilt, die dieses sodann an die Kindesmutter weitergegeben hatte. Auf Nachfrage hatte das Jugendamt dem Kindesvater erklärt, zur Einholung derartiger Auskünfte bei seinem Arbeitgeber berechtigt zu sein, woraufhin sich der Vater an mich gewandt hat.

In der Tat, die Auffassung des Jugendamtes war falsch:
Die Jugendämter sind nicht befugt, den dem Unterhaltsberechtigten zustehenden Auskunftsanspruch nach § 1605 Abs. 1 BGB geltend zu machen und dazu Angaben über das Einkommen und Vermögen des Unterhaltspflichtigen zu verarbeiten, d. h. diese zu erheben, zu nutzen oder wie hier an Dritte weiterzugeben. Denn gemäß § 62 Abs. 1 SGB VIII darf das Jugendamt Sozialdaten nur erheben, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Im vorliegenden Fall erfüllte das Jugendamt aber schon keine ihm durch Gesetz zugewiesene Aufgabe.

Namentlich die Vorschrift des § 18 SGB VIII konnte hierfür - entgegen der Auffassung des betroffenen Jugendamtes - nämlich nicht herangezogen werden. Zwar verpflichtet § 18 SGB VIII den Träger der Jugendhilfe zur Beratung und Unterstützung von alleinerziehenden Müttern und Vätern bei der Ausübung der Personensorge einschließlich der Geltendmachung von Unterhaltsansprüchen des Kindes oder Jugendlichen, wobei die Unterstützung auch in Form der Gewährung konkreter juristischer Hilfen geleistet werden kann, so insbesondere bei einer Beratung, die die Geltendmachung von Unterhaltsansprüchen betrifft. Jedoch umfasst die Unterstützung nicht über die rechtliche Beratung hinaus auch die gerichtliche oder außergerichtliche *Vertretung* des alleinsorgenden Elternteils oder des Kindes durch den Träger der Jugendhilfe bei der Geltendmachung von Ansprüchen. Denn nach Art. 1 § 3 Nr. 1 des Rechtsberatungsgesetzes ist den Behörden nur die Rechtsberatung und die Rechtsbetreuung erlaubt, nicht jedoch die Rechtsbesorgung im Sinne von § 1 Rechtsberatungsgesetz (Fischer in Schellhorn, SGB VIII/KJHG, § 18 Rdnr. 9 und Kunkel in LPK-SGB VIII, Rdnr. 4 zu § 18). Demnach dürfte das Jugendamt die Kindesmutter zwar hinsichtlich der Höhe des dem Kind zustehenden Unterhaltes beraten, z. B. den Unterhalt anhand der Unterhaltsrichtlinien des Oberlandesgerichtes Dresden berechnen. Die hierfür erforderlichen Angaben über das Einkommen des Unterhaltspflichtigen hätte aber die Mutter als gesetzliche Vertreterin des minderjährigen Kindes selbst beibringen bzw. besorgen müssen; d. h. sie selbst oder ein anderer zur Vertretung Berechtigter, z. B. ein dazu bevollmächtigter Rechtsanwalt, hätte den Auskunftsanspruch des Kindes nach § 1605 BGB für dieses geltend machen müssen.

Das Jugendamt hatte somit Sozialdaten erhoben, in Akten gespeichert und auch übermittelt, ohne hierzu (gemäß den §§ 62 Abs. 1, 63 Abs. 1, 64 Abs. 1 SGB VIII) befugt gewesen zu sein.

Das Jugendamt hat Einsicht gezeigt: Wie von mir gemäß § 84 Abs. 2 Satz 1 SGB X i. V. m. § 61 Abs. 1 Satz 1 SGB VIII verlangt, hat es die betreffenden personenbezogenen Daten gelöscht. Auch ist mir versichert worden, dass zukünftig entsprechende Auskunftsansprüche nach § 1605 Abs. 1 BGB nicht mehr durch Mitarbeiter des Jugendamtes geltend gemacht werden.

Anders ist die Rechtslage nur dann, wenn ein Mitarbeiter des Jugendamtes infolge schriftlichen Antrages eines Elternteils zum *Beistand* des Kindes wird (§§ 1712 Abs. 1, 1714 BGB; siehe hierzu 10/10.2.7), mit der Folge, dass das Jugendamt durch die Beistandschaft die Vertretungsmacht für die Wahrnehmung der in § 1712 Abs. 1 BGB genannten Rechtsangelegenheiten erhält, zu denen namentlich auch die Geltendmachung von Unterhaltsansprüchen gehört. Hierzu gehören wiederum sämtliche Ansprüche aus den §§ 1601 ff. BGB gegen alle in Frage kommenden Unterhaltsverpflichteten, mithin auch der in § 1605 BGB normierte Auskunftsanspruch (Palandt-Diederichsen, 62. Auflage, § 1712 Rdnr. 5); aber auch dieser Auskunftsanspruch richtet sich bekanntlich nicht gegen den Arbeitgeber des Auskunfts- bzw. Unterhaltspflichtigen (daran ändert sich erst in der Zwangsvollstreckung etwas - § 840 ZPO).

Es gilt, diese Einsicht allen sächsischen Jugendämtern zu vermitteln.

10.2.16 Hartz IV - SGB II: Eine Annäherung

Nachdem man schon seit einigen Jahren in örtlich begrenzten Versuchen, z. B. auch in Leipzig, eine - datenschutzrechtlich mehr oder weniger ausreichend abgesicherte - engere Zusammenarbeit zwischen Sozialhilfebehörden und Arbeitsämtern erprobt hatte, ist es, wie man weiß, unter der Bezeichnung „Hartz IV“ zu einer weitgehenden Zusammenlegung von Sozialhilfe und Arbeitslosenhilfe gekommen: Durch Art. 1 des „Vierten Gesetzes für moderne Dienstleistungen am Arbeitsplatz“ vom 24. Dezember 2003 (BGBl. S. 2954) hat der Bund die sog. „Grundsicherung für Arbeitsuchende“ als neue Sozialleistung geschaffen, für alle Erwerbsfähigen, die kein Arbeitslosengeld (neuerdings „Arbeitslosengeld I“) bekommen, also insbesondere auch alle erwerbsfähigen ehemaligen Sozialhilfeempfänger. Geregelt ist das im neuen Zweiten Buch des Sozialgesetzbuches.

Die Zuständigkeit für die Ausführung des Gesetzes ist mit dem ein halbes Jahr später erlassenen Änderungsgesetz (Art. 1 des Gesetzes zur optionalen Trägerschaft von Kommunen nach dem Zweiten Buch Sozialgesetzbuch [Kommunales Optionsgesetz] vom 30. Juli 2004, BGBl. S. 2014) auf von den Landkreisen und kreisfreien Städten (die ja zugleich örtlicher Träger der Sozialhilfe sind) jeweils (für ihren örtlichen Zuständigkeitsbereich) mit der inzwischen ja in „Bundesagentur für Arbeit“ umbe-

nannten Bundesanstalt für Arbeit (im Folgenden kurz BA) gebildete Arbeitsgemeinschaften übertragen worden - von beiden zusammen gebildete gemeinschaftliche Organisationen, die durch privatrechtliche oder aber auch (!) öffentlich-rechtliche Verträge zu bilden sind (§ 44 b Abs. 1 Satz 1 SGB II) und die der Aufsicht der zuständigen obersten Landesbehörde im Benehmen mit dem BMWA unterstehen (§ 44 b Abs. 3 SGB II). Dies ist jedoch nur noch der Regelfall, denn es ist die Möglichkeit hinzugekommen, dass eine begrenzte Anzahl von Landkreisen und kreisfreien Städten die Aufgabe auch allein übernehmen kann - das sind die sog. optierenden Kommunen nach § 6 a SGB II, von denen es (nach Abs. 3 Satz 1 dieser Vorschrift) im gesamten Bundesgebiet höchstens 69 geben kann (in Sachsen sind dies die Landkreise Bautzen, Döbeln, Kamenz, Löbau-Zittau, Meißen und der Muldentalkreis).

Insoweit diese Mischverwaltungs-Konstruktionen der SGB II-Arbeitsgemeinschaften wirklich verfassungsgemäß sind, wird sich wohl erst noch herausstellen müssen. Ihre Zweckmäßigkeit wird von Fachleuten wie dem früheren Sächsischen Ministerpräsidenten Biedenkopf in dessen Eigenschaft als Mitglied des von der Bundesregierung (ohne gesetzliche Grundlage) eingesetzten Beschwerde- und Beratungsgremiums nachdrücklich und mit überzeugenden Argumenten verneint („langfristig nicht brauchbarer Kompromiss“, DNN/LVZ 16. Juni 2005).

Da die SGB II-Arbeitsgemeinschaften keine Stellen des Bundes sind, muss man aus § 81 Abs. 1 Nr. 2 SGB X wohl folgern, dass zuständig für die Datenschutzaufsicht jeweils der Landesdatenschutzbeauftragte ist. Allerdings ist naturgemäß faktisch die BA der maßgebliche Partner - weil er nicht nur mindestens so viel Erfahrung auf diesem Feld der Sozialverwaltung mitbringt wie der kommunale Teil, sondern auch den personellen Apparat und das Geld hat, Einheitslösungen zu erarbeiten, die dann natürlich auch weitgehend durchgesetzt werden und im Hinblick auf bundesweite Vermittlung von Arbeitsplätzen sich auch in mancher Hinsicht anbieten.
Faktisch hat daher doch der Bundesdatenschutzbeauftragte den weitaus wichtigsten Part bei der Datenschutzaufsicht zu spielen, vor allem, was einheitliche Verfahrensweisen wie EDV-Programme und Datenbanken sowie Vordrucke betrifft: Er ist es, der zentral mit der BA korrespondiert. Die Landesdatenschutzbeauftragten liefern Beobachtungen aus der Praxis, Ideen und Anregungen.

Die Frage, welche Rechtsnatur die SGB II-Arbeitsgemeinschaften haben, ist noch nicht geklärt, und somit z. B. auch noch nicht die Frage, ob „verantwortliche Stelle“ im Sinne von § 67 Abs. 9 Satz 1 SGB X die Arbeitsgemeinschaften selbst oder aber die beiden sie bildenden Partner sind; für letzteres spricht, dass nach § 44 b Abs. 1 Satz 1 SGB II die letzteren und nicht die Arbeitsgemeinschaft Leistungsträger sind, und darauf stellt im Hinblick auf die Bestimmung der verantwortlichen Stelle § 67 Abs. 9 Satz 2 SGB X

ab. Daraus wiederum könnte man leicht zwei Teil-Zuständigkeiten für die Datenschutzkontrolle gemäß § 81 Abs. 1 SGB X folgern. (Immerhin steht das in den SGB II-Arbeitsgemeinschaften arbeitende Personal unverändert ausschließlich im Dienst desjenigen Leistungsträgers, der es für die Arbeitsgemeinschaft abstellt!) Dieses Ergebnis lässt sich nicht ohne weiteres durch den - die Maßgeblichkeit des funktionalen Stellenbegriffes herstellenden - Satz 3 der genannten Vorschrift vermeiden, weil der Tatbestand des § 67 Abs. 9 Satz 3 SGB X dadurch, dass er darauf abstellt, ob Leistungsträger eine Gebietskörperschaft ist, insoweit zu eng formuliert ist.

Auch die Frage, wie ein Zugriff der in den SGB II-Arbeitsgemeinschaften tätigen Bediensteten, die nicht von der BA gestellt werden, auf zentrale personenbezogene Datenbestände der BA rechtlich einzuordnen ist, bereitet Kopfzerbrechen.

Was nun die eigentliche Verarbeitung personenbezogener Daten betrifft, gibt es selbstverständlich aus der Sozialhilfe vertraute unveränderte Fragestellungen, wie die Frage des Verlangens nach Vorlage sowie die Speicherung von (Teilen von) Kontoauszügen (siehe dazu 9/10.2.6), bei denen sich die Feinheiten, in denen sich die Auffassungen der verschiedenen Landesdatenschutzbeauftragten zum Teil auch unterscheiden, nicht zwingend dem Gesetz und überhaupt nicht bisher ergangener Rechtsprechung entnehmen lassen.
Entsprechendes gilt für die aus der Sozialhilfe bekannten Hausbesuche bei Antragstellern bzw. Leistungsempfängern.
Ganz neu für die Landesdatenschutzbeauftragten sind die Fragen, die sich aus dem Umfang des Datensatzes ergeben, der zur Vermittlung des Hilfeempfängers auf dem Arbeitsmarkt erhoben und weiterverarbeitet werden soll. Wenn ein Träger öffentlicher Gewalt sinnvoll Bewerber auf dem Arbeitsmarkt vermitteln können will, gerade auch in von seinem bisherigen beruflichen Werdegang möglicherweise abweichende Bereiche, werden durch die „Obrigkeit“ viele persönliche Daten gesammelt - und eben auch von ihr benötigt, zumal am Anfang der Vermittlungsbemühungen naturgemäß nicht bekannt sein kann, in welche Richtung es in einem konkreteren Stadium möglicherweise gehen wird. Hier sind Grenzen schwer zu bestimmen (etwa für eine gestufte, schrittweise den für die Erhebung zusätzlicher Daten maßgebenden Gesichtspunkt einengende Vorgehensweise). Unter der Bezeichnung „Beschäftigungsorientiertes Fallmanagement im SGB II“ hat dieses Problem schon Schlagzeilen gemacht.

Der organisatorische und personelle Neuaufbau verschärft bei knappen öffentlichen Kassen auch das eine oder andere sonstige schon bekannte datenschutzrechtliche Problem, wie eine Eingabe gezeigt hat, die gemacht wurde, weil ein Petent bei der Abgabe seines Antrages auf Arbeitslosengeld II erlebt hatte, dass neben zwei Sachbearbeiterinnen des Amtes noch ein weiterer Antragsteller sich im Dienstzimmer aufhielt und

dadurch Kenntnis von ihn betreffenden Daten, also z. B. seinen Vermögensverhältnissen, hat erhalten können. Rein rechtlich gesehen ein glatter Verstoß gegen das Sozialgeheimnis durch unbefugte Übermittlung an den Dritten.

Die Stellungnahme des betroffenen Amtes zeigte sehr schnell, was ich bereits vermutet hatte: Nicht ein mangelndes datenschutzrechtliches Bewusstsein war die Ursache, sondern fehlende organisatorische Möglichkeiten, verbunden mit einem ernormen Arbeitsanfall. Dennoch hat das Amt für die nächste Zeit im Rahmen des derzeit Möglichen versucht, Abhilfe zu schaffen, um den Sozialdatenschutz auch in dieser Hinsicht so weit wie möglich zu gewährleisten. Dazu ist in diesem Amt geplant, dass sich der für die Bearbeitung der lebensunterhaltsichernden Anträge zuständige Sachbearbeiter und der für Eingliederung desselben Personenkreises in den Arbeitsmarkt zuständige Sachbearbeiter (sog. Fallmanager) ein Doppelzimmer teilen. Auf diese Weise kann gewährleistet werden, dass die Daten der Leistungsempfänger auch nur den jeweils zuständigen Behördenmitarbeitern bekannt werden. Zusätzlich nutzen diese sog. Fallmanager die Zeiten, in denen das Amt nicht für den Publikumsverkehr geöffnet ist, indem sie überwiegend mit Terminvereinbarungen arbeiten. Auch soll jeder dieser Zweier-Mannschaften noch ein kleines Ausweichzimmer zur Verfügung stehen, um mit Betroffenen unter vier Augen sprechen zu können.

Das Beispiel ist exemplarisch: Bei dem rechtlich-organisatorischen Kraftakt der weitgehenden Zusammenlegung von Sozialhilfe und Arbeitslosenhilfe werden die datenschutzrechtlichen Probleme erst mit einiger Verzögerung, eben nachrangig angegangen. Dies wird für alle Beteiligten noch viel Arbeit mit sich bringen.

10.3 Lebensmittelüberwachung und Veterinärwesen

In diesem Jahr nicht belegt.

10.4 Rehabilitierungsgesetze

10.4.1 Zweckänderung „zu historischen Zwecken“ - ‚unterhalb’ der wissenschaftlichen Forschung: Zum neuen § 13 Abs. 2 Nr. 4 SächsDSG

Der Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik, zu dessen Aufgaben gemäß § 3 Abs. 1 Nr. 1 LBStUG die *Unterrichtung der Öffentlichkeit über Struktur, Methoden und Wirkungsweise des Staatssicherheitsdienstes als eines Instrumentes der Sozialistischen Einheitspartei Deutschlands* gehört, möchte die von der Stasi angewandten Methoden einer verdeckten ‚Bestrafung ohne Urteil’ veranschaulichen, also der sog. *Zersetzungsmaßnahmen* („Formen, Mittel und Methoden der Zersetzung“ nach MfS-Richtlinie 1/76 -

Operative Vorgänge; z. B. „systematische Organisierung beruflicher und gesellschaftlicher Misserfolge zur Untergrabung des Selbstvertrauens einzelner Personen“), und zwar anhand von Einzelbeispielen. Dies soll zweckmäßig vor allem durch Verwendung der diese Maßnahmen dokumentierenden Stasi-Unterlagen geschehen. Um dafür nicht nur auf die Fälle von Personen zurückgreifen zu können, mit denen seine Behörde ohnehin schon Kontakt hat, hat sich der Landesbeauftragte an das Landesamt für Familie und Soziales gewandt, welches in seiner Eigenschaft als Rehabilitierungsbehörde (§ 14 Abs. 2 Satz 2 SächsVwOrgG) über die Anträge auf Rehabilitierung nach dem Zweiten SED-Unrechtsbereinigungsgesetz, also dem Verwaltungsrechtlichen und dem Beruflichen Rehabilitierungsgesetz, entscheidet. In vielen dieser Akten vermutet der Landesbeauftragte naheliegenderweise Unterlagen zu *Zersetzungsaktionen* der Stasi, und seine Frage an mich war, ob nicht ein Bediensteter seiner Behörde in den Rehabilitierungsverfahrens-Akten des Landesamtes nach einschlägigen Unterlagen suchen könnte; denn das Landesamt habe sich aus Kapazitätsgründen außerstande erklärt, diese Sucharbeit selbst zu leisten. Diejenigen Antragsteller, in deren Akten sich Unterlagen zu Zersetzungsmaßnahmen finden lassen würden, sollten dann vom Landesamt angeschrieben und über das Anliegen des Landesbeauftragten unterrichtet werden sowie dadurch die Möglichkeit erhalten, dem Landesbeauftragten ihre Unterlagen zur Verfügung zu stellen und in deren Verwendung zu Zwecken der politischen Bildungsarbeit des Landesbeauftragten einzuwilligen.

Ich habe dem Landesbeauftragten erläutert, dass die Vorgehensweise, einen Bediensteten seiner Behörde in den Rehabilitierungsakten des Landesamtes suchen zu lassen, nur dann datenschutzrechtlich einwandfrei wäre, wenn der Bedienstete förmlich an das Landesamt abgeordnet würde.
Die Begründung dafür ist folgende: Wäre der im Landesamt die Akten durchsehende Bedienstete kein Bediensteter des Landesamtes selbst, sondern einer der Behörde des Landesbeauftragten, handelte es sich um eine Übermittlung personenbezogener Daten vom Landesamt an den Landesbeauftragten (vgl. § 3 Abs. 2 Nr. 5 Buchst. b SächsDSG). Für die Zulässigkeit dieser Übermittlung fehlte es jedoch an der nach § 14 Abs. 1 Nr. 1 SächsDSG nötigen Erforderlichkeit der Kenntnis der Daten (Name, Anschrift, Zersetzungsmaßnahmenopfer-Eigenschaft) durch die Behörde des Landesbeauftragten für die von ihr auszusprechende Einladung an die Betroffenen, ihr Unterlagen zur Verfügung zu stellen. Denn die so genannte Adressmittlung, also die Weitergabe der Einladung des Landesbeauftragten, durch diejenige Behörde, welche die Daten ohnehin auf gesetzlicher Grundlage hat, also hier des Landesamtes, ließe sich auch ohne Datenübermittlung durchführen.

Bei einer solchen Anwendung des Adressmittlungsverfahrens handelte es sich jedoch um eine *Datennutzung* zu einem geänderten Zweck. Diese Nutzung personenbezogener Daten ließe sich nicht auf die besonderen - die Anwendbarkeit der Übermittlungsvorschriften des Sächsischen Datenschutzgesetzes nicht ausschließenden - Datennutzungs- und -übermittlungs-Erlaubnisse der §§ 25 a StrRehaG, 11 VwRehaG, 19 BerRehaG stützen. Denn der Sächsische Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik ist keine für „Verfahren zur Rehabilitierung, Wiedergutmachung oder Gewährung von Leistungen nach dem Häftlingshilfegesetz“ zuständige Behörde, wie es die genannten Vorschriften verlangen.

Rechtsgrundlage für diese Datennutzung wäre jedoch § 13 Abs. 2 Nr. 4 SächsDSG, der die zweckändernde Nutzung *zu historischen Zwecken* - soweit erforderlich - erlaubt, sofern *das Interesse an der Durchführung des Vorhabens das Interesse des Betroffenen an dem Unterbleiben der Zweckänderung erheblich überwiegt.* Diese Voraussetzungen liegen hier m. E. vor: Der Landesbeauftragte hat gemäß § 3 Abs. 1 Nr. 1 und Nr. 4 LBStUG die Aufgabe, entsprechende Erkenntnisse zu erarbeiten und an die Öffentlichkeit weiterzugeben. In dieser Arbeit handelt es sich um eine *dem ursprünglichen Zweck* der Datenverarbeitung *sehr nahe* Zweckverfolgung: In beiden Fällen geht es ja um Aufarbeitung von DDR-Unrecht. Auch stellte die Nutzung für die bloße Adressmittlung einen vergleichsweise recht geringfügigen Eingriff in das Grundrecht dar, so dass unter diesen besonderen Umständen Zweifel an dem nötigen *erheblichen Überwiegen* des öffentlichen Interesses an der Durchführung des Vorhabens gegenüber des Interesses des Betroffenen am Unterbleiben der Zweckänderung wohl kaum zu begründen wären, wenn es überhaupt Sachverhalte geben können soll, die unter diese Vorschrift fallen.

Unerlässlich wäre, wie bei jeder Adressmittlung, dass das Sächsische Landesamt für Familie und Soziales in seinem Anschreiben zu dem Einladungsschreiben des Sächsischen Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik deutlich machte, dass es selbst die Fälle aus den bei ihm vorhandenen Unterlagen herausgesucht hat, also Namen und Anschriften nicht dem Landesbeauftragten übermittelt hat. Das Schreiben des Landesbeauftragten dürfte nur Anlage des Schreibens des Landesamtes sein. Das Landesamt hätte beim Postversand der alleinige Absender zu sein; (möglicherweise bedürfte es daher einer Portokostenerstattung).

Die Tätigkeit des förmlich in das Landesamt abgeordneten Bediensteten des Landesbeauftragten wäre dann ausschließlich eine solche im Verantwortungsbereich des SMS. Denn der Bedienstete wäre dann ausschließlich für das Landesamt tätig.

