Sächsischer Landtag DRUCKSACHE 3/9041

3. Wahlperiode

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

11. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 2003

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 29. September 2003 Ausgegeben am: 29. September 2003

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

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

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

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

Internet: http://www.datenschutz.sachsen.de

Besucheranschrift: Devrientstraße 1
01067 Dresden

Vervielfältigung erwünscht.

Herstellung: OTTO Verlag & Druckerei GmbH & Co.KG
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)
ASiG	Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit vom 12. Dezember 1973 (BGBl. I S. 1885), zuletzt geändert durch Artikel 32 des Gesetzes vom 21. Dezember 2000 (BGBl. I S. 1983)
AsylVfG	Gesetz über das Asylverfahren (Asylverfahrensgesetz) in der Fassung der Bekanntmachung vom 27. Juli 1993 (BGBl. I S. 1361), zuletzt geändert durch Artikel 12 des Gesetzes vom 9. Januar 2002 (BGBl. I S. 361)
AuslDatV	Verordnung über die Führung von Ausländerdateien durch die Ausländerbehörden, zuletzt geändert am 9. Januar 2002 (BGBl. I S. 361)
AuslG	Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet (Ausländergesetz) vom 9. Juli 1990 (BGBl. I S. 1354), zuletzt geändert durch Art. 11 des Gesetzes vom 9. Januar 2002 (BGBl. I S. 361)
BAföG	Bundesgesetz über individuelle Förderung der Ausbildung (Bundesausbildungsförderungsgesetz) in der Fassung der Bekanntmachung vom 6. Juni 1983 (BGBl. I S. 645), zuletzt geändert durch Gesetz vom 20. Juni 2002 (BGBl. I S. 1946)
BAT-O	Bundes-Angestelltentarifvertrag in der in den neuen Ländern geltenden Fassung
BauGB	Baugesetzbuch
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BGB	Bürgerliches Gesetzbuch

BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz) in der Fassung vom 26. September 2002 (BGBl. I S. 3830)
BNotO	Bundesnotarordnung, i. d. F. d. Bek. vom 24. Februar 1961 (BGBl. I S. 97), zuletzt geändert am 27. April 2002 (BGBl. I S. 1467)
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)
BundesVwKostG	Bundesverwaltungskostengesetz
BWO	Bundeswahlordnung
DVAuslG	Verordnung zur Durchführung des Ausländergesetzes vom 18. Dezember 1990 (BGBl. I S. 1990, 2983), zuletzt geändert durch Gesetz vom 09.01.2002 (BGBl. I S. 361)
EG-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbebezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (ABl. EG L 281 vom 23. November 1995, S. 31)
EStG	Einkommensteuergesetz
FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnisverordnung) vom 18. August 1998 (BGBl. I S. 2214)
FVG	Gesetz über die Finanzverwaltung (Finanzverwaltungsgesetz)
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
HandwO	Gesetz zur Ordnung des Handwerks (Handwerksordnung) zuletzt geändert durch Art. 13 vom 10. November 2001 (BGBl. I S. 2992)
ImSchZuV	Verordnung des SMUL über Zuständigkeiten zur Ausführung des Bundes-Immissionsschutzgesetzes, des Benzinbleigesetzes und der aufgrund dieser Gesetze ergangenen Verordnungen (Zuständigkeitsverordnung Immissionsschutz) vom 12. Juli 2002 (SächsGVBl. S. 243)

InsO	Insolvenzordnung vom 5. Oktober 1994 (BGBl. I S. 2866), zuletzt geändert am 14. März 2003 (BGBl. I S. 345)
KpS-Richtlinien	Richtlinien des Sächsischen Staatsministeriums des Innern für die Führung Kriminalpolizeilicher personenbezogener Sammlungen in den Polizeidienststellen des Freistaates Sachsen vom 15. Juli 1993 (SächsABl. S. 1094)
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie vom 9. Januar 1907 (RGBl. S. 7), zuletzt geändert durch Art. 3 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266)
LuftVG	Luftverkehrsgesetz vom 1. August 1922 (RGBl. I S. 681) in der Fassung der Bekanntmachung vom 