Eine andere Möglichkeit wäre, dass das Landesamt befristet jemanden einstellte und die Kosten dafür aus den Haushaltsmitteln des Landesbeauftragten erstattet bekäme.
Dem Vorhaben des Landesbeauftragten kommt hier eine Gesetzesformulierung zugute, die ich im Vorfeld der Verabschiedung der Neufassung des Sächsischen Datenschutzgesetzes heftig kritisiert habe, weil sie zu einer verfassungsrechtlich zumindest höchst bedenklichen Einschränkung des Grundrechts auf informationelle Selbstbestimmung führt - deren man wohl nur durch eine verfassungskonforme sehr enge Auslegung Herr werden kann - und dabei keineswegs durch die EG-Datenschutzrichtlinie erzwungen wird, weil sie insoweit auf einem Übersetzungsfehler bzw. einem Missverständnis der EG-Datenschutzrichtlinie beruht, dessen erkennbares Verbreitungsgebiet in Deutschland sich zudem auf Sachsen beschränkt, wie der Vergleich mit § 14 BDSG sowie den folgenden Vorschriften in Landesdatenschutzgesetzen zeigt: BB § 13, BE § 11 Abs. 4, BW § 15, BY Art. 15 Abs. 7 Nr. 7 mit Art. 17 Abs. 2 Nr. 11, HB § 12, HE § 13, HH § 13, MV § 10, NI § 10, NW § 13, RP § 13, SH § 13, SL § 13, ST § 10 und TH § 20, jeweils zusammen mit der in dem betreffenden Gesetz enthaltenen Erlaubnis zur Zweckänderung zu tatsächlich *wissenschaftlichen* Zwecken (‚Forschungsklausel').

Der Gesetzgeber täte daher unverändert gut daran, wie seinerzeit von mir gefordert, in Übereinstimmung mit allen im Zuge der Umsetzung der Richtlinie ergangenen deutschen Gesetzen und in Übereinstimmung mit dem Sinn von Art. 6 Abs. 1 Buchst. b Satz 2 EG-Datenschutzrichtlinie durch Verzicht auf eine Änderung gegenüber dem bisherigen Rechtszustand die durch nichts gerechtfertigte Verminderung des Datenschutzes zu vermeiden, mit der Folge, dass § 13 Abs. 2 Nr. 4 SächsDSG ersatzlos zu entfallen hätte, weil diese Vorschrift, d. h. § 12 Abs. 2 Nr. 4 SächsDSG *a. F.*, wie ebenfalls von mir seinerzeit vorgeschlagen, zusammen mit § 30 Abs. 1 *a. F.* SächsDSG in dem neuen § 36 Abs. 1 SächsDSG aufgegangen ist.

Der Gesetzestext ist leider, nicht zuletzt auch wegen des Nebeneinanders mit § 36 Abs. 1 SächsDSG, zwingend so auszulegen, dass auch nicht-wissenschaftliche Untersuchungen, die zu beschreibenden, „theoretischen" Zwecke historische (= abgeschlossene) Sachverhalte zum Gegenstand haben oder sich der Methode der Statistik (Zusammenzählen von nach Merkmalen unterschiedenen Erscheinungen) bedienen, als privilegierter Zweck anerkannt werden. Zumal in Anbetracht des verfassungsrechtlich vorgegebenen eher weiten Wissenschaftsbegriffes ist dies eine entschieden abzulehnende Einschränkung des Grundrechts auf informationelle Selbstbestimmung. Wissenschaftlich wertlose Chroniken (vgl. 7/5.8.3) oder von vornherein kaum wissenschaftliche Erkenntnisse versprechende Untersuchungen (vgl. zu der Problematik die Entscheidung des OLG Hamm vom 28. November 1995 - 1 VAs 38/94, NJW 1996, 940) werden wissenschaftlichen Untersuchungen gleichgestellt. Das zusätzliche Über-

wiegens-Erfordernis gleicht das nicht aus, und zwar schon deswegen nicht, weil ausgesprochen unklar bleibt, was denn genau abzuwägen sein soll; insbesondere ist ja nicht erkennbar, inwieweit das Grundrecht auf informationelle Selbstbestimmung mit der Ausübung eines anderen Grundrechts abzuwägen sein könnte.

Der Wertungs-Widerspruch zu anderen Gesetzen, die ausschließlich oder fast ausschließlich Daten zu *wissenschaftlichen Zwecken* zu übermitteln erlauben, etwa dem Archivgesetz, ist offensichtlich: An dem Persönlichkeitsrechtsschutz unterliegende Daten in archivierten Unterlagen kommen Dritte nach Sächsischen Archivgesetz unterhalb der Schwelle wissenschaftlicher Forschung nicht heran. Diese Diskrepanz lässt sich nicht begründen, sie lässt sich eben nur durch nicht genügend bedachtes Abschreiben von Formulierungen aus der deutschen Übersetzung der EG-Datenschutzrichtlinie *erklären.*

10.4.2 Probleme der Zweistufigkeit des Verfahrens nach dem Beruflichen Rehabilitierungsgesetz; ein Beispiel für legitimen Einsatz des Instruments der Einwilligung

(1) Wer im Sinne des § 1 des Gesetzes über den Ausgleich beruflicher Benachteiligungen für Opfer politischer Verfolgungen im Beitrittsgebiet, oder kürzer: des Beruflichen Rehabilitierungsgesetzes (BerRehaG), zwischen dem 8. Mai 1945 und dem 2. Oktober 1990 auf dem Gebiet von SBZ bzw. DDR mit nachteiligen Folgen für seine Ausbildung bzw. die Möglichkeit, einer beruflichen Tätigkeit nachzugehen, verfolgt worden ist, hat, sofern er nicht selbst gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen oder in schwerwiegendem Maße seine Stellung zum eigenen Vorteil oder zum Nachteil anderer missbraucht hat (§ 4 BerRehaG, der aus dem Lastenausgleichsrecht übernommene Standard-Ausschlussgrund), abgesehen vom Ausgleich von Nachteilen in der Rentenversicherung (§§ 10-16 BerRehaG), Anspruch auf Unterstützung für berufliche Fortbildung bzw. Umschulung (§§ 6 f. BerRehaG) und im Falle besonderer Bedürftigkeit auf sog. Ausgleichsleistungen in Form einer Geldrente (§§ 8 f. BerRehaG).

In einem ersten Verfahren entscheidet - auf Antrag des Betroffenen (§ 20 BerRehaG) - die Rehabilitierungsbehörde (§ 17 BerRehaG, das ist in Sachsen das Landesamt für Familie und Soziales, § 14 Abs. 2 Satz 2 SächsVwOrgG) darüber, inwieweit tatsächlich *Verfolgung* in diesem Sinne gegeben ist und außerdem kein Ausschlussgrund vorliegt, durch einen feststellenden Verwaltungsakt.

Da dieser Verwaltungsakt aber nur Vorstufe zu einem Verfahren ist, in dem von einer anderen Behörde über *Leistungen* dieser oder jener der drei genannten Arten

entschieden wird, sieht das Gesetz in einer sehr ins einzelne gehenden Regelung vor, dass die Rehabilitierungsbehörde eine „Rehabilitierungsbescheinigung“ ausstellt (§ 17 BerRehaG), in der alle für einen der Leistungsansprüche möglicherweise relevanten Umstände anzugeben sind (§ 22 Abs. 1 und 2 BerRehaG), mit Bindungswirkung für die für die Leistungsgewährung zuständige Behörde (§ 20 Abs. 3 BerRehaG).

(2) Für die Entscheidung über die sog. *Ausgleichsleistungen* sind gemäß § 24 Abs. 2 BerRehaG die Sozialhilfe-Behörden zuständig, also die Landratsämter und die Stadtverwaltungen der kreisfreien Städte als örtliche Träger der Sozialhilfe (§§ 96 f. BSHG). Diese haben sich, wie sich herausgestellt hat, von den Antragstellern als Nachweis für die Erfüllung der Voraussetzungen einer Leistungsgewährung vielfach den gesamten Rehabilitierungsbescheid vorlegen lassen, manche auch demgegenüber nur Rubrum und Tenor des Bescheides, während andere dieser Behörden stattdessen die Rehabilitierungs-*Bescheinigung* (nach §§ 17, 22 BerRehaG) verlangt haben.

Das war zum Teil zuviel des Guten:
Die gemäß § 24 Abs. 2 BerRehaG für die Gewährung von Ausgleichsleistungen nach § 8 BerRehaG zuständigen Sozialämter dürfen Daten nur insoweit erheben, als deren Kenntnis zur Erfüllung ihrer Aufgabe *erforderlich* ist: § 67 a Abs. 1 Satz 1 SGB X i. V. m. § 25 Abs. 4 BerRehaG (gemäß § 12 Abs. 1 SächsDSG gälte nichts anderes). Welche Angaben und Nachweise die Behörde benötigt, ergibt sich aus den für ihre Entscheidung maßgeblichen Vorschriften, also § 8 und § 4 BerRehaG. Unter den danach geltenden Anspruchsvoraussetzungen für Ausgleichsleistungen sind nur folgende Gegenstand von Feststellungen der Rehabilitierungsbehörde:

(a) Eigenschaft, „Verfolgter nach § 1 Abs. 1“ BerRehaG zu sein, § 8 Abs. 1 Satz 1 BerRehaG
(b) Nichtvorliegen von Leistungs-Ausschlussgründen im Sinne von § 4 BerRehaG
(c) Ende der Verfolgungszeit, § 8 Abs. 2 Satz 1 BerRehaG
(d) Dauer der Verfolgungszeit, § 8 Abs. 2 Satz 1 (Rückausnahme) BerRehaG
(e) Beginn der Verfolgungszeit, § 8 Abs. 2 Satz 2 BerRehaG.

Diese fünf für die von der Behörde nach § 8 BerRehaG zu treffende Entscheidung maßgeblichen Umstände sind auch in der im Gesetz inhaltlich vorgegebenen, von der Behörde gemäß §§ 17 Abs. 1, 22 Abs. 1 BerRehaG zu erteilenden Rehabilitierungs-*Bescheinigung* aufgeführt:

(a) Verfolgteneigenschaft: § 22 Abs. 1 Nr. 1 BerRehaG
(b) Nichtvorliegen von Ausschlussgründen: § 22 Abs. 1 Nr. 2 BerRehaG
(c), (d) und (e) Beginn und Ende (und somit die Dauer der Verfolgungszeit[en]): § 22 Abs. 1 Nr. 3 BerRehaG.

Darüber hinaus enthält die in § 22 BerRehaG inhaltlich vorgeschriebene Rehabilitierungs-*Bescheinigung*, die in der Praxis vielfach mit dem feststellenden Verwaltungsakt „Rehabilitierungs-*Bescheid“* gleichgesetzt zu werden scheint, eine Vielzahl weiterer Angaben über den Verfolgten. Diese Angaben sind jedoch *nicht erforderlich* für die Entscheidung des Sozialhilfeträgers, ob dem Verfolgten eine Ausgleichsleistung gemäß § 8 BerRehaG zu gewähren ist. Die Erhebung dieser überschießenden Daten durch die Sozialhilfebehörde ist daher *unzulässig*. Diese darf sich demnach nicht die vollständige Rehabilitierungs-*Bescheinigung* vorlegen lassen.

Mein Thüringer Kollege hat aufgrund dessen bei der dortigen Rehabilitierungsbehörde erreicht, dass diese zusätzlich zur eigentlichen Rehabilitierungs-*Bescheinigung* nach § 22 Abs. 1 BerRehaG, die vielfach auch als Vordruck mit der Bezeichnung „Bescheinigung nach § 17 i. V. m. § 22 BerRehaG *für Zwecke der Rentenversicherung*“ im Umlauf ist (und damit mit einem Zusatz, der sachlich denjenigen Verwendungszweck beschreibt, für den wohl die sämtlichen in § 22 Abs. 1 vorgesehenen Angaben erforderlich sind), eine „*Bescheinigung zur Vorlage bei Sozialämtern*“ ausstellt. Diese vereinfachte Bescheinigung beschränkt sich auf die Angabe, dass der namentlich benannten Person mit dem genannten Datum ein Bescheid nach dem Beruflichen Rehabilitierungsgesetz erteilt worden ist, der die Feststellungen umfasst, dass der Betreffende

- Verfolgter im Sinne des § 1 Abs. 1 BerRehaG ist und
- Ausschlussgründe nach § 4 BerRehaG ihn betreffend nicht vorliegen, und der die
- Zeitpunkte des Beginnes und des Endes der Verfolgungszeit(en) angibt.

Eine solche Verfahrensweise ist einfacher, als wenn die Sozialhilfebehörden den größten Teil der ihnen vorgelegten Bescheinigungen zu schwärzen haben.
Nach zähem Ringen mit dem SMS ist dieses dieser Anregung sowie dem Wunsch, die Antragsteller durch ein Merkblatt unterrichten zu lassen, dass sie nicht die vollständige Rehabilitierungs-*Bescheinigung*, sondern nur die Angaben nach § 22 Abs. 1 Nr. 1-3 BerRehaG vorlegen müssen, nicht gefolgt, es hat aber stattdessen dann doch die Sozialhilfeträger (mit Rundschreiben 19/2004A) angewiesen,

- nicht mehr die Vorlage der „Bescheinigung nach § 17 i. V. m. § 22 BerRehaG für Zwecke der Rentenversicherung“ zu verlangen und
- nicht mehr die Vorlage des gesamten formularähnlich aufgebauten und als „Rehabilitierungs-Bescheinigung nach §§ 17 und 22 Abs. 1 des BerRehaG“ bezeichneten Rehabilitierungs-*Bescheides* zu verlangen, sondern nur dessen erste Seite, und damit zusätzlich zu den oben genannten drei Angaben lediglich Angaben zur verfolgungsbedingten Unterbrechung von Schul- und Berufsschulausbildung.

Damit kann man zurechtkommen. In den wenigen Einzelfällen, in denen Rehabilitierungs-Bescheide aus anderen Bundesländern vorgelegt werden, müssen die Sozialhilfebehörden dann *im Sinne* dieser Weisung handeln.

(3) Umgekehrt erleben die Sozialämter, dass ihnen im Zusammenhang mit Anträgen auf Ausgleichsleistungen Ablichtungen oder sogar die Originale von Schriftstücken überlassen werden, aus denen die Verfolgung im Einzelnen hervorgeht. Verbunden wird dies mit der Bitte, diese Schriftstücke doch zu den Akten zu nehmen, damit dort festgehalten - also aktenkundig - ist, was dem Betreffenden widerfahren ist. Die Antragsteller haben in diesem Zusammenhang vielfach auch das Bedürfnis, mit dem für sie zuständigen Sachbearbeiter in der Sozialhilfebehörde darüber im Einzelnen zu sprechen. Es ist offensichtlich, dass dieses Sprechen für die Betroffenen Teil der Bewältigung ihres Verfolgungs-Schicksals ist.

Der sich hier abzeichnende Konflikt zwischen einem sich nicht nur auf - wenn man so will: lieblose - bloße Gesetzesausführung beschränkende Handeln der Behörde und dem Datenschutz lässt sich lösen: Hier liegt ein legitimes Feld für die Heranziehung der *Einwilligung* des Betroffenen als Rechtsgrundlage für die Verarbeitung seiner personenbezogenen Daten durch die Behörde. Zwar ist die Kenntnis der in den Schriftstücken enthaltenen Daten in diesen Fällen nicht zur Aufgabenerfüllung des Sozialamtes erforderlich, weil die notwendigen Feststellungen ja bereits von der Rehabilitierungsbehörde getroffen worden sind und diese Feststellungen der Sozialhilfebehörde auch vorliegen. Aber bei natürlicher, d. h. dem Empfinden des Verfolgten und Antragstellers entsprechender Betrachtungsweise handelt es sich um einen einheitlichen Lebensvorgang, nämlich dass er für seine Verfolgung einen Ausgleich erhält. Deswegen ist es kein Verstoß gegen den Vorbehalt des Gesetzes, wenn die Behörde in dem Maße, wie dies vom Betroffenen gewünscht wird, auf Einwilligungsgrundlage die in diesen ihr überlassenen Schriftstücken enthaltenen Daten erhebt und speichert. Ich habe dafür folgende Vorgehensweise vorgeschlagen: Der jeweilige Bearbeiter erläutert dem Betroffenen die datenschutzrechtliche Rechtslage (dass nämlich eigentlich die Sozialhilfebehörde nichts mehr an Daten betreffend die Verfolgung des Antragstellers als solche zu prüfen hat) und vermerkt dies in der Akte oder auf einem der vorgelegten Schriftstücke. Anschließend bezeugt der Betroffene ebenfalls darauf durch seine Unterschrift, dass er (gleichwohl) wünscht, dass die Behörde die von ihm vorgelegten Schriftstücke zur Akte nimmt und damit die in ihnen enthaltenen Daten erhebt und speichert. Werden die Schriftstücke nicht persönlich übergeben, sondern per Post, muss die Aufklärung und die Einholung der Einwilligungserklärung schriftlich erfolgen.

11 Landwirtschaft, Ernährung und Forsten

11.1 Ein Leihbeamter, ein Forsthaus, ein Heckenschütze, ein Vernebelungsversuch - ein Fall für den Staatsanwalt

Der Fall rechtfertigt die ausnahmsweise etwas reißerische Überschrift: Die Inhaberin eines Forstbetriebes mit zwei rund 60 km auseinanderliegenden Betriebsteilen (in Sachsen) hatte herausgefunden, dass ein Abteilungsleiter des SMUL sie betreffende Daten an die Bodenverwertungs- und -verwaltungs GmbH Berlin (kurz: BVVG) übermittelt hatte. Nachdem das SMUL der Petentin auf ihre Beschwerde hin auch noch mitgeteilt hatte, dass darin keine Rechtsverstöße zu sehen seien und der Abteilungsleiter lediglich seinen dienstlichen Pflichten nachgekommen sei, hat die Betroffene mich um Prüfung des Vorgangs gebeten.

Dabei kam Folgendes zu Tage: Die Petentin, gelernte Forstassessorin, hatte in den Jahren 2002/2003 auf der Grundlage des Entschädigungs- und Ausgleichleistungsgesetzes (EALG) und der Flächenerwerbsverordnung (FlErwV) durch Vertrag von der zuständigen BVVG Waldflächen (aus ehemaligem Volkseigentum) erworben. *Eine* Voraussetzung für den rechtmäßigen Erwerb ist dabei, dass der Erwerber ortsansässig ist, d. h. seinen Hauptwohnsitz in der Nähe der Betriebsstätte hat oder ihn dorthin verlegt. Nachdem die Petentin dann Anfang Mai 2004 in substantiierter Weise verwaltungstechnische Fehler der Forstverwaltung bei der Bewilligung von Fördermitteln für die Borkenkäferbekämpfung geltend gemacht (und allem Anschein nach beträchtliche Verbesserungen der Verwaltungspraxis bewirkt) hatte, hat der betreffende Abteilungsleiter sich veranlasst gesehen, der BVVG in einem Schreiben u. a. mitzuteilen, dass die von der Erwerberin, wie zu vermuten sei, gegenüber der BVVG gemachte Angabe zu ihrer Wohnung nicht zutreffen könne, dass vielmehr *nur noch eine sporadische Nutzung dieser Wohnung durch die Eheleute zu verzeichnen und der Charakter einer Hauptwohnung nicht mehr gegeben sei*. Begründung: Der Ehemann der Petentin (ein ehemaliger Referatsleiter des SML), sei 1999 in die baden-württembergische Forstverwaltung zurückversetzt worden, mit der Folge entsprechender Residenzpflicht in einem im Schreiben genannten bestimmten dortigen Forstamt. Es handle sich um ein seinerzeit dem Ehemann als Dienstwohnung überlassenes Forsthaus, das die Eheleute aber noch nicht geräumt hätten, was Gegenstand eines Rechtsstreites sei. In einer zur hausinternen Rechtfertigung des Vorgehens verfertigten Stellungnahme des Abteilungsleiters gegenüber dem für Personalangelegenheiten zuständigen Abteilungsleiter finden sich hierzu u. a. noch folgende Angaben: „… Es besteht zumindest erheblicher Zweifel, dass Frau … die Voraussetzung der Ortsansässigkeit zum Zeitpunkt des Erwerbs erfüllte bzw. zum jetzigen Zeitpunkt noch erfüllt … Aus diesem Grund hat die Abteilung … die BVVG über diesen Sachverhalt mit Schreiben vom 24. Mai 2004 informiert und es

anheimgestellt zu prüfen, ob sich hieraus im Hinblick auf den Erwerb von Waldflächen … Konsequenzen ergeben. Zwischenzeitlich wurden wir informiert, dass sie z. Zt. keinen Handlungsbedarf sieht … Trotzdem weisen wir darauf hin, dass Herr Dr. … noch Jahre nach seiner Tätigkeit als „Leihbeamter“ in der sächsischen Forstverwaltung ein Wohnhaus der Staatsverwaltung ohne schriftlichen Mietvertrag bewohnt, obwohl dies als Revierdienststelle dringend benötigt wird. Nichtsdestotrotz erwarb seine Ehefrau unter Angabe dieser Adresse Waldflächen von der BVVG und verhinderte [gemeint ist: bewirkte] somit, dass andere Bewerber, die tatsächlich ihren Lebensmittelpunkt in Sachsen haben, von dem Erwerb dieser Flächen ausgeschlossen werden. Hierin liegt die eigentliche Brisanz dieses Vorgangs, die uns geradezu verpflichtet hat, tätig zu werden …“

Rechtlich stellt sich die Sache ganz anders dar, und niemand in sächsischen öffentlichen Stellen musste das so gut wissen wie die obersten Forstbeamten in Sachsen: Es besteht bzw. bestand zu keinem Zeitpunkt eine Zuständigkeit des SMUL in dem vorliegenden Verfahren, das Staatsministerium war und ist für vor- oder nachvertragliche Aktivitäten im Zusammenhang mit konkreten Flächenerwerbsvorgängen nicht zuständig. Die erfolgte Datenübermittlung zählte daher nicht zur Aufgabenerfüllung des SMUL:

Im Rahmen des Abschlusses des Kaufvertrages hat die Privatisierungsstelle ihr Prüfungsergebnis der zuständigen Landesbehörde zuzuleiten, § 9 Abs. 3 FlErwV. Der Erwerb der Waldflächen durch die Petentin erfolgte 2002/2003. Nach der damals gültigen Zuständigkeitsverordnung - SMULZuVO - vom 26. Mai 2000 (GVBl. 2000, 259 ff.) war zuständige Landesbehörde die Forstdirektion. Nach der nunmehr gültigen SMULZuVO vom 15. Juni 2004 (GVBl. 2004, 274 ff.) ist es das Landesforstpräsidium.

Im Rahmen des Verfahrens zur sogenannten Sicherung der Zweckbindung steht dem Veräußerer, also der BVVG, nach § 12 Abs. 1 FlErwV u. a. dann ein Rücktrittsrecht zu, wenn der Erwerber den für den Erwerb maßgeblichen Hauptwohnsitz (siehe § 4 FlErwV) aufgibt. Es ist Aufgabe der BVVG, diese Voraussetzung zu überprüfen. Wenn die BVVG bei ihrer Überprüfung zu dem Ergebnis kommt, es liege ein Rücktrittsgrund vor, - aber auch erst dann! - kann sie nach § 12 Abs. 8 FlErwV unter Berücksichtigung einer Stellungnahme der zuständigen Landesbehörde entscheiden und dabei auch von einem Rücktritt absehen. Es besteht indes keine Datenübermittlungsbefugnis der zuständigen Landesbehörde hinsichtlich Tatsachen, die einen Rücktrittsgrund belegen könnten. Im Übrigen gilt auch im Rahmen des § 12 Abs. 8 FlErwV: Nach der Zuständigkeitsverordnung - SMULZuVO - vom 26. Mai 2000 war zuständige Landesbehörde die Forstdirektion. Nach der nunmehr gültigen SMULZuVO vom 15. Juni 2004 ist es das Landesforstpräsidium, also auch insoweit zu keinem Zeitpunkt das SMUL. Auch vertragliche Vereinbarungen aus dem Jahr 1996 zwischen der BVVG und dem

SMUL stellen keine Rechtsnorm dar, die die Übermittlung personenbezogener Daten seitens des SMUL rechtfertigen könnten.

Hinzu kommt: Die vom Abteilungsleiter weitergegebenen persönlichen Angaben über die Petentin und ihrer Familie als Nachweis für den angeblich fehlenden Hauptwohnsitz in Betriebsnähe waren zum damaligen Zeitpunkt in der Sache rechtlich ohne Belang: Nach § 4 Abs. 2 Satz 2 FlErwV muss der Käufer seinen Hauptwohnsitz erst innerhalb von zwei Jahren nach Erwerb der Waldflächen in der Nähe der Betriebsstätte nehmen - diese Frist war für die Petentin seinerzeit noch nicht abgelaufen.

Das SMUL kam nach Einschaltung seines für Datenschutzfragen zuständigen Rechtsreferats sehr schnell zum selben rechtlichen Ergebnis und räumte mir gegenüber umgehend die Rechtswidrigkeit der Datenübermittlung ein. Ärgerlich war dabei jedoch der Versuch des SMUL, mir weismachen zu wollen, die Fülle der - angeblichen - Mitwirkungspflichten der Forstbehörden vor und nach dem Abschluss des Kaufvertrages habe zu einem Irrtum der Forstabteilung des SMUL geführt, und der betroffene Abteilungsleiter sei daher irrtümlich davon ausgegangen, auch nach Vertragsabschluss berechtigt gewesen zu sein, Informationen an die BVVG zu übermitteln. Ein Rechtfertigungsversuch, der infolge der aufgezeigten generellen Unzuständigkeit des SMUL in derartigen Flächenerwerbsverfahren bereits im Ansatz nicht überzeugen konnte und der lediglich dazu dienen sollte, gegenüber der Petentin wie auch mir gegenüber das tatsächliche Ausmaß dieses erheblichen Datenschutzverstoßes des Leiters der Forstabteilung des SMUL zu verschleiern.

Diesen Verharmlosungsversuch habe ich gegenüber dem SMUL als einen Verstoß gegen § 27 Abs. 1 Satz 2 Nr. 1 SächsDSG gewertet. Nach dieser Vorschrift sind die öffentlichen Stellen verpflichtet, dem Sächsischen Datenschutzbeauftragten und seinen Beauftragten Auskunft zu ihren Fragen zu geben. Selbstverständlich ist damit eine wahrheitsgemäße, insbesondere auch vollständige Auskunft gemeint. (Ich hatte das SMUL gebeten, „zeitnah und umfassend … Stellung“ zu nehmen.)

Mit dieser gesetzlichen Verpflichtung ist es allgemein (und war es im konkreten Fall) unvereinbar, rechtliche Erkenntnisse, die sich bei der um Auskunft gebetenen öffentlichen Stelle inzwischen ergeben haben (und sich hier für das SMUL ergeben hatten), zurückzuhalten und nach Art eines Anwaltsschriftsatzes den Versuch zu unternehmen, durch eine gezielt am Problem vorbeigehende rechtliche Argumentation den Datenschutzbeauftragten ‚ruhigzustellen’, in der Hoffnung, dieser werde, zumal in Anbetracht des Erfolges für die Petentin, sich nicht um eine weitere rechtliche Durchdringung der Angelegenheit bemühen.

Der Petentin gegenüber hatte das SMUL mit einer demgegenüber stark vereinfachten Abwandlung des Verschleierungsversuches gearbeitet. Aus der Bindung der vollziehenden Gewalt an Gesetz und Recht (Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf) folgt meiner Auffassung nach unmittelbar, dass auch eine solche Verfahrensweise von Trägern öffentlicher Gewalt unzulässig ist. Das hat im vorliegenden Fall - wenn auch auf eine sehr mittelbare Weise - auch das Grundrecht auf informationelle Selbstbestimmung berührt. Im Vordergrund steht jedoch der Versuch, wider eigene schon vorhandene Einsicht dem Sächsischen Datenschutzbeauftragten gegenüber das Ausmaß, in dem es an einer hinreichenden Voraussetzung für die Zulässigkeit einer zu bemängelnden Datenverarbeitungshandlung gefehlt hat, zu verschleiern. Dies ist genau wie entsprechende Verharmlosungsbemühungen gegenüber der Petentin - wohlgemerkt bei Einräumung des Umstandes der Rechtswidrigkeit der Datenverarbeitungshandlung durch die Behörde - im Hinblick auf § 27 Abs. 1 Satz 2 Nr. 1 SächsDSG und im Hinblick auf Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf ein Datenschutzverstoß.

Auf dementsprechende Nachfrage an das SMUL, aus welchen Gründen es davon abgesehen habe, eine der zutreffenden Rechtsauffassung seines Rechtsreferates vollständig entsprechende Stellungnahme abzugeben, die den Datenschutzverstoß des Abteilungsleiters in erheblich deutlicherem Umfang und damit in seinem tatsächlichen Ausmaß dargestellt hätte, hat sich das SMUL dann mir gegenüber, allerdings mit beträchtlichem Widerstreben, einsichtig gezeigt - oder zumindest gegeben. Solche ‚Spielchen' erzeugen vermeidbaren Verwaltungsaufwand.

Allem Anschein nach hat das datenschutzwidrige Treiben von Bediensteten der sächsischen Forstverwaltung damit noch nicht sein Ende gehabt: Im Dezember 2004 ist nämlich dann in einer Stadtteilzeitung unter der Überschrift „Wilderei am Waldessaum?" ein mit dem Pseudonym „Waldigel" unterzeichneter Artikel erschienen, in dem zu dem genannten Forsthaus - es liegt bei etwa zwei Dritteln des Weges zwischen den beiden Betriebsteilen - unter anderem Folgendes ausgeführt wurde:

> „Ab 1991 sanierte das Sächsische Hochbauamt das Haus, es sollte nach Fertigstellung Domizil des nachfolgenden ….er Revierförsters werden. Doch gefehlt - 1992 zog hier ein Leihbeamter des Landwirtschaftsministeriums (SMUL), Herr … mit Familie ein, wie es hieß ‚befristet'.
> …
> Seit März dieses Jahres ruhen Bauarbeiten und Wald. Nichts geschieht? Gemach: Dem Vernehmen nach sollen beide Gebäude nunmehr zum Verkauf ausgeschrieben werden. Obwohl seitens des SMUL Bedarf besteht und angemeldet ist. Denn Bürger - so das SMUL - sollten ihre Anliegen dem Förster ja hier vortragen können und nicht jenseits [Name

> eines großen Waldgebietes] im weit entfernten … Sollte etwa für den Beamten - sein Kaufantrag für das sanierte Haus soll vorliegen - aus des Försters saniertem ‚Prachtschuppen' vielleicht noch eine Ferienwohnung heraussspringen? Wir werden genau hinsehen, was mit der einstigen staatlichen Forstwartei wird …
>
> PS: Wer die Tagespresse verfolgt weiß, dass eine Frau [es folgt derselbe Name wie oben bei dem Leihbeamten] kürzlich Wald [es folgt eine Ortsangabe über eine vom Standort des Forsthauses etwa 25 km entfernte Gegend] erwarb …"

Es ist offenkundig, dass „Waldigel" Informationen aus der Sächsischen Forstverwaltung bekommen hat, und eben personenbezogene, und rechtswidrig.

Inzwischen hat der Vorgang zu staatsanwaltschaftlichen Ermittlungen gegen den betreffenden Abteilungsleiter geführt.

12 Umwelt und Landesentwicklung

12.1 Umweltinformationsgesetz

Nachdem der Bund zur Umsetzung der neuen Umweltinformations-Richtlinie der EG (Richtlinie 2003/4/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003, ABl. L 41 S. 26) im Jahr 2004 ein neues, nunmehr nur für Stellen des Bundes geltendes Umweltinformationsgesetz erlassen hat (Art. 1 des Gesetzes zur Neugestaltung des Umweltinformationsgesetzes und zur Änderung der Rechtsgrundlagen zum Immissionshandel vom 22. Dezember 2004, BGBl. S. 3704), steht ein Landes-Umweltinformationsgesetz zu erwarten.

Angesichts der im UIG 2004 des Bundes im Hinblick auf personenbezogene Umweltinformationen getroffenen Regelung habe ich Zweifel, ob mit einer solchen Regelung, die möglicherweise in den Ländern und namentlich auch in Sachsen Schule machen wird, die durch die Umweltinformations-Richtlinie gebotenen Möglichkeiten, das Grundrecht auf informationelle Selbstbestimmung zu wahren, ausgeschöpft worden sind, und ferner, ob eine solche Regelung deutschem, insbesondere auch sächsischem (Verhältnis von Art. 33 zu Art. 34 SächsVerf), Verfassungsrecht entspricht.

Abgesehen davon ist zweifelhaft, ob die Umweltinformations-Richtlinie inhaltlich frei von Widerspruch zur Datenschutz-Richtlinie (95/46/EG) von 1995 (ABl. L 281 S. 31) ist.

Möglicherweise wird die Landesgesetzgebung diejenige Diskussion auslösen, die im Zusammenhang mit der Bundesgesetzgebung, soweit erkennbar, ausgeblieben ist.

12.2 Anspruch auf personenbezogene Umweltinformationen - ein Fall aus der Praxis

Nach dem (alten, ersten) Umweltinformationsgesetz des Bundes von 1994 (UIG - BGBl. 1994, S. 1490) war folgender Fall zu entscheiden: Eine sächsische Stadt hatte einem als Einzelgewerbetreibender tätigen Schädlingsbekämpfer über etliche Jahre eine Vielzahl von Aufträgen erteilt, namentlich auch betreffend die Imprägnierung von Holz. Durch Anwalt verlangte eine Privatperson, die geltend machte, der Schädlingsbekämpfer habe zeitweise auf seinem Grundstück Substanzen gelagert, die sich auf sie als Bewohnerin des Nachbargrundstückes gesundheitsschädlich ausgewirkt hätten, von der betreffenden Stadt unter Berufung auf § 4 Abs. 1 Satz 1 UIG 1994 folgende Auskünfte:

- „Welche einzelnen Aufträge zur Schädlingsbekämpfung hat die Stadt dem Schädlingsbekämpfer seit dem Jahr 1992 bis heute erteilt?

- Welches Ziel wurde mit den jeweiligen Aufträgen verfolgt?

- Welche chemischen Substanzen wurden bei der Schädlingsbekämpfung verwendet?

- An welchen Orten wurden die jeweiligen Maßnahmen zur Schädlingsbekämpfung durchgeführt?“

Zur gleichen Zeit hat der Betreffende auch ein strafrechtliches Ermittlungsverfahren gegen den Schädlingsbekämpfer in Gang gebracht, mit dem Vorwurf strafbarer Körperverletzung und strafbarer Verstöße gegen Umweltvorschriften, beides durch Einsatz von Schädlingsbekämpfungsmitteln.

Der Antragsteller wollte Datensätze übermittelt bekommen, die wegen der vierten von ihm gestellten Frage parzellengenau hätten beantwortet werden sollen.

Insoweit die Stadt den Schädlingsbekämpfer auf eigenen (städtischen) Grundstücken hatte tätig sein lassen, fehlte es schon an den Anspruchsvoraussetzungen des § 4 UIG. Wäre man dem weiten Behördenbegriff gefolgt, der möglicherweise dem Regelungszweck der mit dem UIG umgesetzten Richtlinie 90/313/EWG entsprochen hätte und der als Behörde im Sinne des § 3 Abs. 1 Satz 1 UIG nicht nur Behörden ansah, die sich ausschließlich oder überwiegend dem Umweltschutz widmen, sondern auch solche Stellen, denen umweltspezifische Belange bei der Ausführung anderer Aufgaben überantwortet sind (so Scherzberg, DVBl. 1994, 733 ff., 735 lSp.), so wäre die Stadt Behörde im Sinne des § 3 Abs. 1 Satz 1 UIG auch insoweit gewesen, als sie fiskalisch tätig gewesen ist und einen Schädlingsbekämpfer, eben fiskalprivatrechtlich, damit beauftragt hat, in den in ihrem Eigentum stehenden Gebäuden Schädlinge zu bekämpfen. Diese weite Auffassung war jedoch vom Wortlaut des Gesetzes nicht gedeckt. Denn die allgemeine Pflicht, sein Handeln auch unter dem Gesichtspunkt seiner Auswirkungen auf die (natürliche) Umwelt zu prüfen, d. h. die Umweltschutzvorschriften, die für alle gelten, einzuhalten, ist erheblich weniger als die Pflichtenstellung, die sich dann ergibt, wenn man als öffentliche Stelle *Aufgaben des Umweltschutzes wahrzunehmen hat*, wie es in § 3 Abs. 1 Satz 1 UIG hieß. Dies entsprach auch genau der erklärten Absicht des Gesetzgebers: Im Gesetzentwurf der Bundesregierung, BT-Drs. 12/7138 S. 12, heißt es nämlich in der Begründung zu § 3: „Informationen über die Umwelt, über die Behörden aufgrund ihrer fiskalischen Tätigkeit (z. B. im Rahmen der staatlichen Liegenschaftsverwaltung, des staatseigenen Hochbaus oder des Beschaffungswesens) verfügen, werden also nicht erfasst.“ Die abweichende Auffassung von Schomerus im Hk-UIG, 2. Aufl.

2002, Rdnr. 48 zu § 3 verkennt den Unterschied zwischen Verwaltungsprivatrecht und Fiskalprivatrecht bzw. das Fehlen des öffentlichen Eigentums in der deutschen Rechtsordnung.

Allerdings hatte die Stadt den Schädlingsbekämpfer auch in ihrer Eigenschaft als Polizeibehörde (Ordnungsamt) wegen Rattenbefalls und als Bauaufsichtsbehörde wegen Hausschwammbefalls tätig werden lassen.

Insoweit war die Stadt grundsätzlich auskunftspflichtig gewesen.
Dies hätte allerdings nicht für den vollen Umfang der im Antrag genannten Auskünfte gegolten. *Informationen über die Umwelt* im Sinne des Gesetzes waren nur Angaben über Einsatzort, Einsatzzeit sowie verwendete Mittel, einschließlich des Wirkstoffes sowie der Menge der verwendeten Mittel. Ein Informationsanspruch konnte also nur darauf gerichtet sein, in welchen Zeiträumen welche Mittel bzw. Wirkstoffe bei der Erledigung von der Stadt - wie gesagt: *als Behörde* - erteilter Aufträge in welchen Mengen eingesetzt worden waren. Denn nur an solchen auf den Schädlingsbekämpfer, nicht auf die Eigentümer von Grundstücken bezogenen Daten hatte der Antragsteller ein Interesse, das dasjenige des Betroffenen (Schädlingsbekämpfers) überwog, da er eben geltend machte, möglicherweise dadurch beeinträchtigt zu sein, dass der Schädlingsbekämpfer zeitweise auf dessen Nachbargrundstück von ihm eingesetzte Schädlingsbekämpfungsmittel gelagert habe. Hinsichtlich des Einsatzortes dieser Mittel war ein das Recht auf informationelle Selbstbestimmung sowohl der betroffenen Grundstückseigentümer als auch des Schädlingsbekämpfers mit Aussicht auf Überwiegen abzuwägendes Interesse des Antragstellers nicht zu erkennen. Die Interessenabwägung, die im Rahmen von § 8 Abs. 1 Satz Nr. 1 UIG 1994 vorzunehmen war, konnte nämlich für jeden Bestandteil des Datensatzes unterschiedlich ausfallen.

Hinzu ist dann gekommen, dass hinsichtlich derjenigen vom Antragsteller verlangten Daten, die Gegenstand des strafrechtlichen Ermittlungsverfahrens geworden waren, dadurch der Auskunftsanspruch durch § 7 Abs. 1 Nr. 2 UIG ausgeschlossen war.

12.3 Kontrollzuständigkeit aufgrund von Schein-Funktionsübertragung

(1) Skurrile Fälle werfen oft bemerkenswerte Rechtsfragen auf, wie folgendes Beispiel zeigt: Ein Grundstückseigentümer hatte einen Vordruck mit der Überschrift „Formblatt 01/2003 des Abwasserverein [sic!] [D-]dorf e. V.“ (mit Angabe der Nummer im Vereinsregister) erhalten, in den er unter anderem
- die Namen aller *im Grundstück wohnenden bzw. die Klärgrube benutzenden Personen*,
- die Anzahl der gehaltenen Pferde, Kühe, Schweine sowie Schafe und Ziegen,

- die Art seiner Anlage sowie
- etwaige Veränderungsabsichten hinsichtlich seiner Abwasseranlage

eintragen sollte. Im Vordruck wie in dem vom Vereinsvorsitzenden unterzeichneten Anschreiben nahm der Verein für sich in Anspruch, gemäß (genau bezeichnetem) Gemeinderatsbeschluss „im Auftrag der Gemeinde“ an *der Erstellung des Abwasserkonzeptes* bzw., wie es an anderer Stelle hieß, an der *Umsetzung des Abwasserkonzeptes* zu arbeiten. Er sei, schrieb der Verein, *durch diese Beauftragung durch die Gemeinde legitimiert worden, notwendige Informationen zur konkreten Planung der dezentralen Entsorgung der Abwässer von den Bürgern zu erfragen.*

Von dem betreffenden Einwohner eingeschaltet, erhielt ich auf meine Frage, inwiefern und womit genau die Gemeinde dem Verein derartige Aufgaben übertragen habe, die Antwort, es gebe zwar den Gemeinderatsbeschluss des Inhaltes „der Abwasserverein [D-]dorf wird zur [sic!] Mitarbeit bei der Umsetzung des Abwasserkonzeptes im Ortsteil [D-]dorf beauftragt“, aber es gebe noch keine vertragliche Vereinbarung mit dem Verein, insbesondere habe die Gemeinde den Verein nicht beauftragt, eine Befragung der durchgeführten Art vorzunehmen, also personenbezogene Daten zu sammeln. Die Gemeinde habe erst durch Anfragen von Einwohnern von der Befragung und namentlich auch dem dabei verwendeten Vordruck erfahren.

(2) Die Frage war nun, ob ich mich auch an den Verein selbst wenden konnte, der ja über die Daten verfügte, d. h. ob ich für diesen insoweit zuständig war.

Mit folgenden Überlegungen habe ich diese Zuständigkeit (damals noch nach § 24 Abs. 1 SächsDSG a. F.) begründet gesehen:
Es handelte sich vorliegend nicht um eine Datenverarbeitung im Auftrag im Sinne des § 7 Abs. 1 SächsDSG (a. F.), bei der der Auftraggeber, hier die Gemeinde, für die Einhaltung der Vorschriften über den Datenschutz verantwortlich wäre. Die Formulierung des Gemeinderatsbeschlusses, wonach der Abwasserverein mit der *Mitarbeit bei der Umsetzung des Abwasserkonzeptes* im Ortsteil D-Dorf beauftragt wurde oder besser gesagt werden sollte, besagte, dass der Verein mehr tun sollte als nur eine technische Hilfeleistung bei der von Hause aus durch die Gemeinde selbst vorzunehmenden Verarbeitung personenbezogener Daten zu erbringen. In diesem Sinne hat die Gemeindeverwaltung den Beschluss nach ihren eigenen Angaben auch immer verstanden.

Stattdessen war der Abwasserverein, als juristische Person des Privatrechtes, gemäß § 2 Abs. 2 Satz 1 SächsDSG (a. F.) insoweit als öffentliche Stelle im Sinne des Sächsischen Datenschutzgesetzes anzusehen, als er mit der Befragung der Einwohner eine Aufgabe der öffentlichen Verwaltung wahrgenommen hat (*Funktionsübertragung* auf einen sogenannten beauftragten Unternehmer; im vorliegenden kein Unterschied zu § 2 Abs. 2

Satz 3 SächsDSG n. F.). Dieses Ergebnis, und damit die Zuständigkeit des Sächsischen Datenschutzbeauftragten für die durch den Verein vorgenommene Verarbeitung personenbezogener Daten, war jedoch nicht ganz einfach zu begründen:

(a) Zu der von der Gemeinde zu erfüllenden Aufgabe der Abwasserbeseitigung (§ 63 Abs. 2 Satz 1 SächsWG) gehört auch die *Aufstellung* eines „Abwasserbeseitigungskonzeptes“ (§ 63 Abs. 2 Satz 2 SächsWG), und denknotwendig auch die *Umsetzung* eines solchen „Konzeptes“. Die Gemeinde kann nach Beteiligung der zuständigen Wasserbehörde und bei vorliegen bestimmter Voraussetzungen ihre Abwasserbeseitigungspflicht auf Personen des Privatrechts übertragen (§ 63 Abs. 4 SächsWG). Wenn aber sogar die Aufgabe der Abwasserbeseitigung als solche übertragbar ist, ist es erst recht die (Teil-)Aufgabe der Erstellung und Umsetzung einer Abwasserbeseitigungskonzeption. Die Gemeinde konnte mithin die Aufgabe der Erstellung und Umsetzung einer Abwasserbeseitigungskonzeption grundsätzlich einer Person des Privatrechtes wie dem Abwasserverein übertragen.

(b) Eine wirksame derartige Aufgabenübertragung war jedoch nicht durch den Gemeinderatsbeschluss erfolgt. Denn dieser Beschluss hat nicht bestimmt, welche Tätigkeiten genau der Verein im Rahmen seiner „Mitarbeit bei der Umsetzung des Abwasserkonzepts“ erbringen sollte. Dies hätte vielmehr einer konkreten Ausgestaltung bedurft. Auch hat die Gemeinde erklärt, sie habe von der Befragung durch den Verein erst durch Bürgeranfragen erfahren. Daraufhin habe der Bürgermeister dem Vereinsvorsitzenden sein „Missfallen“ über diese Vorgehensweise mitgeteilt und dies auch in der nächsten Sitzung des einschlägigen Gemeinderats-Ausschusses dargelegt. Gleichwohl hat der Rechtsschein einer solchen Aufgabenübertragung vorgelegen. Denn die Angaben des Vereins auf dem Fragebogen und in dem Anschreiben haben im Rechtsverkehr nach objektiven Maßstäben auf die wirksame Beauftragung des Vereins durch die Gemeinde schließen lassen.

Bis zum Zeitpunkt der Erlangung der Kenntnis von der durch den Verein durchgeführten Befragung ist dieser Anschein einer Aufgabenübertragung, wenn man einmal die zur durch Rechtsschein entstandenen *Vollmacht* entwickelte Terminologie heranzieht, in Gestalt eines *Anscheins*-Auftrages, danach in Gestalt eines *Duldungs*-Auftrages erzeugt worden. Zunächst kannte die Gemeinde das Handeln des Vereins zwar nicht, hätte es aber bei pflichtgemäßer Sorgfalt kennen und verhindern können. Denn die Gemeinde hat voraussehen können, dass der Verein unter Berufung auf den ihm durch den Gemeinderatsbeschluss erteilten Auftrag tätig werden, insbesondere sich an die betroffenen Einwohner wenden würde. Sie hätte dieses Tätigwerden des Vereins auch verhindern können, und zwar dadurch, dass sie ihm oder auch der Einwohnerschaft

gegenüber erklärt hätte, dass seine „Mitwirkung“ erst durch eine Vertrag konkretisiert werden müsse, bevor er tätig werden könne.

Später hat die Gemeinde es dann wissentlich geschehen lassen, also geduldet, dass der Verein mittels Fragebogens personenbezogene Daten von Einwohnern erhoben und sich dabei auf einen Auftrag der Gemeinde berufen hat. Denn in den Erklärungen des Bürgermeisters sowohl dem Verein wie den Mitgliedern des Ausschusses des Ortschaftsrates gegenüber ist kein Widerspruch gegen die Befragung zu sehen gewesen, der den „Rechtsschein“, also den Anschein eines Handelns im Auftrag der Gemeinde, zerstört hätte. Das „Missfallen“ des Bürgermeisters richtete sich, wie aus dem Protokoll der betreffenden Ausschusssitzung hervorging, nämlich nicht gegen die Befragung als solche, sondern allein gegen das (zeitliche) Vorpreschen des Vereins mit der Befragung im Ortsteil D-Dorf; nach dem Willen des Bürgermeisters hätte eine Befragung stattdessen abgestimmt in allen Ortsteilen erfolgen sollen.

(c) Ein solcher durch eine öffentliche Stelle hervorgerufener Anschein einer kraft öffentlichen Rechts stattfindenden Verarbeitung personenbezogener Daten durch Dritte, insbesondere auch durch Private, muss die datenschutzrechtliche Zuständigkeit der für die datenschutzrechtliche Kontrolle der *öffentlichen* Stellen zuständigen Behörde, also hier des Sächsischen Datenschutzbeauftragten, begründen. Anders wäre das Handeln der öffentlichen Stelle nicht ausreichend (kompetent) kontrolliert. Wenn zudem der private Dritte selbst ebenfalls, wie es hier der Fall gewesen ist, den Eindruck erweckt, er übernehme Funktionen der öffentlichen Stelle mit deren Willen, gibt es keinen Grund, ihn für insoweit der für die öffentlichen Stellen zuständigen Datenschutzkontrolle entzogen zu halten; man nimmt ihn beim Wort und unterwirft ihn derjenigen Kontrollkompetenz, die für den Fall, dass er die von ihm beanspruchte Funktion tatsächlich übertragen bekommen hätte, tatsächlich begründet wäre.

(d) Somit war insoweit das Ergebnis, dass die Gemeinde als öffentliche Stelle den Rechtsschein erzeugt hatte, dem Abwasserverein eine Aufgabe der öffentlichen Verwaltung übertragen zu haben, und gemäß § 2 Abs. 2 Satz 1 SächsDSG a. F. der Verein, soweit er diese scheinbar wahrgenommen hat, als öffentliche Stelle des Freistaates Sachsen anzusehen war, mit der Wirkung, dass ich bei ihm gemäß § 24 Abs. 1 SächsDSG a. F., wie nach § 27 Abs. 1 Satz 1 SächsDSG n. F., insoweit die Einhaltung der Vorschriften über den Datenschutz zu kontrollieren hatte.

(3) Der von privaten Dritten in Anspruch genommene und von einem Träger öffentlicher Gewalt erzeugte Rechtsschein einer Funktionsübertragung begründet die Befugnis des Sächsischen Datenschutzbeauftragten, die in Inanspruchnahme der scheinbaren Funktionsübertragung vorgenommene Verarbeitung personenbezogener Daten zu kon-

trollieren und insbesondere auch rechtlich zu beurteilen. Der Rechtsschein begründet indes noch nicht die Befugnis des betreffenden privaten Dritten, die betreffenden personenbezogenen Daten zu verarbeiten, so weit reicht die Ähnlichkeit mit Anscheins- und Duldungsvollmacht des Zivilrechts nicht: Es ist keine Funktionsübertragung kraft Rechtsscheins.

(4) Abgesehen davon war die betreffende Erhebung und Speicherung personenbezogener Daten auch inhaltlich unzulässig, weil ohne Rechtsgrundlage: § 63 Abs. 2 Satz 2 SächsWG lässt, insbesondere im Zusammenhang mit den in dem darauf folgenden Satz 4 enthaltenen genauen Angaben über den notwendigen Inhalt einer Abwasserbeseitigungskonzeption, nicht eine Aufgabe erkennen, für deren Erfüllung es, in Anwendung der §§ 11 f. SächsDSG a. F. *erforderlich* gewesen wäre, die betreffenden Daten zu verarbeiten.

Eine zur Sammlung der Daten ermächtigende Satzung der Gemeinde existierte nicht. Der andeutungsweise unternommene Versuch, die Befragung der Grundstückseigentümer auf die Rechtsgrundlage einer Einwilligung zu stellen, war schon von der dafür verwendeten Formulierung her gescheitert.

Die Daten sind auf mein auf § 19 SächsDSG a. F. gestütztes Verlangen gelöscht worden.

(5) In ähnlicher Weise habe ich übrigens im Jahre 2003 die Zuständigkeit des Sächsischen Datenschutzbeauftragten begründet gesehen, als ein anderer Datenschutzbeauftragter aufgrund einer behaupteten, jedoch so nicht bestehenden öffentlich-rechtlichen Zuständigkeit die Verarbeitung personenbezogener Daten durch die Deutsche Bahn auf dem Dresdner Hauptbahnhof kontrolliert und dabei seinerseits personenbezogene Daten erhoben hat. Insoweit könnte man von einer Zuständigkeit des Sächsischen Datenschutzbeauftragten für das Handeln scheinbar für Sachsen zuständiger öffentlicher nichtsächsischer Stellen sprechen, soweit diese in Sachsen belegene Sachverhalte betreffend personenbezogene Daten verarbeiten.

(6) Wie dies letztere Beispiel zeigt, lässt sich der Gedanke der Zuständigkeitsbegründung durch Rechtsschein eben noch fortführen:
Es ist nicht erforderlich, dass tatsächlich - wie es die betreffende Gemeinde getan hatte - eine sächsische öffentliche Stelle den Rechtsschein einer Funktionsübertragung erzeugt hat, damit die Zuständigkeit des Sächsischen Datenschutzbeauftragten für die Kontrolle der betreffenden Verarbeitung personenbezogener Daten durch den Privaten begründet wird. Die Anmaßung einer auf (sächsische) öffentliche Gewalt gestützten Befugnis zur Verarbeitung personenbezogener Daten durch einen Privaten allein muss schon

ausreichen, die Zuständigkeit des Sächsischen Datenschutzbeauftragten zu begründen. Denn damit hinreichend geprüft werden kann, ob der Private befugterweise auf Befugnisse eines Trägers öffentlicher Gewalt gestützt personenbezogene Daten verarbeitet, muss eine Kontrollzuständigkeit derjenigen Stelle bestehen, die zuständig ist, falls das Vorbringen des Privaten richtig ist, er also zu recht eine Übertragung einer Befugnis zur Verarbeitung personenbezogener Daten gegenüber den Betroffenen bzw. der Öffentlichkeit in Anspruch nimmt. Denn sonst dürfte niemals diejenige Stelle, die ausschließlich zuständig ist, falls der ‚Anspruch' zu recht erhoben ist, eben der Sächsische Datenschutzbeauftragte, Daten über die von dem Privaten vorgenommene Verarbeitung der Daten Dritter und damit über den Daten verarbeitenden Privaten erheben, falls dessen Berufung auf behördliche Funktionsübertragung sich doch als unbegründet herausstellt.

Kurz: Ähnlich wie man es aus dem gerichtlichen Verfahren, also namentlich im Hinblick auf die Klagebefugnis nach § 42 Abs. 2 VwGO, aber z. B. auch im Hinblick auf die Bestimmungen der Zugehörigkeit zum öffentlichen Recht nach der sog. Schlüssigkeitstheorie (Kopp/Schenke, [13]2003, Rdnr. 6 zu § 40 VwGO) kennt, besteht in solchen Fällen, in denen es möglich ist - insbesondere von dem Verarbeiter *beansprucht* wird -, dass die Verarbeitung personenbezogener Daten auf öffentlich-rechtlicher Grundlage stattfindet, die Kontrollzuständigkeit des Sächsischen Datenschutzbeauftragten bis zur Feststellung seiner Unzuständigkeit.

13 Wissenschaft und Kunst

13.1 Administrative Messung der Leistungen des wissenschaftlichen Hochschulpersonals? - Das Ringen um eine Hochschulpersonaldatenverordnung

Zwischen (dem denkwürdigen) August 2002 und dem Frühjahr 2005 bin ich nahezu mit einem runden Dutzend von Entwürfen einer auf § 106 Abs. 3 Satz 2 SächsHG zu stützenden HochschulpersonaldatenVO befasst gewesen. Dieser langwierige Verlauf hat zugegebenermaßen in starkem Maße daran gelegen, dass ich - pflichtgemäß - immer wieder datenschutzrechtliche Haare in der Suppe der Entwürfe gefunden habe. Zur langen Dauer der Prozedur hat vor allem aber auch beigetragen, dass das SMWK immer wieder Fassungen von Vorschriften, auf die man sich schon fast geeinigt zu haben schien, dann doch nicht akzeptiert und durch Rückgriff auf den Inhalt von ihm vorgelegter früherer Fassungen ersetzt hat - allem Anschein nach auch unter dem Einfluss des Kanzlers der TU Dresden, der, was Sachsen betrifft, wohl als der Vorreiter bei den Bestrebungen anzusehen ist, *administrativ* wissenschaftliche Leistungen der Hochschulbediensteten, insbesondere der Hochschullehrer, zu bewerten. Das Bestreben, und zwar auch der Haushaltspolitik, ist, den Hochschulen mehr Freiheit bei der Mittelverwendung einzuräumen - im Gegenzug zu Erfolgskontrollen in Gestalt sogenannter „Leistungskennziffern“, wobei das Problem die Messung der Leistungen in der *Forschung* ist, und bei Forschung und Lehre vor allem die Messung der *Qualität*.

Dabei geht es - natürlich - vor allem darum, wer es denn sein soll, der die wissenschaftlichen Leistungen misst, oder praxisnäher, wer die Kriterien aufstellt, nach denen die Leistungen in Forschung und Lehre, aber auch in der Selbstverwaltung, schematisch gemessen werden sollen.

Die Auffassung, die ich dazu entwickelt habe, ist folgende: Wissenschaftliche Leistungen, namentlich diejenigen in der Forschung, können zuverlässig nur durch Wissenschaftler desselben Faches beurteilt werden. Die Diskussion unter den Fachgenossen ist ja das Prinzip des Wissenschaftsbetriebes; wenn man so will ja sein Motor wie auch seine Steuerung. Wenn es überhaupt in Anbetracht das Grundrechtes auf Wissenschaftsfreiheit (Art. 5 Abs. 3 Satz 1 GG, Art. 21 Satz 1 SächsVerf), welches insbesondere den Hochschullehrern gegenüber der staatlichen sowie der universitären Hochschulverwaltung zukommt, überhaupt eine Beurteilung wissenschaftlicher Leistungen der Hochschulbediensteten innerhalb der Hochschule *mit Verwaltungs- bzw. Rechtsrelevanz* (nicht als Bestandteil der wissenschaftlichen Diskussion) geben darf (wie wir es ja als Bestandteil von Promotions-, Habilitations- und Berufungsverfahren

kennen), dann darf dies nur durch Wissenschaftler nach den Regeln des Faches erfolgen.

Da dies aber nunmehr für Zwecke der Mittelverteilung außerhalb solcher Verfahren flächendeckend und andauernd durchgeführt werden soll, kann dies aus Gründen des Aufwandes nur anhand äußerer Kriterien unternommen werden. Das halte ich unverändert für ein Unding - kaum einer der Befürworter dieser Bestrebungen, der nicht zugibt, dass ein *Einstein* in einem solchen System keine Chancen gehabt hätte. Wenn man dergleichen gleichwohl versuchen will, braucht man einen Kriterienkatalog bzw. Maßeinheiten, die an äußeren Tatsachen wie Veröffentlichungen oder Patenten anknüpfen.

Mein pragmatischer Vorschlag dafür ist nun gewesen: Wenn die Wissenschaftler des Fachbereiches mit einer der Einstimmigkeit einigermaßen nahekommenden Mehrheit (Grundrechtsausübung ist bekanntlich nicht majorisierbar!) sich auf einen Kriterienkatalog geeinigt haben, dann wird wohl kein Jurist, insbesondere auch nicht der im Streitfall zuständige Verwaltungsrichter, sich trauen dürfen, zu der Einschätzung zu kommen, dieser Maßstab (Kriterienkatalog) sei untauglich, wissenschaftliche Leistungen in diesem Fach zu messen, und daher rechtlich unzulässig.

Im Hinblick darauf hat es in folgenden drei Punkten gegensätzliche Rechtsauffassungen gegeben:

(1) Die Befugnis zur Aufstellung des Leistungsmessungsmaßstabes (mit anderen Worten: der konkreten Evaluationskriterien) für jede einzelne Fakultät musste meiner Auffassung nach bei den Habilitierten dieser Fakultät liegen, und zwar bei einem Quorum von mindestens drei Vierteln - das SMWK wollte hingegen die einfache Mehrheit ausreichen lassen.

(2) Das Staatsministerium wollte dem Rektoratskollegium das Recht zubilligen, den Leistungsmessungsmaßstab für die Fakultät selbst zu bestimmen, wenn der von dieser beschlossene ihm nicht gefällt - wohingegen ich nur die Festsetzung eines vorläufigen Maßstabes durch das Rektoratskollegium für zulässig gehalten habe, der den für die Einführung des Gesamtsystems nötigen Einigungsdruck auf die Hochschullehrer der betreffenden Fakultät ausüben darf.

(3) Nach den Vorstellungen des SMWK sollte die Universitätsleitung die Daten über sämtliche einzelnen in die Leistungsbewertung eingehenden Aktivitäten jedes einzelnen Wissenschaftlers sich übermitteln lassen und weiterverarbeiten dürfen, statt, wie ich es für zwingend halte, lediglich den Gesamtpunktwert, den der Wissenschaftler bei Anwendung des für seine Fakultät geltenden Leistungsmessungsmaßstabes erreicht hat. Letzteres reicht für die Zwecke der Zuweisung von Haushaltsmitteln an den Wissen-

schaftler und für Zwecke des Leistungsnachweises der Hochschule gegenüber der Wissenschaftsverwaltung vollständig aus, sodass ein Mehr an Datenverarbeitung durch die zentrale Hochschulverwaltung wegen Verstoßes gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz rechtswidrig wäre.

Nach Bekanntwerden des Beschlusses des Bundesverfassungsgerichts (vom 26. Oktober 2004 - 1 BvR 911/00, u. a. abgedruckt in NVwZ 2005, 315 und DVBl. 2005, 109) hat das Staatsministerium gemeint, durch dieses Urteil nunmehr in seiner Rechtsauffassung in vollem Umfang bestätigt zu sein. Dem ist aber keineswegs so: Die Entscheidung (die im Übrigen schon einige für mich gut nachvollziehbare Kritik als zu zentralisierungsfreundlich gefunden hat: Entscheidungsbesprechung von Gärditz NVwZ 2005, 407; vgl. auch Lege, Die Akkreditierung von Studiengängen, JZ 2005, 698 ff., Fn 108, 113 und 117) zwingt mich nur, meinen bisherigen Rechtsstandpunkt zu Punkt 2 zu modifizieren: Das Gericht hat es für zulässig erklärt, dass der Gesetzgeber vorsieht, dass universitätszentral der *Senat,* also ein größeres Gremium (in dem Hochschullehrer die Mehrheit haben), für die fakultätsweise oder sogar fachweise („Disziplin“, BVerfG a. a. O. C II 2 b) vorzunehmende Festlegung der Kriterien der Beurteilung der Leistungen insbesondere in der Forschung zuständig ist (Abschnitt C II 2 c bb der Entscheidung). Davon ist ersichtlich in der Tat eine Minderung des Quorums auf die vom SMWK aus § 67 Abs. 5 SächsHochschulG in den VO-Entwurf übernommene Mehrheit gedeckt.

In einer solchen Zuständigkeitsverteilung sieht das Bundesverfassungsgericht eine *strukturelle Gefahr wissenschaftsinadäquater Entscheidungen* ausgeschlossen, es erklärt jedoch den Urheber solcher Zuständigkeitsregelungen für verpflichtet, die Auswirkungen einer solchen Regelung auf den Wissenschaftsbetrieb *zu beobachten und gegebenenfalls nachzubessern*. Außerdem hebt das Gericht in der Entscheidung hervor, dass der jeweilige Grundrechtsträger in dem Falle, dass die Anwendung einer als strukturell wissenschaftsungefährlich anzusehenden Regelung *im Einzelfall* zu einer die Wissenschaftsfreiheit verletzenden Maßnahme führt, der jeweilige Grundrechtsträger durch die Möglichkeit rechtlicher Gegenmaßnahmen geschützt ist (BVerfG a. a. O. C I 3). Die Nichtberücksichtigung der Besonderheiten einzelner Teilbereiche von Fächern (Beispiel: Statistik innerhalb der Wirtschaftswissenschaft), die durch mit einfacher Mehrheit der Hochschullehrer eines Fachbereiches aufgestellte Leistungsmessungskriterien bewirkt werden kann, kann also vor den Verwaltungsgerichten auszutragende Rechtsstreitigkeiten fördern, in denen dann, dem Rückgriff des Bundesverfassungsgerichtes auf § 4 Abs. 2 Brandenburgisches Hochschulgesetz (a. a. O. C II 2 c, 1. Absatz, sowie d bb) folgend, die entsprechende Regelung in § 5 Abs. 2 SächsHochschulG den Maßstab der Entscheidung des Verwaltungsgerichts abzugeben hätte. Solche gerichtlichen Auseinandersetzungen mit ihrer möglicherweise jahrelangen die Mittelvergabe blockierenden

Wirkung könnten mit der Einführung des von mir seinerzeit verlangten Quorums von drei Vierteln weitgehend vermieden werden.

Kurz: Ein solches Quorum wäre eine kluge, wenn auch nach derzeitigem Stand der Verfassungsrechtsprechung nicht verfassungsrechtlich unerlässliche Regelung.

Von dieser Vorgabe des Bundesverfassungsgerichtes, nämlich dass der *Senat* die Befugnis zugesprochen bekommen darf, mit einfacher Mehrheit die Kriterien für die Beurteilung der Leistungen festzulegen, nicht mehr gedeckt wäre jedoch ein Recht der Hochschulleitung (Rektor, Prorektoren, Kanzler), letztlich allein darüber zu entscheiden, anhand welcher Kriterien die Leistungen des wissenschaftlichen Personals in den einzelnen Fachbereichen zu messen sein sollen. Denn: Der wissenschaftliche Sachverstand des Senates - der dem Bundesverfassungsgericht gewährleistet, dass die gesetzliche Regelung keine strukturelle Gefahr wissenschaftsinadäquater Entscheidung schafft (Bundesverfassungsgericht a. a. O. C II 2 c bb) - ist um einiges breiter gefächert als derjenige des Rektors und seiner bis zu drei Prorektoren, die nicht einmal notwendig verschiedenen Fakultäten angehören müssen (§ 94 Abs. 1 Satz 2 SächsHochschulG; strukturelle Betrachtungsweise).

Wie zu Punkt 1 der drei oben genannten Meinungsverschiedenheiten kann man sich aber auch zu Punkt 3 nicht auf die Entscheidung des Bundesverfassungsgerichtes berufen:
Nach der vom Gericht geprüften Regelung des Brandenburgischen Hochschulgesetzes ist die Beurteilung der Leistung des einzelnen Wissenschaftlers ausschließlich Sache des Fachbereiches bzw. des Dekans (BVerfG a. a. O.), während die Universitätsleitung lediglich für „die Evaluation der Forschung an den Fachbereichen und zentralen Einrichtungen *auf der Grundlage der Forschungsberichte“* zuständig ist (§ 65 Abs. 1 Satz 4 Nr. 4 Brandenburgisches Hochschulgesetz). Entsprechend ist in diesem Gesetz der Universitätsspitze auch nur die Zuweisung von Mitteln *an die Fachbereiche* zugebilligt (Nr. 5 der zuletzt zitierten Vorschrift), während die Mittelverteilung innerhalb der Fachbereiche an die einzelnen „Einrichtungen“ des Fachbereiches dem Dekan zusteht (§ 73 Abs. 3 Satz 1 Brandenburgisches Hochschulgesetz).

Was das hochschulorganisatorische Gesamtgefüge betrifft, auf welches das Bundesverfassungsgericht (unter C I 3) einleuchtenderweise abstellt, ist die brandenburgische Regelung wesentlich weniger zentralistisch als der vom Sächsischen Staatsministerium für Wissenschaft und Kunst zuletzt vorgelegte Entwurf es gewesen ist.

Ich habe daher unter datenschutzrechtlichen Gesichtspunkten nur dringend davon abraten können, die betroffenen Regelungen zum Verordnungsinhalt zu machen: Sie verstießen gegen höherrangiges Recht.

Von meinen Einwänden ist möglicherweise inzwischen von anderer juristischer Seite, innerhalb der Staatsregierung, so viel bestätigt worden, dass das Vorhaben zunächst aufgeschoben worden ist (Antwort der Staatsregierung vom 3. Juni 2005 auf eine Kleine Anfrage der Abgeordneten Heike Werner und Heiko Hilker, LT-DS 4/1563, zu Nr. 2).

Wohlgemerkt: Die Rechtsfragen sind im Wesentlichen verfassungsrechtlicher Natur, durch Änderungen am Sächsischen Hochschulgesetz wird man ihnen nicht entgehen können.

13.2 Anschwärzung eines Hochschulkanzlers

Vereinfacht war der Sachverhalt folgender: Zwei Landesbedienstete, die eine Hochschuleinrichtung leiteten, hatten an einer dem Erfahrungsaustausch dienenden Fachtagung hochrangiger Hochschulverwaltungsfachkräfte teilgenommen, auf der der Kanzler einer anderen sächsischen Hochschule einen Kurzvortrag gehalten hatte, in dem er in Gegenüberstellung zu den Erfahrungsberichten anderer Teilnehmer in allgemeiner Form auf den konkreten Stand zu sprechen gekommen war, den die den Gegenstand der Veranstaltung bildende hochschulorganisatorische und hochschulrechtliche Problematik an seiner Hochschule hatte.

Heimgekehrt, rief eine der beiden Leitungskräfte von sich aus den für das Sachgebiet zuständigen Referatsleiter des SMWK an und berichtete über die Tagung, dass er und sein Kollege genauso wie auch der (externe) Wirtschaftsprüfer seiner Einrichtung sowie sein Vorgänger empört gewesen seien, dass der Kanzler (der anderen Universität) die dortigen Auseinandersetzungen und damit sächsische (!) Interna auf das Forum der Kanzler-Fortbildungstagung gezerrt habe; auch habe der Kanzler sich nachteilig über die Sächsische Staatsregierung und die einschlägigen landesgesetzlichen Vorschriften geäußert.

Einige Tage später haben beide dann auf telefonische Bitte des Referatsleiters einen Aktenvermerk über ihre diesbezüglichen Feststellungen angefertigt und diese zunächst dem Wirtschaftsprüfer der Einrichtung und dann dem Staatsministerium zukommen lassen, zusammen mit einem - aktenzeichenlosen - Begleitschreiben.

In diesem Aktenvermerk heißt es, der betreffende Kanzler habe in seinem Vortrag im Wesentlichen nur eine „subjektive“ Darstellung des Standes der Problematik an seiner Hochschule gegeben, namentlich einen bestimmten hochrangigen Verantwortlichen ge-

nannt, mangelnde Kooperationsbereitschaft der Verwaltungsspitze moniert und nicht nur allgemein die in Fachkreisen wohlbekannte Tatsache angesprochen, dass es zwischen Verwaltungsspitze und Wissenschaftlern heftige Auseinandersetzungen gebe, sondern auch konkret die Neuigkeit mitgeteilt, dass die Mehrheit der führenden Wissenschaftler der Einrichtung ein „Misstrauensvotum“ gegen den Vorstand beschlossen habe. Der Redebeitrag des Kanzlers habe *jegliche objektive Darstellung der sächsischen gesetzlichen Regelungen vermissen lassen* und bei Außenstehenden den Eindruck erweckt, dass diese Regelungen in der Praxis zu großen Problemen führten.

Diesen Aktenvermerk schickte der Referatsleiter auch an den früheren Leiter der betreffenden Einrichtung, mit dem er auch über die Angelegenheit telefoniert hat.

In der Folgezeit erfuhr der Kanzler zunächst, dass der Staatssekretär des SMF etwa einen Monat später in einer Besprechung erklärt hatte, der Kanzler habe „mit seinem Reden und Handeln in der Öffentlichkeit durchaus nicht zur Mäßigung beigetragen, im Gegenteil“, und hatte sich das nicht erklären können. Dann erreichten den Kanzler Gerüchte, das SMWK bereite disziplinarische Maßnahmen gegen ihn vor.

Etwa zwei Monate nach der Anfertigung der Aktennotiz erhielt der Kanzler Kenntnis von dem Aktenvermerk, der dem Leiter der betreffenden Hochschuleinrichtung und dann auch dem Rektor übermittelt worden war. Daraufhin wandte sich der Kanzler, etwa drei Monate nach Anfertigung der Aktennotiz, an den Staatssekretär des SMWK, weil ihm das Gerücht zu Ohren gekommen sei, das SMWK bereite disziplinarische Maßnahmen gegen ihn vor, weil er auf der Fachtagung die Leitung der betreffenden Einrichtung an seiner Hochschule angegriffen und von einem Konflikt der Leitung mit Wissenschaftlern berichtet habe. Inzwischen habe er von dem Grund des Vorwurfs, eben dem Aktenvermerk, erfahren und sich mittels der Tonbandabschrift vergewissert, dass er diese Äußerung über die Vertrauensaufkündigung seitens der Wissenschaftler nicht getan habe, und er werde sein Widerrufsverlangen gegenüber den Verfassern der Aktennotiz nötigenfalls gerichtlich geltend machen. Darüber hinaus protestierte der Kanzler dagegen, dass das Staatsministerium, dem der Aktenvermerk vorliege, ihm nicht schon längst Gelegenheit zur Stellungnahme gegeben habe. Fast zwei Monate später, und damit fast fünf Monate nach dem Eingang der Aktennotiz im SMWK, erhielt der Kanzler ein Antwortschreiben des Staatssekretärs, wonach an das Staatsministerium verschiedene Informationen herangetragen worden seien, die Anlass zu der Frage gäben, ob er seine Dienstpflichten verletzt habe, und dass das Staatsministerium ihn deswegen noch nicht in der Sache befragt habe, weil es immer noch in der Prüfung der ihm bekannt gewordenen Informationen begriffen sei, um zu entscheiden, ob es Vorermittlungen veranlassen werde, in deren Rahmen ihm dann gemäß § 24 Abs. 3 Satz 2 SächsDO Gelegenheit zur Äußerung gegeben werde.

Letzteres war unzutreffend: Das Staatsministerium hatte in der Angelegenheit seit dreieinhalb Monaten nichts mehr geprüft. Es hatte den Vorgang auf Vorrat gesammelt und für etwaigen Bedarf ‚hingelegt'; das Staatsministerium, ja die Staatsregierung, stand ganz entschieden auf Seiten der Verwaltungsleitung der betreffenden Einrichtung, und der Kanzler war in Fachkreisen als Kritiker der betreffenden landesgesetzlichen Regelungen bekannt.

Nachdem seine persönliche Widerrufsforderung wegen der angeblichen - dienstgeheimnisverletzenden - Aussage über konkrete Beschlüsse im Konflikt zwischen Verwaltung und Professoren von den beiden Verfassern des Aktenvermerks zurückgewiesen worden war, hat dann der Kanzler durch anwaltliche Forderungsschreiben schon eine Woche später eben diesen Widerruf und die Erklärung erwirkt, sich für die Zukunft zur Unterlassung zu verpflichten und dies auch dem SMWK als dem Adressaten der Aktennotiz mitzuteilen (die beiden Verwaltungsleiter wollten allerdings nicht einsehen, dass sie die Anwaltskosten des Kanzlers zu erstatten hatten).

In dieser Lage hat sich der Kanzler dann an mich gewandt.

Abgesehen von Fragen zur Aktenführung in diesem Fall, über die ich mich in der Folgezeit mit dem SMWK auseinandergesetzt habe, sind folgende rechtswidrigen Verarbeitungshandlungen festzustellen gewesen:

(1) Die beiden leitenden Verwaltungskräfte hatten, als für die von ihnen geleitete öffentliche Stelle handelnd, ein unzutreffendes Datum an das SMWK übermittelt. Das war auch schon datenschutzrechtlich unzulässig, weil die Übermittlung solcher Daten für die Aufgabenerfüllung keiner der beiden beteiligten öffentlichen Stellen geeignet und erforderlich (§ 13 Abs. 1 Nr. 1 SächsDSG a. F., unverändert § 14 Abs. 1 Nr. 1 SächsDSG n. F.) war.

(2) Die Übermittlung der Aktennotiz durch die Leitung der Hochschuleinrichtung an den (externen) Wirtschaftsprüfer war rechtswidrig: Der Wirtschaftsprüfer war hier weder als Rechtsvertreter einer öffentlichen Stelle tätig noch Teil der betreffenden öffentlichen Stelle. Für eine Übermittlung des Datums, welche Angaben die Verwaltungsleitung über das Auftreten des Kanzlers der fremden Hochschule in ihren Akten notiert hat, lässt sich keine gesetzliche Erlaubnis finden. Schon die Unterrichtung des SMWK war keine gesetzlich vorgesehene Aufgabe der Einrichtung, und selbst wenn sie es gewesen wäre, wäre die Übermittlung der eigenen ‚Zeugenaussage' an einen anderen ‚Zeugen' alles andere als der Aufgabe dienlich gewesen, dem SMWK *zuverlässige*, *glaubhafte* Berichte zu verschaffen. Überdies hat auch der Wirtschaftsprüfer sich die im

entscheidenden Teil gerade falsche ‚Berichterstattung' der Verwaltungsleiter zu Eigen gemacht; aus dreier ‚Zeugen' Mund ist hier keineswegs die Wahrheit kundgeworden.

(3) Aus entsprechenden Gründen war die Übermittlung des Berichtes der Verwaltungsleiter an den auswärtigen Vorgänger durch das SMWK ebenfalls nicht nach § 15 Abs. 1 Nr. 1 a. F. (entsprechend § 16 Abs. 1 Nr. 1 n. F.) SächsDSG zulässig.

(4) Rechtswidrig war schließlich die mangelnde Offenlegung der Datenerhebung und -speicherung durch das SMWK gegenüber dem Kanzler (nach zulässiger Entgegennahme der Daten von Dritten) im Hinblick auf den - zunächst begründet scheinenden - Verdacht des SMWK, der Kanzler habe mit konkreteren Angaben über die im Übrigen bekannten Auseinandersetzungen seine Pflicht zur Verschwiegenheit in Dienstangelegenheiten verletzt. Diese Unterlassung hat, wie ich dem SMWK geschrieben habe, den größten Beitrag zu der für alle Beteiligten unwürdigen Situation geleistet.

Die Geschichte hat dann noch ein Nachspiel gehabt, der Kanzler hat den Verlauf der Anschwärzung mitsamt Anschwärzern publik gemacht: Er hat, und zwar in einem mit dem Briefkopf des Kanzlers seiner Hochschule versehenen Schreiben, Ausschnitte aus meiner den seiner Eingabe zugrunde liegenden Fall darstellenden und datenschutzrechtlich bewertenden Stellungnahme gegenüber dem SMWK als Anlage einer eigenen Schilderung des Vorganges an die Mitglieder desjenigen Arbeitskreises leitender Hochschulverwaltungskräfte geschickt, auf dessen Tagung er seinerzeit gesprochen hatte. In diesen Ausschnitten waren auch die Namen der beiden Verwaltungsleiter enthalten, die ihn seinerzeit angeschwärzt hatten, auch wurde der Staatssekretär mit Namen erwähnt.

Daraufhin haben sich die beiden erstgenannten beschwert, und das SMWK hat das mit der Überlegung unterstützt, dass die Namensnennung zur Rechtsverteidigung nicht erforderlich gewesen sei.

Ich habe dem Kanzler daraufhin in folgendem Sinne geschrieben: Wie der Bundesgerichtshof in seinem Urteil vom 9. Dezember 2002, Az. 5 StR 276/02, in der Strafsache gegen den damaligen Sächsischen Datenschutzbeauftragten Dr. Thomas Giesen wegen Verletzung des Dienstgeheimnisses unter II 2c, S. 12 (11/16.2.1), bestätigt hat, ist der Sächsische Datenschutzbeauftragte befugt, im Falle des Aussprechens einer Beanstandung den Anspruch des Petenten auf Bescheidung seiner Eingabe dadurch zu erfüllen, dass er ihm eine Abschrift der Beanstandung überlässt.

Inwieweit ein Petent als Privatperson dann seinerseits den Inhalt der Beanstandung Dritten zur Kenntnis geben darf, hat der Sächsische Datenschutzbeauftragte nicht zu beurteilen. Jedenfalls ergeben sich aus etwaigen Grenzen dieses Rechtes nach der

genannten BGH-Entscheidung keine Einschränkungen der Befugnis des Datenschutzbeauftragten, dem Petenten den Text der Beanstandung zukommen zu lassen.

Im vorliegenden Falle stand jedoch nicht zweifelsfrei fest, ob der Kanzler bei seiner Übersendung des Auszuges aus dem von mir gegenüber dem SMWK abgegebenen Stellungnahme an die Mitglieder des betreffenden Arbeitskreises als Petent, also als Privatperson, oder aber - worauf die Verwendung des Briefkopfes der Hochschule hingedeutet hat - nicht vielmehr in seiner Funktion als Kanzler dieser Hochschule gehandelt hat. Wäre letzteres der Fall, bestünden wohl erhebliche Bedenken gegen die Rechtmäßigkeit der Datenübermittlung. In derartigen Fällen sollte der Petent, der Inhaber eines öffentlichen Amtes und zugleich wegen (nicht: in!) dieser Eigenschaft als Grundrechtsträger von einer rechtswidrigen Verarbeitung personenbezogener Daten betroffen gewesen ist, nicht mit amtlichen Briefkopf, sondern in jeder Hinsicht eindeutig als Privatperson handeln, wenn er Dritte personenbezogen vom Ergebnis einer datenschutzrechtlichen Kontrolle unterrichtet. (Dies gilt selbstverständlich nicht nur dann, wenn das Ergebnis der Kontrolle in einer förmlichen Beanstandung gemäß § 29 Abs. 1 Satz 1 SächsDSG enthalten ist.)

13.3 Auskunftsanspruch gegen das Sächsische Staatsministerium für Wissenschaft und Kunst

Bereits im Jahr 1998 kam es zu einer Auseinandersetzung zwischen dem Datenschutzbeauftragten und dem damaligen Staatsminister für Wissenschaft und Kunst. Der Staatsminister hatte versucht, bei der Besetzung einer Professur an der Technischen Universität Dresden unter Bezug auf eine unzureichende Bewerberlage auf das Verfahren einzuwirken. Er war zu diesem Zeitpunkt jedoch noch nicht beteiligt und hätte deshalb auch noch keine Informationen über einzelne Bewerber haben dürfen. Um den dahinter liegenden datenschutzrechtlichen Verstoß aufzuklären, hatte der Datenschutzbeauftragte den Staatsminister um Auskunft gebeten, von wem er die Informationen über das Besetzungsverfahren bekommen hatte. Dies verweigerte der Staatsminister. Der Datenschutzbeauftragte klagte und bekam in der ersten Instanz Recht. Das SMWK ging in Berufung. Vor der im Februar 2004 angesetzten Verhandlung vor dem Oberverwaltungsgericht zog das SMWK die Berufung zurück, so dass das Urteil der Erstinstanz rechtsgültig wurde. Ich habe mich daraufhin an das SMWK gewandt, gegen das der Rechtsanspruch des Datenschutzbeauftragten auf Auskunft besteht. Darüber hinaus habe ich sowohl ein Gespräch mit dem (zu diesem Zeitpunkt bereits lange ausgeschiedenen) ehemaligen Staatsminister gesucht, als auch bei der TU Dresden die Umstände des damaligen Besetzungsverfahrens untersucht. Das Staatsministerium versuchte ebenfalls, an die Auskunft zu gelangen. Der Staatsminister a. D. verweigerte

sowohl der Staatsministerin als auch mir eine Namensnennung, machte mir gegenüber allerdings nähere Ausführungen zum Geschehen. Nach Gesprächen mit den Mitgliedern der Berufungskommission und der Durchsicht der Berufungsakte stellt sich der Vorgang folgendermaßen dar: Da es um die Besetzung einer Professur zur Lokalgeschichte Sachsens ging, wurde in der Berufungskommission die Frage diskutiert, ob das Kriterium „sächsische Herkunft“ bei der Berufung eine Rolle spielen sollte. Diese Frage wurde nach einhelliger Schilderung der Mitglieder der Kommission ohne Bezug auf einzelne Kandidaten auch mit Außenstehenden besprochen, um Hilfe für die Entscheidungsfindung zu bekommen. Einer dieser Außenstehenden hat diesen Diskussionsgegenstand auch an den Staatsminister herangetragen, der sich dann an die Universität wandte. Der Berufungskommission, in der der eventuelle datenschutzrechtliche Verstoß geschehen wäre, ist danach meines Erachtens kein Vorwurf zu machen.

Ich habe mich entschieden, da der Vorgang sieben Jahre zurückliegt, die Professur besetzt ist, wobei das Schreiben des Staatsministers keine Wirkung zeigte, beide Amtsnachfolger des Staatsministers zugesichert haben, dass dies unzulässig gewesen sei und mit ihnen nicht wieder geschehen würde, und selbst bei einer Namensnennung des Ministerinformanten wahrscheinlich keine weiteren datenschutzrechtlichen Konsequenzen erwachsen wären, von einer Weiterverfolgung des Rechtsanspruches abzusehen.

Vgl. auch oben 5.7.6

14 Technischer und organisatorischer Datenschutz

14.1 Drahtlose Netze - Risiken und Sicherheitsmaßnahmen

Drahtlose Netze ermöglichen den Datenaustausch zwischen zwei oder mehreren IT-Geräten (z. B. Handy, PC, Notebook, Drucker, Funktastatur, Funkmaus, Fernbedienung) durch Funkübertragung. Kabellose Netze verbessern die Mobilität, Flexibilität und den Komfort, weil keine direkten physikalischen Kabel-Verbindungen erforderlich sind. Die Reichweiten der Funknetze können je nach Verfahren und vorliegenden Umweltbedingungen zwischen 10 und 150 m liegen, bei Richtfunkstrecken sogar mehrere Kilometer.

Drahtlose Netze verbreiten sich gegenwärtig sehr stark. Sie werden vor allem wegen ihrer Mobilität auch in Firmen- und Krankenhausnetzen und in der öffentlichen Verwaltung eingesetzt.

Zum Aufbau kabelloser Netze oder zur Erweiterung drahtgebundener Netzwerke können verschiedene Funk-Standards bzw. Schnittstellen mit unterschiedlichen Eigenschaften (Datenrate, Reichweite, Vernetzung, Bauform, Sicherheit) genutzt werden. Die bekanntesten Standards sind: Infrarot, Bluetooth und Wireless Local Area Networks (WLAN). Diese sollen zum besseren Verständnis kurz erläutert werden.

Die Infrarot-Technik wird schon relativ lange zur Funkübertragung über kurze Distanzen genutzt und von den meisten Betriebssystemen unterstützt. Infrarot-Schnittstellen werden beispielsweise zur Fernbedienung des Fernsehgerätes, zur Kommunikation mit Mobiltelefonen, Laptops, PDAs[19], Druckern oder mit Peripheriegeräten, wie Funktastatur oder Funkmaus eingesetzt. Infrarot-Kommunikationen erfordern einen direkten Sichtkontakt der miteinander kommunizierenden IT-Geräte.

Obwohl bei der Infrarotübertragung nur eine geringe Entfernung von einigen Metern überbrückt werden kann, ist ein Mithören der Kommunikation nicht auszuschließen. Der Infrarot-Standard sieht aber keine Sicherheitsmechanismen zur Gewährleistung der Vertraulichkeit vor. Deshalb muss der Nutzer bei Bedarf selbst für die Sicherheit der zu schützenden Daten durch den Einsatz kryptographischer Verfahren auf der Anwendungsebene sorgen.

Die Infrarot-Technologie wird zunehmend durch Bluetooth verdrängt. Die Bluetooth Special Interest Group (SIG) entwickelte unter dem Codenamen Bluetooth (Blauzahn)

[19] PDA (Personal Digital Assistent) ist ein besonders kleiner und leichter Computer (batteriebetriebenes Handgerät) mit spez. Funktionsumfang (Kalender, Notizen, Adressdatenbank, Taschenrechner).

eine Technologie zur drahtlosen Übermittlung von Sprache und Daten mit Funkwellen. Bluetooth nutzt dazu das frei verfügbare Funknetz ISM (Industrial-Scientific-Medical).

Diese Technologie ist weit verbreitet und wird von vielen Herstellern unterstützt. Im Gegensatz zur Infrarotübertragung spielen Wände und Gegenstände zwischen Sender und Empfänger kaum eine Rolle.

Bluetooth wird hauptsächlich für den Aufbau drahtloser Ad-hoc-Verbindungen über kurze Distanzen zwischen IT-Geräten unterschiedlicher Art eingesetzt. Die Reichweite des Funknetzes ist abhängig von der Sendeleistung der Bluetoothgeräte. Hinsichtlich der Sendeleistung unterscheidet man drei Geräteklassen. IT-Geräte der Klasse 3 (bis 1mW Sendeleistung) können nur Reichweiten von 10 cm bis max. 10 m erreichen, während Geräte der Klasse 1 (bis 100mW Sendeleistung) sogar Distanzen bis zu 100 m überbrücken können.

Ein auf den elektronischen Geräten integrierter Bluetooth-Mikrochip ermöglicht die Kommunikation, sofern die Benutzer ihre IT-Geräte dazu eingerichtet haben. Der Bluetooth-Standard bietet darüber hinaus auch Sicherheitsmechanismen, wie Authentifizierungs- und Verschlüsselungs-Algorithmen zur geschützten Datenübertragung personenbezogener Daten an.

WLAN bezeichnet ein drahtloses lokales Funknetzwerk, das im IEEE 802.11-Standard festgelegt ist. Dieser Standard, der nur grundlegende Festlegungen zu WLAN enthält, wurde weiter entwickelt u. a. mit höheren Datenübertragungsraten (IEEE 802.11 b, 802.11 g) und größeren Reichweiten sowie mit verbesserter Sicherheit (IEEE 802.11 i).

Während moderne Notebooks meist schon für drahtlose lokale Netzwerke vorbereitet sind, müssen ältere IT-Geräte mit WLAN-Karten ausgestattet und Funknetzwerke eingerichtet werden, bevor sie per Funk kommunizieren können. Der WLAN-Standard sieht bereits Sicherheitsmechanismen durch das WEP-Verfahren (Wired Equivalent Privacy) vor. Allerdings bewerten Experten das WEP-Verfahren wegen zu kurzer Schlüssellängen (40 bzw. 104 Bit) und des eingesetzten kryptographischen Verfahrens (RC4) als unsicher. Deshalb wurden neuere Sicherheitsstandards WEP2 (WEP Version 2) und WPA (Wi-Fi Protected Access) entwickelt.

WLAN-Funknetze können neben der lokalen Vernetzung auch Zugang zum Internet (z. B. im Wartebereich von Kongresszentren, Messen oder Flughäfen) durch so genannte „Hot-Spots“ ermöglichen. „Hot-Spots“ sind Access Points, die als zentrale Funkbrücke oder Gateway die Reichweite des Funknetzes erweitern und das Funk-LAN mit dem „verkabelten“ LAN oder wie hier mit dem Internet verbinden.

Oft sind in mobilen IT-Geräten (PDAs) zugleich verschiedene Schnittstellen wie Infrarot, WLAN und Bluetooth implementiert.

Der Vorteil drahtloser Netze besteht darin, dass sie ohne aufwendige Neuverkabelung von Geräten, Räumen oder Gebäuden sofort einsatzfähig sind. Diesen Vorzügen stehen aber erhebliche Risiken durch die sich unbegrenzt und unkontrolliert ausbreitenden Funkwellen gegenüber, die sich auch von Raum- oder Gebäudemauern nur geringfügig dämpfen lassen. Die „Luftschnittstelle“ ist im Allgemeinen ungeschützt und oft öffentlich zugänglich. Sie ermöglicht das Orten bzw. die Anwesenheitskontrolle von mobilen IT-Geräten und somit auch das Erstellen von Bewegungsprofilen ihrer Nutzer. Dies gilt besonders für Bluetooth-Systeme, die standardmäßig immer eingeschaltet sind.

Die Luftschnittstelle erleichtert außerdem das Abhören von Funknetzen, Kopieren und Manipulieren (z. B. Man-in-the-Middle-Angriff) der Daten. Dabei ist zu beachten, dass die Ausbreitung der Funkwellen von der Sendeleistung, Mauerdicke, Art der Fenster, Reflektionen der Funkwellen usw. abhängig ist. Außerdem kann sich durch den Einsatz mobiler IT-Geräte die Gefahr des Verlustes oder Diebstahls der Geräte und der darauf gespeicherten personenbezogenen Daten erhöhen.

Um die Risiken drahtloser Netze besser beherrschen zu können, sind zusätzliche Sicherheitsmaßnahmen erforderlich. Dies gilt insbesondere für die Verarbeitung sensibler Daten wie Gesundheits-, Sozial-, Steuer- und Personaldaten, sowie Daten, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, die Gewerkschaftszugehörigkeit oder das Sexualleben hervorgehen.

Neben dem Einsatz ausreichend sicherer Verschlüsselungsverfahren für die Daten-Übermittlung auf der leicht abhörbaren Luftschnittstelle, sollte die Sendeleistung so gering wie möglich eingestellt und nicht benötigte Dienste deaktiviert werden. Außerdem können VPN-Tunnel oder Radius-Server die Sicherheit drahtloser Netze wesentlich erhöhen. Ausführliche Informationen über mögliche Gefährdungen und geeignete Schutzmaßnahmen beim Einsatz drahtloser Technologien enthält die Orientierungshilfe „Datenschutz in drahtlosen Netzen“, die derzeit von den Arbeitskreisen „Technik“ und „Medien“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt wird.[20] Sie wendet sich besonders an behördliche Datenschutzbeauftragte, IT-Verantwortliche und Administratoren, die sich mit der Planung, dem Aufbau und dem Betrieb von drahtlosen Netzen befassen.

[20] Die Orientierungshilfe lag zum Zeitpunkt der Drucklegung noch nicht in verabschiedeter Fassung vor und wird mit ihrem Erscheinen unter www.datenschutz.sachsen.de veröffentlicht.

Außerdem informiert das BSI über drahtlose Kommunikation in der Broschüre „Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte“ (zu finden unter: http://www.bsi.bund.de/literat/doc/drahtloskom/index.htm).

14.2 Biometrische Merkmale in neuen Ausweispapieren

Die EU-Kommission hat bereits 2004 vorgeschlagen einheitliche EU-Pässe mit biometrischen Merkmalen zur Erhöhung der Fälschungssicherheit und damit auch zur Einschränkung von Missbrauch einzuführen.

Auch die Bundesregierung beabsichtigt biometrische Merkmale in Reisepässen (ab Herbst 2005) und in Personalausweisen (ab 2007) einzusetzen. Die rechtlichen Voraussetzungen dafür wurden durch Änderungen des Personalausweisgesetzes und des Passgesetzes sowie weiterer gesetzlicher Regelungen geschaffen. Über die datenschutzrechtlichen Anforderungen und Randbedingungen zur Nutzung biometrischer Merkmale in Ausweisen wurde bereits in 10/14.7 berichtet.

Hier soll nun über weitere Planungen zur Einführung einer computergestützten Identifizierung von Ausweisinhabern aus datenschutztechnischer Sicht informiert werden. Elektronische Pässe sollen nach den Empfehlungen der internationalen Zivilluftfahrtorganisation ICAO (International Civil Aviation Organization), der EU und der Bundesregierung folgende biometrische Verfahren nutzen: Gesichts-, Fingerabdruck- und Iriserkennung. Die Bundesregierung hat die Gesichtserkennung als erstes biometrisches Merkmal für ihre Ausweispapiere festgelegt. Als zweites biometrisches Merkmal soll später voraussichtlich die Fingerabdruckerkennung hinzugefügt werden.

Zur Gesichtserkennung soll das digitalisierte Passbild als Referenzdatei im RFID-Chip (Radio Frequency Identification) des Ausweises gespeichert werden. Entsprechend der EU-Verordnung (EG Nr. 2252/2004) vom Dezember 2004 werden RFID-Chips als Speichermedium für biometrische Merkmale vorgeschrieben. Außer dem Lichtbild dürfen auch die Unterschrift und weitere Angaben zur Person in verschlüsselter Form gespeichert werden.

Zur computergestützten Identifizierung von Ausweisinhabern müssen die im RFID-Chip gespeicherten biometrischen Daten mittels Chipkartenlesers gelesen werden. Diese Daten können elektronisch auf einer graphischen Oberfläche angezeigt und entweder manuell von einem Beamten mit der Person des Ausweisinhabers verglichen oder mit aktuellen Aufnahmen der Person in einem Hintergrundsystem elektronisch verglichen werden. Das Ergebnis des automatisierten Abgleichs kann richtig oder falsch sein. Somit kann die Identität der Person elektronisch bestätigt oder abgelehnt werden. Eine

„nicht identifizierte Person“ muss dann auf herkömmliche Weise, z. B. durch einen Grenzkontrollbeamten, identifiziert werden.

Eine datenschutzrechtliche Bewertung zum Einsatz biometrischer Merkmale in Ausweispapieren kann zurzeit nur die geplanten Sicherheitsmaßnahmen der Bundesregierung berücksichtigen, die den Antworten (Drucksachen des Deutschen Bundestages) auf „Kleine Anfragen“ zu biometrischen Daten in Ausweispapieren entnommen wurden.

Aus datenschutzrechtlicher Sicht ist die Speicherung biometrischer Daten in RFID-Chips (s. unter 16.2.8) problematisch. Bei der Funkkommunikation zwischen einem kontaktlosen Chipkartenleser und einem RFID-Chip könnten die übermittelten Daten in Abhängigkeit von der Sendeleistung auf der Funkstrecke im Abstand bis zu mehreren Metern mitgelesen und eventuell manipuliert werden. Die Funkwellen breiten sich nahezu unkontrolliert und unbegrenzt aus. Die Luftschnittstelle ist im Allgemeinen ungeschützt und öffentlich zugänglich. Daher muss eine unbefugte Kenntnisnahme von Ausweis-Daten durch Dritte verhindert werden. Dies kann durch eine ausreichend sichere Verschlüsselung der Daten während der Funkübermittlung erreicht werden. Um Fehler, Manipulationen bzw. die Unversehrtheit der übermittelten Daten erkennen zu können, müssen deren Authentizität und Integrität geprüft werden.

Die Bundesregierung hat zur Nutzung biometrischer Daten in Ausweispapieren folgende Zugriffsschutzmaßnahmen (BR-Drs. 15/4616 und 15/5018) vorgesehen. EU und ICAO schreiben Basic Access Control (BAC) als minimalen Zugriffsschutz für die gespeicherten digitalisierten Passbilddaten im RFID-Chip vor. Für dieses Sicherheitsverfahren muss zunächst die maschinenlesbare Zone des EU-Passes mittels optischen Lesers gelesen werden. Aus den optisch gelesenen Daten wird ein Zugriffsschlüssel berechnet. Danach erfolgt die Authentisierung des kontaktlosen Chipkartenlesegerätes gegenüber dem RFID-Chip und das Aushandeln eines dynamischen Sitzungsschlüssels (Triple-DES) zur verschlüsselten Kommunikation. Dadurch kann sichergestellt werden, dass ein unberechtigtes Entschlüsseln der abgehörten Daten nach derzeitigem Stand der Technik nicht möglich ist.

Die vorgesehenen Sicherheitsmaßnahmen dürften aber keinesfalls für die zweite Stufe des EU-Passes ausreichend sein, bei der Fingerabdrücke digital gespeichert werden sollen. Gegenüber dem Passbild ist der Fingerabdruck ein viel sensibleres personenbezogenes Datum. Die Bundesregierung will deshalb einen stärkeren Zugriffsschutz für diese Daten durch Extended Access Control (EAC) durchsetzen. Mit diesem Zugriffsschutz soll es möglich sein, dass nur befugte Stellen unter Mitwirkung des Passinhabers Zugang zu den im Chip gespeicherten Daten erhalten. Zusätzlich sind kryptographische

Algorithmen für digitale Signaturen und Verschlüsselung der Kommunikation festgelegt.

Für digitale Signaturen, die die Authentizität und Integrität der übermittelten Daten überprüfen können, sind RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm) und ECDSA (Elliptic Curve Digital Signature Algorithm) vorgesehen. Die Prüfung digitaler Signaturen setzt allerdings auch eine vorhandene PKI-Infrastruktur (Public-Key-Infrastructure) voraus. Dazu sind beispielsweise Organisationskonzepte zur Beantragung und Sperrung von Zertifikaten sowie das Vorhalten von Zertifikatslisten erforderlich.

Zum Schutz der Kommunikation zwischen kontaktlosem Chipkarten-Lesegerät und Ausweis soll als Verschlüsselungsalgorithmus 3DES (Triple-DES) genutzt werden und zur Authentisierung ein Message Authetication Code auf der Basis von DES (Data Encrytion Standard).

Die oben genannten kryptographischen Algorithmen sind allgemein als sicher anerkannt und können bei der Verwendung ausreichend sicherer Schlüssellängen als zuverlässig bewertet werden. Jedoch ist die Diskussion zur Realisierung von EAC noch nicht beendet.

Ein wichtiges Kriterium für den Einsatz der computergestützten Identifizierung von Ausweisinhabern ist eine sichere Wiedererkennung von Personen bzw. keine Falschzurückweisung berechtigter Personen durch die Kontrollsysteme. Nach einer Studie des BSI wird bei der Gesichtserkennung die Falschzurückweisung noch mit 8 bis 16 Prozent angegeben. Daher kann die elektronische Abgleichmethode momentan nur als unterstützendes Hilfsmittel genutzt werden. Aufwand und Nutzen stehen in keinem guten Verhältnis.

Auf der CeBIT 2005 wurde ein erstes Produkt zum Lesen zukünftiger elektronischer Ausweise vorgeführt. Im Auftrag des BSI wurde das Software-Applikations-Tool „Golden Reader Tool“ zum elektronischen Lesen von Ausweisen entwickelt. Es gewährleistet den Zugriffsschutz durch „Basic Access Control“. Zur Funktion der Software-Applikation sind neben einem kontaktlosen Smart Card Reader auch ein optischer Passport Reader erforderlich. Bevor die im RFID-Chip gespeicherten Daten gelesen werden können, muss die maschinenlesbare Zone des Ausweises optisch gelesen werden. Aus den Daten der optisch gelesenen Zone wird ein Zugriffsschlüssel (Access Key) zur sicheren Kommunikation zwischen Chipkarten-Leser und RFID-Chip berechnet. Danach werden die Daten über den gesicherten symmetrisch verschlüsselten Kanal aus dem RFID-Chip gelesen und anschließend auf ihre Authentizität und

Integrität überprüft. Ist die Signatur gültig, können die übermittelten Daten über eine graphische Oberfläche angezeigt und diese mit der Person des Ausweisinhabers verglichen werden.

Datenschutzgerecht ist, dass das Lesen der im Ausweis gespeicherten Daten nur mit Kenntnis des Ausweisinhabers möglich ist (z. B. optisches Lesen der maschinenlesbaren Zone). Kryptographische Verfahren können unbefugtes Abhören verhindern sowie Integrität und Authentizität der Daten bestätigen, sofern ausreichend sicher kryptograhische Algorithmen eingesetzt werden und nur befugte Stellen zugreifen können.

Die grundsätzlichen Fragen des Einsatzes biometrischer Merkmale sind noch offen. Die erst jüngst vom BfD geäußerten Bedenken und die darauf erfolgten Reaktionen legen beredtes Zeugnis davon ab. Hier werden organisatorische Weichen für die digitalisierte Erfassung aller Bürger gestellt.

Ich werde die weitere Entwicklung und den großflächigen Einsatz von computergestützten Identifizierungssystemen in Pässen und Ausweisen interessiert verfolgen und weiter darüber berichten.

14.3 Sicheres Löschen

Sowohl aus der Sicht des Datenschutzes als auch der IT-Sicherheit muss eine öffentliche Einrichtung sicherstellen, dass die Löschung von Daten ab einem bestimmten Schutzniveau vollständig und unumkehrbar erfolgt. Dazu habe ich mich schon in 3/14.7 geäußert. Dieses Thema ist aber stets aktuell, wie jüngste Vorkommnisse wiederholt belegen.

So hatte ein Mitarbeiter einer öffentlichen Einrichtung eines anderen Bundeslandes Festplatten ausgemusterter Rechner unberechtigterweise über eine Handelsplattform im Internet versteigert. Der erfolgreiche Bieter war über die (wieder herstellbaren) brisanten Inhalte, zu denen u. a. Alarmpläne, Namenslisten und Einsatzbefehle gehörten, erstaunt und wandte sich glücklicherweise an die zuständigen Polizeibehörden.

Der umfangreiche Problemkreis des sicheren Löschens von vertraulichen Daten erfordert die dauerhafte Sensibilisierung der verantwortlichen Entscheidungsträger und aller Mitarbeiter. Dabei spielt die geeignete Information und Schulung der Mitarbeiter eine wichtige Rolle, um die Kenntnisse der Beteiligten dabei auf dem aktuellen Stand der Technik zu halten. In diesem Zusammenhang möchte ich auf die Orientierungshilfe

„Sicheres Löschen“ des Arbeitskreises Technik[21] hinweisen, die die Problematik des Löschens und der Wiederherstellbarkeit von auf magnetischen Datenträgern gespeicherten Daten umfangreich beschreibt, aber auch auf verfügbare Werkzeuge für das dauerhafte Löschen unter Windows und Linux eingeht.

In dieser Hinsicht ist auch erneut darauf hinzuweisen, dass Informationen nicht nur in den vom jeweiligen Benutzer angelegten Dateien, sondern auch in automatischen Sicherheitskopien, Dateiversionen (durch moderne OFFICE- Programme wie z. B. WORD) sowie auch durch Systemdienste des Betriebssystems im Ordner TEMP/TMP auf der Festplatte dauerhaft abgespeichert werden.

So bieten aktuelle Textverarbeitungsprogramme automatische Speicherungen der aktuell bearbeiteten Dokumente an, die z. B. bei Fehlfunktionen wie Systemabstürzen nicht ebenso automatisch wieder gelöscht werden. Da diese Daten oftmals nicht im Blick der Anwender liegen, bleiben derartige Datenreste häufig auf Festplatten bestehen.

Nicht zu unterschätzen ist auch die „Merkfähigkeit“ von WORD. Je nach Konfiguration enthalten Word-Dokumente auch den Namen des Autors, den Speicherort und vor allem Veränderungen am Inhalt der jeweiligen Datei. Werden solche Dateien elektronisch versendet, kann der versierte Empfänger mit wenigen Handgriffen die Entstehung des Dokumentes wieder am Bildschirm sichtbar machen. Aus datenschutztechnischer Sicht können davon sensible Daten betroffen sein, die der Autor zwar wissentlich entfernt hatte, die jedoch durch die Funktionen der Änderungsnachverfolgung wieder sichtbar gemacht werden können.

Die meisten in diesem Zusammenhang relevanten Einstellungen lassen sich ausschalten. Jedoch bedarf es aus meiner Sicht einer konkreten Information und Regelung für die Mitarbeiter, deren Einhaltung auch durchgesetzt werden muss. Grundsätzliche Lösungsansätze bestehen darin, die Änderungsnachverfolgung auszuschalten, Dokumente vor der Fertigstellung unter anderem Namen erneut abzuspeichern und ggf. dabei ein anderes standardisiertes Format wie .RTF oder .PDF zu wählen.

Aus aktuellem Anlass weise ich darauf hin, dass das Schwärzen von Textpassagen in Textverarbeitungsprogrammen nicht den gewünschten Erfolg bringt, wenn lediglich Vorder- und Hintergrundfarbe auf schwarz eingestellt werden. Auch wenn anschließend eine Formatumwandlung zu einem PDF-Dokument vorgenommen wird, bleiben die Textinformationen erhalten und können mit einfachen Mitteln wieder entnommen und

[21] Http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationsmaterial/informations-technik/sicheres-loeschen-pdf,property=source.pdf.

in beliebigen Texteditoren sichtbar gemacht werden. Eine Analogie zum Schwärzen von Papierdokumenten ist also bei elektronischen Dokumenten nicht gegeben. Soll dennoch eine Schwärzung in einem elektronischen Dokument dargestellt werden, ist im Original die relevante Information tatsächlich zu entfernen und an deren Stelle ein entsprechender Platzhalter einzufügen.

Ein weiteres und nach meiner Erfahrung in der Praxis noch nicht ausreichend bewusst wahrgenommenes Problem ist der Umgang mit permanenten magnetischen Datenspeichern in Geräten der heutigen Büroausstattung. In modernen Fax-Geräten, komfortablen Netzwerkdruckern oder multifunktionalen Kopiergeräten sind heute oftmals Festplatten eingebaut, die zur Zwischenspeicherung von Aufträgen dienen. Bedenklich ist dabei, dass die in diesen Geräten eingesetzten Betriebssysteme in der Regel keine sicheren Löschfunktionen implementiert haben. Werden Druck- oder Faxaufträge zu ihrer Verarbeitung auf den eingebauten Festplatten zwischengespeichert, so werden diese Daten nach erfolgreicher Auftragserledigung zwar gelöscht, jedoch nicht physisch, sondern nur der Verweis auf die Datensektoren in der so genannten FileAllocationTable (FAT), ähnlich dem PC. Verlassen diese Festplatten im Rahmen der Reparatur oder eines Gerätewechsels die öffentliche Einrichtung, so können verbliebene Datenfragmente mit geringem Aufwand in lesbare Dateien zurückverwandelt werden. Die dazu notwendigen Werkzeuge sind im Internet frei verfügbar.

Ich habe verschiedene Kopiererhersteller dazu um Stellungnahme gebeten. Die Rückantworten haben die oben beschriebenen Möglichkeiten bestätigt, gleichzeitig aber auch aufgezeigt, dass das Problem bei den Herstellern inzwischen aufgegriffen wurde. Zur Abhilfe werden spezielle Optionen angeboten, die gelöschte Aufträge durch mehrmaliges Überschreiben mit verschiedenen Bitmustern dauerhaft gegen Wiederherstellung schützen. Auch besteht nach meinem Eindruck die generelle Bereitschaft, den Verbleib derartiger Festplatten in der öffentlichen Einrichtung vertraglich zu regeln oder auf Wunsch vor der Entnahme eine gemeinsame sog. Low-Level-Formatierung durchzuführen.

Mir ist wichtig, dass dieses Problem wahrgenommen wird, bevor sicherheitskritische Informationen oder datenschutz-relevante Inhalte auf diesem Wege in die Öffentlichkeit gelangen.

14.4 Digitalfunk in Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Mit Abschluss des Schengener Abkommens verpflichtete sich auch die Bundesrepublik Deutschland, die Möglichkeiten für die Errichtung eines einheitlichen Sprech- und Datenfunksystems für Sicherheitsbehörden (BOS-Funk) zu prüfen.

Dazu lagen die Anforderungen an ein derartiges Netz seit Februar 2004 mit den sogenannten „Gemeinsamen Anforderungen an das BOS Digitalfunknetz“ (GAN-Standard) vor, wobei die Umsetzung aufgrund der ungeklärten Finanzierung in der Folge fraglich erschien. Seit März 2005 hat das in Gang zu setzende Verfahren neue Konturen bekommen, indem sich der Bund auf die Errichtung eines Rumpfnetzes mit Erweiterungsmöglichkeiten durch die Bundesländer festgelegt hat.

Ich habe Konzeption und Stand der Umsetzung mit den Mitgliedern der für Sachsen zuständigen Arbeitsgruppe der Polizei zuletzt im Januar 2005 besprochen. Nach meinem Eindruck haben die beteiligten Stellen die datenschutzseitigen Belange dieser grundlegenden Technologieumstellung im Blick. Unabhängig davon werde ich die konkrete Umsetzung in Sachsen und damit den datenschutzgerechten Einsatz der angestrebten neuen Leistungsmerkmale auch in Zukunft begleiten.

14.5 Vorabkontrollen

Das Sächsische Datenschutzgesetz fordert für spezielle automatisierte Verfahren, die mit besonderen Risiken für das Recht auf informationelle Selbstbestimmung Betroffener verbunden sein können, Vorabkontrollen (§ 10 Abs. 5 SächsDSG). Bei diesen Kontrollen sind die Zulässigkeit der Datenverarbeitung und die vorgesehenen personellen, technischen und organisatorischen Maßnahmen nach § 9 SächsDSG zu prüfen. Dabei ist zu untersuchen, ob bei der Datenverarbeitung das Recht auf informationelle Selbstbestimmung gefährdet wird oder das noch bestehende Restrisiko hinnehmbar ist.

Ich begrüße diese Maßnahme. Sie ersetzt allerdings nicht die Notwendigkeit, bereits im Vorfeld bei der Planung von Verfahren datenschutzrechtliche Belange ausreichend zu berücksichtigen (10/14.1 Datenschutzgerechte Gestaltung von IT-Produkten).

Diese Vorabkontrollen sind vor dem erstmaligen Einsatz der automatisierten Verfahren oder bei deren wesentlichen Änderungen durchzuführen. Kennzeichen für „wesentliche Änderungen“ sind beispielsweise das Hinzufügen von neuen sensiblen Datenarten (z. B. Daten über Gesundheit, Sexualleben, ethnische Herkunft) oder von zusätzlichen Datenübermittlungen oder automatisierten Abrufen von Daten. Sofern nur die eingesetzte

Hardware oder das Betriebssystem geändert wird, stellt dies noch keine wesentliche Änderung dar.

Kontrolleur ist der Sächsische Datenschutzbeauftragte bzw. der Datenschutzbeauftragte einer öffentlichen Stelle, falls dieser gemäß § 11 SächsDSG bestellt ist.
Zu den zu kontrollierenden Verfahren gehören *automatisierte Abrufverfahren gemäß § 8 SächsDSG*. Bei einem Abrufverfahren wird von mindestens zwei Daten verarbeitenden Stellen ein gemeinsam betriebenes Verfahren eingerichtet, durch das die abrufende Stelle personenbezogene Daten aus einer Datei der bereithaltenden Stelle abrufen kann. Da die bereithaltende (übermittelnde) Stelle die Zulässigkeit der Übermittlung vor dem Abrufen nicht prüfen kann, ist die abrufende Stelle für die Zulässigkeit und Sicherheit der Abrufe verantwortlich. Wegen der besonderen Gefährdung für das Persönlichkeitsrecht des Betroffenen sind vor der Einführung von Abrufverfahren die Notwendigkeit und besonders die damit verbundenen Risiken zu prüfen.

Die Abwägung muss die Schutzwürdigkeit der Daten, den Verwendungszweck und den Empfängerkreis (Missbrauchsgefahr) berücksichtigen. Außerdem muss geprüft werden, ob ein besonderer Grund für eine jederzeitige und schnelle Datenübermittlung besteht und die erwartete Anzahl von Anfragen die Einführung eines automatisierten Abrufverfahrens rechtfertigt. Die bereithaltende Stelle hat als „Herrin der Daten“ sicherzustellen, dass die Zulässigkeit der Übermittlung personenbezogener Daten zumindest stichprobenweise überprüft werden kann (§ 8 Abs. 2 Satz 4 SächsDSG). Ausreichend ist in der Regel eine Protokollierung nach festen oder zufälligen Auswahlkriterien. Die Protokollauswertungen sollten zeitnah erfolgen, um auf Missbrauchsversuche zügig reagieren zu können. Der Abwägungsprozess muss sicherstellen, dass das Recht auf informationelle Selbstbestimmung in ausreichendem Maße gewährleistet wird.

Für automatisierte Verfahren, die besonders sensible personenbezogene *Daten im Sinne von § 4 Abs. 2 SächsDSG verarbeiten*, sind Vorabkontrollen gesetzlich vorgeschrieben. Zu diesen Daten gehören:
- Daten über rassische oder ethnische Herkunft,
- politische Meinung,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit und
- Daten über Gesundheit oder Sexualleben.

Das Datenschutzrecht sieht nun für diese Arten von personenbezogenen Daten ein besonderes Schutzniveau vor. Dieses ist bei der Zulässigkeitsprüfung zu beachten. Eine automatisierte Datenverarbeitung darf nur eingeführt werden, wenn den erheblichen Gefahren für das Persönlichkeitsrecht durch ausreichend starke Schutzmaßnahmen ent-

gegen gewirkt werden kann und das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist.

Darüber hinaus sind Vorabkontrollen vor dem erstmaligen Einsatz oder wesentlichen Änderungen für automatisierte Verfahren, in denen *Daten von Beschäftigten im Sinne des § 37 SächsDSG* verarbeitet werden, vorgeschrieben. Die öffentliche Stelle darf Daten von Beschäftigten nur verarbeiten, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen *zwingend* erforderlich ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

Automatisierte Verfahren zur Verarbeitung von Beschäftigtendaten sind beispielsweise Personalinformationssysteme, elektronische Arbeitszeiterfassung, Telefon-Gesprächsdatenverarbeitung und elektronische Zutrittssysteme. Für diese Verfahren sind die Zulässigkeit der Datenverarbeitung und die vorgesehenen personellen, technischen und organisatorischen Maßnahmen nach § 9 SächsDSG zu prüfen und zu beurteilen, ob das verbleibende Restrisiko bei der Verarbeitung dieser Daten hinnehmbar ist oder die Gefährdung zu groß wäre.

Die Daten verarbeitende Stelle hat zur Prüfung der Zulässigkeit der Datenverarbeitung und der notwendigen Sicherheitsmaßnahmen die erforderlichen Unterlagen zur Verfügung zu stellen. Gesetzlich wird nicht geregelt, welche Unterlagen das im Einzelnen sind. Zur Beurteilung der Zulässigkeit der Datenverarbeitung, der Sicherheitsmaßnahmen und der Risikoabwägung sind mindestens:

- Verfahrensbeschreibungen bzw. Benutzer-Handbücher,
- Datenfeldbeschreibungen mit Angaben zur Rechtsgrundlage der Verarbeitung,
- Datenübermittlungen einschließlich Rechtsgrundlagen,
- Dokumentation zulässiger Auswertungen,
- Gewährleistung von Rechten der Betroffenen (Auskunft, Berichtigung, Löschung, Sperrung),
- differenzierte Vergabe von Zugriffsrechten (Benutzerprofile) für Mitarbeiter,
- ausreichend sichere Passwortverfahren oder andere Authentifikationsverfahren (Chipkarte, PIN),
- Protokollierung, Log-Auswertungen (Fehlanmeldungen - Missbrauchsversuche),
- Löschungs- und Sperrungsfristen für die zu verarbeitenden Daten,
- regelmäßige Backups von Programmen und Daten,
- vertragliche Regelungen zur Auftragsdatenverarbeitung bzw. Wartung (Weisungsbefugnisse, ausreichend sichere Maßnahmen gemäß § 9 SächsDSG, Kündigung bei Datenschutzverstößen, Unterauftragnehmer nur mit Zustimmung des Auftraggebers),
- Überwachung von Administrations- und Wartungsarbeiten,

- Datenschutz- und Datensicherheitskonzepte für das zu prüfende Verfahren gemäß § 9 Abs. 2 SächsDSG und
- weitere Regelungen zum datenschutzgerechten Umgang mit personenbezogenen Daten bereit zu stellen.

Zur Beurteilung der Sicherheitsmaßnahmen sind vor allem konkrete Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz für das automatisierte Verfahren zu treffen. Besondere Anforderungen sind dabei auch:

- an die Einsatzumgebung der Datenverarbeitung (räumliche Sicherheit),
- die Art der Netzwerke,
- Speicherorte und
- die Übermittlungswege

zu stellen.

Zur Risikoabwägung sind auch Gefährdungen, die sich aus dem zunehmenden Einsatz von drahtlosen Netzwerken in der öffentlichen Verwaltung ergeben, zu beachten. Der Aufbau kabelloser Netze (s. unter 14.1) oder die Anbindung von Peripheriegeräten mittels Funkkommunikation ermöglichen das Abhören, Kopieren und Manipulieren von Daten in Abhängigkeit von Umweltbedingungen und Sendeleistung. Die Reichweiten können zwischen 10 m bis 100 m betragen. Passwörter oder andere sensible Daten könnten mitgehört werden, falls keine ausreichend sichere Verschlüsselung genutzt wird.

Unverschlüsselte Übermittlungen von sensiblen personenbezogenen Daten über das Internet, per E-Mail, Datenträger oder mittels kontaktloser Chipkarten sind nicht zulässig, weil weder Vertraulichkeit noch Integrität oder Authentizität gewährleistet werden könnten.

Die Speicherung sensibler personenbezogener Daten sollte möglichst auf einem gesicherten Server verschlüsselt erfolgen, weil dort die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Revisionsfähigkeit der Daten besser als bei einem Arbeitsplatzrechner gewährleistet werden kann. Zur Speicherung ungeeignet sind vor allem mobile Geräte, wie Laptop oder Notebook, die durch Verlust oder Diebstahl besonders risikobehaftet sind.

Ist das Restrisiko zu hoch, muss geprüft werden, ob durch eine Nachbesserung technischer oder organisatorischer Maßnahmen eine datenschutzgerechte Verarbeitung ermöglicht werden könnte. Ist das nicht der Fall, kann das Verfahren nicht eingeführt oder geändert werden.

Das Ergebnis der Prüfung ist der Daten verarbeitenden Stelle in der Regel innerhalb eines Monats mitzuteilen.

15 Vortrags- und Schulungstätigkeit für behördliche Datenschutzbeauftragte

Das Bedürfnis nach Vorträgen zum Datenschutz und zur Datensicherheit hat unvermindert angehalten. Soweit die Arbeitsbelastung dies zuließ, hat meine Behörde diesem entsprochen.

Nachdem mittlerweile über 200 Datenschutzbeauftragte öffentlicher Stellen gemäß § 11 SächsDSG bestellt wurden, werde ich künftig speziell für diese Schulungen durchführen. Dabei sollen neben Grundsatzfragen zum Recht auf informationelle Selbstbestimmung insbesondere fachspezifische Schwerpunkte thematisiert werden. Ich würde mich hierzu über Anregungen aus dem Kreis der behördlichen Datenschutzbeauftragten freuen.

Ich weise aber ausdrücklich darauf hin, dass die durch mich durchgeführten Schulungen nur als Ergänzung der gemäß § 11 Abs. 2 Satz 4 SächsDSG regelmäßig durchzuführenden Fortbildungen durch die bestellende öffentliche Stelle anzusehen sind (vgl. dazu 2.1 meiner Bekanntmachung zu Datenschutzbeauftragten öffentlicher Stellen vom vom 11. März 2004, aktualisiert am 12. September 2005).

Weiterhin beabsichtige ich, für die Datenschutzbeauftragten öffentlicher Stellen im Rahmen meines Internetangebots ein internes Forum einzurichten. In diesem wird eine geschlossene Benutzergruppe spezielle Fragen und Probleme untereinander diskutieren können. Eine Freischaltung wird nach Schaffung der technischen und organisatorischen Voraussetzungen erfolgen.

16 Materialien

16.1 Bekanntmachungen

16.1.1 Bekanntmachung des Sächsischen Datenschutzbeauftragten zum Verzeichnis automatisierter Verarbeitungsverfahren (§ 10 SächsDSG)

vom 11. März 2004
aktualisierte Fassung vom 12. September 2005

I Führung eines Verfahrensverzeichnisses

Nach § 10 Abs. 1 Satz 1 des Sächsischen Datenschutzgesetzes (SächsDSG) hat jede Daten verarbeitende Stelle ein Verzeichnis über die bei ihr eingesetzten automatisierten Verarbeitungsverfahren zu führen.

Datenverarbeitende Stelle (innerhalb des in § 2 SächsDSG definierten Anwendungsbereichs) ist jede öffentliche Stelle i. S. v. § 2 Abs. 1 und 2 SächsDSG, die personenbezogene Daten für sich selbst oder für Dritte verarbeitet oder durch Dritte verarbeiten lässt (vgl. § 3 Abs. 3 SächsDSG). „Stellen“ sind dabei Verwaltungseinheiten, die gesetzlich zugewiesene, datenschutzrechtlich zweckbestimmt abgeschottete Aufgaben erfüllen (funktionale Stelle). In einer - im organisatorischen Sinn einheitlichen - Gemeindeverwaltung sind beispielsweise Meldeamt und Personalamt jeweils Stellen im funktionalen Sinn.

Verarbeitung i. S. d. Gesetzes ist das Erheben, Speichern, Verändern, Anonymisieren, Übermitteln, Nutzen, Sperren und Löschen personenbezogener Daten (vgl. § 3 Abs. 2 SächsDSG). Eine automatisierte Verarbeitung personenbezogener Daten liegt nach § 3 Abs. 5 SächsDSG vor, wenn diese durch den Einsatz eines elektronischen Datenverarbeitungssystems (Rechner und Software) programmgesteuert durchgeführt wird. Ein automatisiertes Verfahren ist die Gesamtheit der einzelnen automatisierten Verarbeitungen mit einem bestimmten Verwendungszweck.

Die Pflicht zum Führen des Verfahrensverzeichnisses entsteht dort, wo das Verfahren eingesetzt wird. Der Spezialfall des § 8 Abs. 3 SächsDSG bei automatisierten Abrufverfahren ist zu beachten. Gerichte führen die Verzeichnisse nur in Justizverwaltungsangelegenheiten (§ 10 Abs. 2 SächsDSG); ihre Recht sprechende Tätigkeit ist ausgenommen.

Für Verfahren i. S. v. § 10 Abs. 4 SächsDSG (zur Unterstützung allgemeiner Bürotätigkeit oder durch Rechtsvorschrift erstellte Register zur Information der Öffentlichkeit) ist ein Verzeichnis nicht zu führen.

Der bisherige Teil „Geräteverzeichnis“ ist entfallen, da er aufgrund der EG-Datenschutzrichtlinie nicht mehr erforderlich war und ein solches Geräteverzeichnis ohnehin i. d. R. andernorts - meist in der IT-Abteilung - geführt wird.

II Inhaltliche Erläuterungen zum Verfahrenverzeichnis

Es wird empfohlen, für die Beschreibungen das in der Anlage zu dieser Bekanntmachung abgedruckte Muster zu verwenden. Für jedes Verfahren ist ein gesondertes Datenblatt anzulegen. Beim Ausfüllen sollte beachtet werden:

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

Es ist die Stelle (im funktionalen Sinn) zu bezeichnen, bei der die Verarbeitung erfolgt (z. B. das Einwohnermeldeamt der Stadt). Wird das Verfahren von mehreren Stellen genutzt, ist - soweit möglich - eine zusammenfassende Bezeichnung anzugeben oder sind die Stellen einzeln zu nennen.

2. Bezeichnung des Verfahrens

Als Bezeichnung des Verfahrens ist der allgemein übliche oder ein möglichst „sprechender“ Begriff zu wählen. Darüber hinaus sollten Angaben zur eingesetzten Software (z. B. Bezeichnung, Version, Hersteller) gemacht werden.

3. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Es ist der Zweck der Datenverarbeitung zu beschreiben (z. B. Lohn- und Gehaltsabrechnung) sowie die entsprechende gesetzliche Ermächtigung. Einschlägige Rechtsgrundlagen sind eindeutig zu bezeichnen oder hinreichend zu beschreiben. Ist eine spezielle Norm zu nennen, ist diese in zitierfähiger Fassung (mit Fundstelle) anzugeben.

4. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Es sind die den betroffenen Personenkreis kennzeichnenden Merkmale aufzunehmen (z. B. „Wohngeldempfänger“, „Fahrerlaubnisinhaber“). Soweit sich der betroffene Personenkreis aus einem Verfahren im Sinne von § 10 SächsDSG ergibt (z. B. „Einwohnermeldekartei“), kann dieser Bezug verwendet werden. Weiterhin ist die Datenart (z. B. Meldedaten) ggf. unter Nennung der einzelnen Bestandteile des Datensatzes anzugeben (z. B. Personaldaten - Name, Vorname, akademischer Grad, Personalnummer, Familienstand etc.). Eine möglichst präzise Beschreibung ist erforderlich.

5. Empfänger und Art zu übermittelnder Daten

Es sind die zur Weitergabe an Dritte vorgesehenen Daten wie in Nr. 4 zu beschreiben (vgl. § 3 Abs. 4 SächsDSG). Zusätzlich ist der jeweilige Empfänger anzugeben. Ist der Empfänger eine einzelne Stelle oder Person, ist diese identifizierbar anzugeben; sind es mehrere (z. B. die Meldebehörden im Landkreis), genügt eine zusammenfassende Bezeichnung. Darüber hinaus ist die gesetzliche Ermächtigung zur Übermittlung der Daten anzugeben.

6. Beabsichtigte Übermittlung in Drittländer

Im Fall einer Übermittlung in Drittländer sind die Spezialvorschriften des § 17 SächsDSG zu beachten. Anzugeben sind hier der Empfänger, die Rechtsgrundlage und der Umfang der Übermittlung.

7. Regelfristen für die Löschung der Daten

Nach § 20 Abs. 1, 2 SächsDSG sind personenbezogene Daten zu löschen, wenn deren Speicherung unzulässig ist oder ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist - und die Löschung nicht aus den in § 20 Abs. 3, 4 SächsDSG aufgeführten Gründen zu unterbleiben hat. Aus datenschutzorganisatorischen Gründen sind hierfür Regelfristen vorzusehen.

8. Personelle, technische, und organisatorische Maßnahmen

Die gemäß § 9 SächsDSG getroffenen Kontrollmaßnahmen sind jeweils zu beschreiben. Dazu können ggf. vorhandene Datenschutzkonzepte und Dienstanweisungen vorgelegt werden. Dabei kann auf die Ausarbeitungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), z. B. IT-Grundschutzhandbuch, zurückgegriffen werden.

Soweit sich zu den Nummern 1 bis 8 Anlagen erforderlich machen, sind diese beizufügen.

III Mitteilungspflicht an den Sächsischen Datenschutzbeauftragten

Zu führen ist das Verzeichnis grundsätzlich bei der Stelle (im funktionalen Sinn), bei der die Verarbeitung stattfindet (§ 10 Abs. 1 Satz 3 SächsDSG). Jedoch ist es zweckmäßig und regelmäßig zu empfehlen, dass die Verzeichnisse bei der jeweiligen Behörde zentral zusammengeführt und sodann dem Sächsischen Datenschutzbeauftragten gebündelt übersandt werden.

Die Vorlage hat vor der erstmaligen Inbetriebnahme eines Verfahrens zu erfolgen (§ 10 Abs. 3 Satz 1 SächsDSG). Darüber hinaus ist das aktualisierte Verfahrensverzeichnis dem Sächsischen Datenschutzbeauftragten zum 1. März jeden Jahres zuzuleiten (§ 10 Abs. 3 Satz 2 SächsDSG). Auf die Übergangsvorschrift des § 40 Abs. 1 SächsDSG wird hingewiesen.

Eine Mitteilungspflicht entfällt, sofern ein Datenschutzbeauftragter nach § 11 SächsDSG bestellt ist (§ 10 Abs. 3 Satz 3, § 11 SächsDSG). Dann führt dieser das Verfahrensverzeichnis.

Dresden, den 12. September 2005
Der Sächsische Datenschutzbeauftragte
Schurig

Anlage

Verfahrensverzeichnis

**(Mitteilung und Beschreibung der Verfahren nach § 10 SächsDSG
für das Register beim Sächsischen Datenschutzbeauftragten nach § 31 SächsDSG)**

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Die Beschreibung wurde erstellt am:

Die Beschreibung wurde aktualisiert am:

Stempel, Datum, Unterschrift

Bitte ggf. Anlage(n) beifügen

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

2. Bezeichnung des Verfahrens

3. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Zweck	Rechtsgrundlage

4. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Personengruppe	Art der zu verarbeitenden Daten

5. Empfänger und Art zu übermittelnder Daten

Empfänger	Art der zu übermittelnden Daten

6. Beabsichtigte Übermittlung in Drittländer gemäß § 17 SächsDSG (Empfänger, Rechtsgrundlage und Umfang der Übermittlung)

7. Regelfristen für die Löschung der Daten

Art der Daten	Zeitraum

8. Personelle, technische und organisatorische Maßnahmen gemäß § 9 SächsDSG

Wie ist sichergestellt, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),

4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),

5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),

6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz)?

16.1.2 Bekanntmachung des Sächsischen Datenschutzbeauftragten zu Datenschutzbeauftragten öffentlicher Stellen (§ 11 SächsDSG)

vom 11. März 2004
aktualisierte Fassung vom 12. September 2005

1 Bestellung des Datenschutzbeauftragten

1.1 Ermessensentscheidung

Die Entscheidung über die Bestellung eines Datenschutzbeauftragten nach § 11 Abs. 1 Satz 1 SächsDSG ist durch die öffentliche Stelle selbst nach Ermessen zu treffen. Das Sächsische Datenschutzgesetz sieht für öffentliche Stellen (§ 2 Abs. 1 und 2 SächsDSG) keine Pflicht, sondern nur die Möglichkeit der Bestellung eines Datenschutzbeauftragten vor. In größeren Behörden und in Behörden mit Aufgabenvielfalt, d. h. wenn mehrere funktionale öffentliche Stellen im Sinne des Datenschutzgesetzes in einer Behörde "gebündelt" sind, sollten jedoch als unterstützende Maßnahme zur Gewährleistung des Datenschutzes im Sinne von § 9 SächsDSG Datenschutzbeauftragte bestellt werden.

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften und die Beachtung des Rechts auf informationelle Selbstbestimmung verbleibt aber auch bei Bestellung eines Datenschutzbeauftragten beim Leiter der öffentlichen Stelle.

1.2 Schriftliche Bestellung und hausinterne Bekanntmachung

Der Datenschutzbeauftragte wird durch ein förmliches an ihn gerichtetes Schreiben bestellt (§ 11 SächsDSG), das bei eigenen Beschäftigten zu den Personalakten zu nehmen ist. Die bloße Erwähnung in einem Geschäftsverteilungsplan genügt nicht.

Die Bestellung sollte allen Mitarbeitern bekannt gegeben werden (z. B. durch Hausmitteilung oder Aushang).

1.3 Persönliche Voraussetzungen (§ 11 Abs. 2 SächsDSG)

Der Datenschutzbeauftragte muss nicht Bediensteter der Stelle sein, § 11 Abs. 1 Satz 3 SächsDSG. Er ist als natürliche Person zu bestellen. In Fällen der Inanspruchnahme externer Dienstleister, die in Datenschutzfragen beraten und die als juristische Personen des Privatrechts auftreten, z. B. einer GmbH, ist ein Mitarbeiter persönlich zu benennen und zu bestellen.

Der Datenschutzbeauftragte muss zuverlässig und fachkundig sein. Sofern er über die fachlichen Qualifikationen (rechtliche und organisatorische Kenntnisse, Sicherheit im Umgang mit den einschlägigen Spezialvorschriften zum Persönlichkeitsschutz im eigenen Fachbereich und dem Sächsisches Datenschutzgesetz,

Grundkenntnisse in automatisierter Datenverarbeitung) noch nicht verfügt, muss ihm Gelegenheit gegeben werden, diese zu erwerben. Darüber hinaus hat sich der Datenschutzbeauftragte regelmäßig fortzubilden, um Kenntnis der neuen technischen Entwicklungen und der datenschutzrechtlichen Regelungen zu haben.

Der Datenschutzbeauftragte ist nach § 6 SächsDSG auf das Datengeheimnis und ggf. nach § 1 Verpflichtungsgesetz (bei Nicht-Amtsträgern) schriftlich zu verpflichten.

1.4 Inkompatibilität

Dem Datenschutzbeauftragten kommt gegenüber der Behörde, ggf. auch gegenüber Mitarbeitern und Betroffenen eine koordinierende und beratende - aber bis zu einem gewissen Grad auch eine intern kontrollierende - Funktion zu. Ist der Datenschutzbeauftragte ein Mitarbeiter und - wie zumeist - nebenamtlich tätig, sind daher mögliche Interessenkonflikte mit seinen Hauptaufgaben im Vorfeld auszuschließen. Insbesondere bei Bediensteten aus dem Bereich der Personalverwaltung, des Organisationswesens, der Datenverarbeitung oder des Personalrats ergeben sich regelmäßig Spannungsverhältnisse zur eigentlichen Hauptaufgabe. Unzulässig ist die Bestellung von Mitarbeitern in leitenden Funktionen, die in einem besonderen dienstlichen Näheverhältnis zum Leiter der Stelle/Behördenleiter stehen und deren Bestellung regelmäßig im Übermaß Interessenkonflikte hervorrufen würde (z. B. bei Stellvertretern des Leiters, Personalamtsleitern usw.). Dasselbe gilt auch für andere Funktionen, bei denen originär personenbezogene Daten verarbeitet werden, z. B. beim Vorsitzenden des Personalrats.

1.5 Bestellung eines Datenschutzbeauftragten für mehrere öffentliche Stellen

Nach § 11 Abs. 1 Satz 3 SächsDSG können mehrere öffentliche Stellen einen gemeinsamen Datenschutzbeauftragten bestimmen. Dabei ist zu beachten, dass das Sächsische Datenschutzgesetz vom funktionalen Stellenbegriff ausgeht. So verfügt z. B. eine Gemeinde über mehrere öffentliche Stellen im funktionalen Sinn; sie ist eine Bündelungsbehörde. In der schriftlichen Bestellung des Datenschutzbeauftragten ist dessen Aufgabenbereich daher präzise zu bestimmen.

Bsp.: Eine Großstadt verfügt über ihre Verwaltung, Eigenbetriebe, juristische Personen des Privatrechts und ein städtisches Krankenhaus. Für die Eigenbetriebe wird ein Datenschutzbeauftragter nach § 11 SächsDSG bestellt. Für das Krankenhaus wurde bereits ein Datenschutzbeauftragter nach dem Sächsischen Krankenhausgesetz (SächsKHG) bestellt. Der dritte Datenschutzbeauftragte wird für den Rest der Gemeindeverwaltung mit ihren zahlreichen funktionalen Stellen im Sinne des Sächsischen Datenschutzgesetzes bestellt. Die stadteigenen juristischen Personen des Privatrechts, die regelmäßig auch öffentliche Stellen nach § 2 Abs. 2 SächsDSG sind, verfügen über eigene oder einen gemeinsamen Datenschutzbeauftragten.

§ 11 Abs. 1 SächsDSG eröffnet auch die Möglichkeit, dass über die organisatorische Stelle hinaus mehrere Behörden einen gemeinsamen Datenschutzbeauftragten bestellen.

1.6 Berufung eines Vertreters des Datenschutzbeauftragten

Die Bestellung eines Stellvertreters des Datenschutzbeauftragten findet keine gesetzliche Stütze. Der Datenschutzbeauftragte ist Vertrauensperson der Mitarbeiter (vgl. § 11 Abs. 4 SächsDSG) und nimmt seine Aufgaben höchstpersönlich wahr. Ein Vertreter kann den Datenschutzbeauftragten daher nicht mit sämtlichen im Gesetz vorgesehenen Wirkungen vertreten.

Ausgeschlossen ist nach dem Gesetzeswortlaut auch die Bestellung mehrerer Datenschutzbeauftragter für eine öffentliche Stelle im funktionalen Sinn.

Zulässig ist hingegen, dass der Datenschutzbeauftragte über Mitarbeiter verfügt, die ihm zuarbeiten und unterstützende Hilfstätigkeiten erledigen. Verarbeiten diese Mitarbeiter personenbezogene Daten, so ist dabei zu beachten, dass insbesondere die Schweigepflicht nach § 11 Abs. 4 SächsDSG nur für den Datenschutzbeauftragten selbst normiert ist.

1.7 Bisherige behördliche Datenschutzbeauftragte

Bedienstete, die bis zum Inkrafttreten des novellierten Sächsischen Datenschutzgesetzes mit Aufgaben des internen Datenschutzes betraut waren, müssen im Fall der Weiterführung dieser Aufgaben

- eine klarstellende Ergänzung ihrer Bestellung erhalten, wonach sie als Datenschutzbeauftragte nach § 11 Abs. 1 Satz 1 SächsDSG bestellt sind oder

- es muss verdeutlicht werden, dass sie kein Datenschutzbeauftragter im Sinne von § 11 Abs. 1 Satz 1 SächsDSG sein sollen, etwa dann, wenn andere oder weniger Aufgaben, Pflichten und Rechte mit der Funktion verbunden sind.

Ein solcher Klarstellungsbedarf entfällt z. B. bei den nach § 33 Abs. 8 SächsKHG bestellten Datenschutzbeauftragten. Die Vorschrift verweist auf eine frühere Fassung des Bundesdatenschutzgesetzes (BDSG in der Fassung vom 20. Dezember 1990) und ist eine speziellere Datenschutzvorschrift im Sinne von § 2 Abs. 4 SächsDSG. Für die Krankenhäuser als öffentliche Stellen erfolgen somit keine Bestellungen nach § 11 Abs. 1 SächsDSG, sondern nach dem Sächsischen Krankenhausgesetz. Entsprechendes gilt für andere Spezialgesetze, die die Bestellung von Datenschutzbeauftragten zum Inhalt haben.

1.8 Mitteilung über die Bestellung an den Sächsischen Datenschutzbeauftragten

Nach § 11 Abs. 1 Satz 6 SächsDSG ist der Sächsische Datenschutzbeauftragte innerhalb eines Monats von der Bestellung zu unterrichten. Die Meldung muss Folgendes enthalten:

- Vor- und Zuname des Datenschutzbeauftragten (§ 11 Abs. 1 Satz 7),
- Tag der Bestellung (§ 11 Abs. 1 Satz 7),
- sofern mehrere funktionale Stellen umfasst sind, für welche Stellen der Datenschutzbeauftragte zuständig sein soll.

Dies kann durch die Übersendung des Bestellungsschreibens, das die vorgenannten Angaben enthalten muss, an den Sächsischen Datenschutzbeauftragten geschehen. Ferner ist es wegen § 11 Abs. 2 Satz 1 SächsDSG zweckmäßig anzugeben, welche weiteren Funktionen der Datenschutzbeauftragte bei der Stelle ausübt. Ein entsprechendes Formular ist in der Anlage enthalten.

In allen Fällen, in denen keine Mitteilung erfolgt, geht der Sächsische Datenschutzbeauftragte davon aus, dass kein Datenschutzbeauftragter im Sinne von § 11 SächsDSG bestellt worden ist.

Mitteilungspflichtig sind alle sächsischen Behörden und Stellen im Sinne von § 2 Abs. 1 und 2 SächsDSG. Juristische Personen des Privatrechts (Stiftungen, Vereine, GmbH´s, AG´s usw.) sind Stellen im Sinne von § 2 Abs. 2 SächsDSG, wenn sie öffentliche Aufgaben wahrnehmen und wenn öffentliche Stellen im Sinne von § 2 Abs. 1 SächsDSG die juristische Person mehrheitlich beherrschen. Die juristische Person des Privatrechts muss dabei nicht mehrheitlich von *einer* öffentlichen Stelle beherrscht werden.

Ausgenommen von der Mitteilungspflicht sind lediglich die in § 2 Abs. 3 SächsDSG genannten öffentlich-rechtlichen Unternehmen.

2 Gesetzliche Aufgaben und Befugnisse

2.1 Gesetzliche Aufgaben

Mit der Neufassung des Datenschutzgesetzes wird die Datenschutz-Selbstkontrolle der öffentlichen Stellen durch Datenschutzbeauftragte gestärkt. Die nach § 11 Abs. 1 Satz 1 SächsDSG bestellten Datenschutzbeauftragten

a) überwachen die Einhaltung der Datenschutzvorschriften bei der Planung, vor der Einführung von und während der Anwendung automatisierter Verfahren (§ 11 Abs. 3 Nr. 1 SächsDSG),

b) geben Hinweise an andere Mitarbeiter in Datenschutzfragen (§ 11 Abs. 3 Nr. 2 SächsDSG),

c) führen das Verzeichnis automatisierter Verarbeitungsverfahren (§ 11 Abs. 3 Nr. 3 SächsDSG),

d) prüfen nach § 11 Abs. 3 Nr. 4 SächsDSG in Vorabkontrollen die in ihren Stellen vorgesehenen

- automatisierten Abrufverfahren nach § 8 SächsDSG (vgl. § 10 Abs. 5 Nr. 1 SächsDSG),
- automatisierten Verfahren, in denen sensible Daten im Sinne von § 4 Abs. 2 SächsDSG verarbeitet werden (vgl. § 10 Abs. 5 Nr. 2 SächsDSG) oder
- automatisierten Verfahren, in denen Beschäftigtendaten im Sinne von § 37 SächsDSG verarbeitet werden (vgl. § 10 Abs. 5 Nr. 3 SächsDSG),

e) geben Auskunft zum Verfahrensverzeichnis (§ 10 Abs. 1 SächsDSG) nach § 11 Abs. 3 Nr. 5 SächsDSG,

f) werden in Einzelfällen bei Anrufung durch Betroffene oder andere Beschäftigte tätig (vgl. § 11 Abs. 4 SächsDSG).

In Zweifelsfällen kann sich der Datenschutzbeauftragte an den Sächsischen Datenschutzbeauftragten wenden.

Weitere (datenschutzorganisatorische) Aufgaben können dem Datenschutzbeauftragten von seinem Vorgesetzten im Rahmen der gesetzlichen Möglichkeiten übertragen werden. Dem Datenschutzbeauftragten sollten jedoch für eine effektive Aufgabenerfüllung weitere konkretisierte Handlungsbefugnisse durch interne Organisationsverfügung oder eine Stellenbeschreibung, die die im Gesetz festgelegte Weisungsfreiheit betont, verliehen werden. Insbesondere sollte dem Datenschutzbeauftragten zugestanden werden, dass

- Beschäftigte Auskunft auf seine Fragen zu geben haben,

- ihm Einsicht in Akten, Dateien und sonstige Unterlagen gewährt wird, wenn im Einzelfall oder aus grundsätzlichen Erwägungen Datenschutzprobleme zu klären sind (siehe auch 2.2),

- er das Recht hat, Stellungnahmen innerhalb der Dienststelle einzuholen,

- er über die Möglichkeit verfügt, der Behördenleitung direkt und zeitnah vorzutragen.

Darüber hinaus kann der Datenschutzbeauftragte bei automatisierten Verfahren, bei denen personenbezogene Daten verarbeitet werden, auch über den in § 10 Abs. 5 SächsDSG vorgegebenen Katalog hinaus generell einbezogen werden.

Dem Datenschutzbeauftragten sollte die erforderliche Arbeitszeit und Fortbildung zur Erfüllung seiner Aufgaben, auch neben seinen Hauptaufgaben, gewährt werden. Die Fachbereiche müssen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben unterstützen (vgl. § 11 Abs. 2 Satz 4 SächsDSG).

Im Hinblick auf seine Tätigkeit dürfen dem Datenschutzbeauftragten berufliche Nachteile weder drohen noch entstehen, § 11 Abs. 2 Satz 3 SächsDSG. Dies ist Ausdruck seiner Stellung als weisungsfreier Beauftragter.

Er ist als bestellte Vertrauensperson auch nach der Beendigung seiner Tätigkeit zur Verschwiegenheit verpflichtet, § 11 Abs. 4 Satz 1 SächsDSG.

2.2 Befugnisse zur Verarbeitung personenbezogener Daten

Der Datenschutzbeauftragte hat nach dem Gesetz zunächst allgemeine und datenschutzorganisatorische Aufgaben (vgl. § 11 Abs. 3 SächsDSG). Er hat aber keine unbeschränkten Kontrollbefugnisse innerhalb der von ihm beratenen Stelle. Selbst die in § 11 Abs. 2 Satz 2 SächsDSG normierte Weisungsfreiheit berechtigt ihn nur zur Erfüllung seiner gesetzlich in § 11 SächsDSG beschriebenen Aufgaben. Im Rahmen seiner Aufgabenerfüllung hat sich der Datenschutzbeauftragte somit streng am Erforderlichkeitsgrundsatz zu orientieren. Insofern sind seine Möglichkeiten zur Einsichtnahme in Datenverarbeitungsvorgänge mit Personenbezug beschränkt. Dies gilt insbesondere für Daten, die einem Berufsgeheimnis oder einem besonderen Amtsgeheimnis unterliegen. Nach § 11 Abs. 4 SächsDSG kann der Datenschutzbeauftragte tätig werden, wenn sich betroffene Beschäftigte in konkreten Einzelfällen an ihn wenden und um Unterstützung bitten. In diesem Fall kann er auf Grundlage der Einwilligung des Betroffenen die erforderliche Einsicht in Akten, Dateien und sonstige Unterlagen, die personenbezogene Daten des betroffenen Mitarbeiters enthalten, vornehmen.

Dresden, den 12. September 2005
Der Sächsische Datenschutzbeauftragte
Schurig

Anlage

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Ort, Datum

Aktenzeichen

Mitteilung über die Bestellung eines Datenschutzbeauftragten nach § 11 Sächsisches Datenschutzgesetz

Bezeichnung der Stelle	Anschrift der Stelle

Name des Datenschutzbeauftragten (akademischer Grad, Vorname, Name):
……

Datum der Bestellung (laut Urkunde): ……

☐ eingeschränkter Zuständigkeitsbereich[1]
……
……
……

☐ erweiterter Zuständigkeitsbereich (z.B. kommunale Eigenbetriebe)[1]
……
……
……

☐ externer Datenschutzbeauftragter (§ 11 Abs. 1 Satz 4 SächsDSG)

Anschrift: ……

☐ Beschäftigter einer öffentlichen Stelle

sonstige berufliche Aufgaben (§ 11 Abs. 2 Satz 1 SächsDSG)[2]: ……

Telefonnummer	Fax	E-Mail-Adresse

☐ Abschrift der Bestellungsurkunde ist beigefügt.

……
(Name und Funktion des Erklärenden)

……
(Ort, Datum) (Dienststempel) (Unterschrift des Erklärenden)

[1] Soweit der Zuständigkeitsbereich des Datenschutzbeauftragten nicht deckungsgleich mit der öffentlichen Stelle (im organisatorischen Sinne) ist, sind Abweichungen –gegebenenfalls in Anlage - zu beschreiben.
[2] Gem. § 11 Abs. 2 Satz 1 SächsDSG darf ein Datenschutzbeauftragter nur bestellt werden, wenn durch die Bestellung kein Interessenkonflikt mit seinen sonstigen beruflichen Aufgaben entsteht.

16.1.3 Bekanntmachung des Sächsischen Datenschutzbeauftragten zur Vorabkontrolle gemäß § 10 Abs. 5 Sächsisches Datenschutzgesetz (SächsDSG)

vom 12. September 2005

I. Anwendungsbereich

Wann kommt eine Vorabkontrolle in Betracht? Eine Vorabkontrolle ist durchzuführen, wenn entweder

1. ein automatisiertes Abrufverfahren (§ 8 SächsDSG)
2. ein automatisiertes Verfahren zur Verarbeitung besonders schützenswerter Daten (§ 4 Abs. 2 SächsDSG) oder
3. ein automatisiertes Verfahren zur Verarbeitung von Beschäftigtendaten (§ 37 SächsDSG)

erstmals eingesetzt oder wesentlich geändert werden soll.

II. Zuständigkeit und Mitwirkungspflichten

Wer führt die Vorabkontrolle durch? Ist für die *öffentliche* Stelle (i. S. v. § 2 Abs. 1 und 2 SächsDSG), bei der ein o. g. Verfahren eingesetzt oder wesentlich geändert werden soll, ein für diese zuständiger Datenschutzbeauftragter (i. S. v. § 11 SächsDSG) bestellt, so führt dieser die Vorabkontrolle durch, andernfalls der Sächsische Datenschutzbeauftragte. Die Anzeigepflicht für ein solches Verfahren obliegt der Daten verarbeitenden Stelle. Sie hat dafür die zur Prüfung erforderlichen Unterlagen frühestmöglich zur Verfügung zu stellen.

Ergeben sich bei der Vorabkontrolle durch den nach § 11 SächsDSG bestellten Datenschutzbeauftragten Zweifelsfälle, so hat er sich nach vorheriger Unterrichtung des Leiters der öffentlichen Stelle an den Sächsischen Datenschutzbeauftragten zu wenden (vgl. § 11 Abs. 3 Satz 2 Nr. 4 SächsDSG).

III. Inhalt, Zweck und Grenzen der Vorabkontrolle

Weil die o. g. *automatisierten* Verfahren spezifische Datenschutzrisiken für betroffene Personen beinhalten, unterliegen sie der Prüfung *vor Beginn* des Einsatzes.

Die Vorabkontrolle stellt für die einzuführenden automatisierten Verfahren[1] den Schutzbedarf und die Risiken fest und bewertet, insbesondere unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen gemäß § 9 SächsDSG,

[1] Eine automatisierte Verarbeitung personenbezogener Daten liegt nach § 3 Abs. 5 SächsDSG vor, wenn diese durch den Einsatz eines elektronischen Datenverarbeitungssystems (Rechner und Software) programmgesteuert durchgeführt wird. Ein automatisiertes Verfahren ist die Gesamtheit der einzelnen automatisierten Verarbeitungen mit einem bestimmten Verwendungszweck.

ob und wie Gefahren für die informationelle Selbstbestimmung Betroffener angemessen verhindert werden können. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (vgl. § 9 Abs. 1 Satz 2 SächsDSG).

Eine Vorabkontrolle ist *rechtzeitig vor ihrem erstmaligen* Einsatz oder *vor einer wesentlichen Änderung* durchzuführen und auf ihre Vereinbarkeit mit den datenschutzrechtlichen Anforderungen zu überprüfen. Der *erstmalige Einsatz* beginnt spätestens mit der Nutzung des Verfahrens im Betrieb (auch Probebetrieb) im realen Arbeitsumfeld mit Echtdaten.

Wesentlich sind *Änderungen*, soweit sie den betroffenen Personenkreis erweitern oder den Schutz bisher Betroffener vermindern. Diese können insbesondere vorliegen, wenn neue (schützenswerte) Datenarten in die Verarbeitung einbezogen werden, neue regelmäßige Datenverarbeitungen (z. B. Übermittlungen) auf weitere Empfänger ausgedehnt werden oder Soft- oder Hardware den Schutz der Betroffenen entscheidend vermindert. Ein Indiz dafür, dass ein Verfahren wesentliche Änderungen erfährt, findet sich im Katalog des § 9 Abs. 2 Nrn. 1 bis 6 SächsDSG.

Die Vorabkontrolle ist mit einer Stellungnahme abzuschließen. Sie ist der Behördenleitung bzw. dem Verfahrensverantwortlichen zuzuleiten und soll innerhalb *eines Monats* abgegeben werden (vgl. § 10 Abs. 5 Satz 3 SächsDSG). Die Monatsfrist beginnt erst, wenn alle für die Vorabkontrolle erforderlichen Unterlagen eingegangen sind. Das Ergebnis der Vorabkontrolle wird Bestandteil des Datenschutz- und Datensicherheitskonzeptes. Aus Revisionsgründen sollte in dem Verfahrensverzeichnis auf die durchgeführte Vorabkontrolle verwiesen werden.

Die Vorabkontrolle als eine vorausgehende Zulässigkeitskontrolle findet i. d. R. gelöst von ihrer Einsatzumgebung statt. Daher besteht die Notwendigkeit, während des Betriebes der neuen Technologie bzw. des automatisierten Verfahrens weitere Kontroll- und Revisionstätigkeiten durchzuführen.

IV. Die Verfahrensarten im Einzelnen

IV.1. Automatisierte Abrufverfahren

Durchzuführen ist die Vorabkontrolle für ein automatisiertes Verfahren, das eine Übermittlung personenbezogener Daten an Dritte durch Abruf ermöglicht (vgl. § 8 Abs. 1 Satz 1 erster Halbsatz SächsDSG). Ein automatisiertes Abrufverfahren ist ein von mindestens zwei Daten verarbeitenden Stellen gemeinsam eingerichtetes und betriebenes Verfahren, durch das die abrufende Stelle personenbezogene Daten aus einer von der bereithaltenden Stelle eingerichteten Datei abrufen kann. Die abrufende Stelle (Datenempfänger) bestimmt allein darüber, ob und wann sie welche Daten (innerhalb eines vorgegebenen Rahmens) abruft.

IV.2. Automatisierte Verarbeitung besonders schützenswerter Daten

Durchzuführen ist die Vorabkontrolle für ein automatisiertes Verfahren, mit dem personenbezogene Daten verarbeitet werden, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben (vgl. § 4 Abs. 2 SächsDSG). Die Verarbeitung dieser Daten ist nur zu den in § 4 Abs. 2 SächsDSG genannten Zwecken zulässig.

IV.3. Automatisierte Verarbeitung von Beschäftigtendaten

Durchzuführen ist die Vorabkontrolle für ein automatisiertes Verfahren, in dem Daten von Beschäftigten oder Bewerbern zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht, verarbeitet werden (vgl. § 37 Abs. 1 SächsDSG).

V. Inhaltliche Erläuterungen zum Verfahrensverzeichnis

Es wird empfohlen, das in der Anlage zu dieser Bekanntmachung abgedruckte Muster zu verwenden. Für jedes Verfahren ist ein gesondertes Datenblatt anzulegen. Beim Ausfüllen sollte beachtet werden:

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

Es ist die Stelle (im funktionalen Sinn) zu bezeichnen, bei der die Verarbeitung erfolgt (z. B. das Einwohnermeldeamt der Stadt). Wird das Verfahren von mehreren Stellen genutzt, ist - soweit möglich - eine zusammenfassende Bezeichnung anzugeben oder sind die Stellen einzeln zu nennen.

2. Bezeichnung des Verfahrens

Als Bezeichnung des Verfahrens ist der allgemein übliche oder ein möglichst „sprechender“ Begriff zu wählen. Darüber hinaus sollten Angaben zur eingesetzten Software (z. B. Bezeichnung, Version, Hersteller) gemacht werden.

3. vorliegende Unterlagen

Die Verfahrensbeschreibung enthält zum einen eine Darstellung der eingesetzten Programme, der Beziehung zu anderen Programmen sowie der Schnittstellen und der Teile, die als Auftragsdatenverarbeitung ausgelagert sind. Zum anderen ist die Einsatzumgebung (eingesetzte Hard- und Standardsoftware, z. B. Betriebssystem) darzustellen. Verträge über Auftragsdatenverarbeitung oder Wartungsarbeiten sind gemäß § 7 Abs. 2 Satz 2 SächsDSG schriftlich zu schließen. Dabei sind Weisungsbefugnisse, ausreichend sichere Maßnahmen gemäß § 9 SächsDSG, die Möglichkeit der Kündigung bei Daten-

schutzverstößen sowie ein eventueller Einsatz von Unterauftragnehmern nur mit Zustimmung des Auftraggebers sicherzustellen.
Das Datenschutz- und Sicherheitskonzept enthält Ausführungen, wie den Anforderungen von § 9 Abs. 2 SächsDSG entsprochen wird. Dazu können ggf. vorhandene Dienstvereinbarungen und Dienstanweisungen vorgelegt werden. Ich weise aber ausdrücklich darauf hin, dass nur eine Dienstvereinbarung einen normativen Charakter i. S. d. § 4 Abs. 1 Satz 1 SächsDSG hat.

4. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Es ist zu prüfen, ob der angegebene Zweck der Datenverarbeitung (z. B. Lohn- und Gehaltsabrechnung) von der entsprechenden gesetzlichen Ermächtigung gedeckt ist.

5. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Es ist zu prüfen, ob die für den betroffenen Personenkreis geplante Verarbeitung der konkret anzugebenden personenbezogenen Daten jeweils rechtmäßig ist.

6. Empfänger und Art zu übermittelnder Daten

Es ist zu prüfen, ob die für den betroffenen Personenkreis geplante Übermittlung der konkret anzugebenden personenbezogenen Daten und Empfänger jeweils rechtmäßig ist.

7. Beabsichtigte Übermittlung in Drittländer

Es ist zu prüfen, ob die für den betroffenen Personenkreis geplante Übermittlung der konkret anzugebenden personenbezogenen Daten und Empfänger in Drittländer jeweils rechtmäßig ist.

8. Regelfristen für die Löschung der Daten

Es ist zu prüfen, ob die Regelfristen für die Löschung den Anforderungen aus § 20 SächsDSG entsprechen.

9. Personelle, technische, und organisatorische Maßnahmen

Die gemäß § 9 SächsDSG getroffenen Maßnahmen sind jeweils zu beschreiben. Dabei kann auch auf die Ausarbeitungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), z. B. IT-Grundschutzhandbuch, zurückgegriffen werden.

Besondere Risikofaktoren sind Gefährdungen, die über die üblicherweise bestehenden hinausgehen und demzufolge bei der Risikoabwägung besonders zu berücksichtigen sind. Eine solche Gefährdung liegt zum Beispiel bei dem Einsatz mobiler Datenträger oder bei dem zunehmenden Einsatz von drahtlosen Netzwerken in der öffentlichen Verwaltung vor.

10. Stellungnahme

Eine automatisierte Datenverarbeitung darf nur eingeführt werden, wenn den erheblichen Gefahren für das Persönlichkeitsrecht durch ausreichend starke Schutzmaßnahmen entgegen gewirkt werden kann und das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist.
Ist das Restrisiko zu hoch, muss geprüft werden, ob durch eine Nachbesserung technischer oder organisatorischer Maßnahmen eine datenschutzgerechte Verarbeitung ermöglicht werden könnte. Ist das nicht der Fall, kann das Verfahren nicht eingeführt oder geändert werden.

Dresden, den 12. September 2005
Der Sächsische Datenschutzbeauftragte
Schurig

Anlage

Vorabkontrolle gemäß § 10 Abs. 5 SächsDSG

wegen:

☐ eines Verfahrens nach § 8

☐ eines automatisierten Verfahrens, in dem Daten im Sinne des § 4 Abs. 2 verarbeitet werden

☐ eines automatisierten Verfahrens, in dem Daten von Beschäftigten im Sinne des § 37 verarbeitet werden

1. Bezeichnung und Anschrift der Daten verarbeitenden Stelle

2. Bezeichnung des Verfahrens

3. Vorliegende Unterlagen

☐ Verfahrensbeschreibungen bzw. Benutzer-Handbücher,

☐ gegebenenfalls schriftliche Regelungen zur Auftragsdatenverarbeitung bzw. Wartung

☐ Datenschutz- und Datensicherheitskonzepte für das zu prüfende Verfahren gemäß § 9 Abs. 2 SächsDSG (vgl. dazu unten unter 9.)

☐ Dienstvereinbarung / Dienstanweisung

4. Zweck und Rechtsgrundlage der Verarbeitung personenbezogener Daten

Zweck	Rechtsgrundlage	Ergebnis der Prüfung

5. Betroffene Personengruppen und Art der zu verarbeitenden Daten

Personengruppe	Art der zu verarbeitenden Daten	Ergebnis der Prüfung

6. Empfänger und Art zu übermittelnder Daten

Empfänger	Art der zu übermittelnden Daten	Ergebnis der Prüfung

7. Beabsichtigte Übermittlung in Drittländer gemäß § 17 SächsDSG

Empfänger	Art der zu übermitteln-den Daten	Rechtsgrundlage	Ergebnis der Prüfung

8. Regelfristen für die Löschung der Daten

Art der Daten	Zeitraum	Ergebnis der Prüfung

9. Das Datenschutz- und Datensicherheitskonzept

umfasst mindestens

☐ die differenzierte Vergabe von Zugriffsrechten (Benutzerprofile) für Mitarbeiter,

☐ die Dokumentation zulässiger Auswertungen,

☐ die Gewährleistung von Rechten der Betroffenen (Auskunft, Berichtigung, Löschung, Sperrung),

☐ ein ausreichend sicheres Passwortverfahren oder andere Authentifikationsverfahren (Chipkarte, PIN),

☐ die Protokollierung und Log-Auswertungen (Fehlanmeldungen - Missbrauchsversuche),

☐ regelmäßige Backups von Programmen und Daten,

☐ die Überwachung von Administrations- und Wartungsarbeiten,

Gibt es besondere Risikofaktoren?

Wie ist sichergestellt, dass

a) nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

b) personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

c) personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),

d) jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),

e) festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),

f) die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz)?

10. Stellungnahme

Ort, Datum: ……. **Stempel, Unterschrift:** ……..

16.2 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.2.1 Entschließung zwischen der 65. und 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum automatischen Software-Update

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

1) Immer öfter werden dabei - oftmals vom Nutzer unbemerkt oder zumindest nicht transparent - Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne das dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.

2) Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.

3) Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das - unbemerkte - Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss.

Personenbezogen Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

16.2.2 Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig zum Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.

- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z. B. mit data-warehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist, und dass

- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in Bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

16.2.3 Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig: Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai diesen Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten “Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen” vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2149; 2001; 3868) hat,

- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,

- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,

- in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,

- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,

- die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, ¾ aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,

- lediglich 24 % der Beschlüsse substanziell begründet werden,

- es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

- 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden.

Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann - entgegen häufig gegebener Deutung - nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).

- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

- Der Umfang des - seit Einführung der Vorschrift regelmäßig erweiterten - Straftatenkataloges des § 100 a StPO muss reduziert werden.

- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Gesprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die

Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

- Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs.2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

16.2.4 Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken zur Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,

- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,

- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

16.2.5 Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken zu Personennummern

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z. B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

16.2.6 Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken zur Automatischen Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

16.2.7 Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken: Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon

betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

16.2.8 Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken zu Radio-Frequency Identification

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 20. November 2003 an (Übersetzung):

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Ein-

führung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a) sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

b) wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

c) dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und

d) soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

16.2.9 Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken: Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig

sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

16.2.10 Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken: Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch

bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

16.2.11 Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken: Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.9.2004 sog. "Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II" zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden

Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

16.2.12 Entschließung zwischen der 68. und 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Staatliche Kontenkontrolle muss auf den Prüfstand!

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z. B. anlässlich Steuererklärung, BaföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substan-

tiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

16.2.13 Entschließung zwischen der 68. und 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse: Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Die strafprozessuale DNA-Analyse ist - insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten - ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z. B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber - auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung - in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer voran-

gegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

16.2.14 Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10./11. März 2005 in Kiel zur Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen - technischen wie organisatorischen - Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

16.2.15 Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10./11. März 2005 in Kiel: Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

Stichwortverzeichnis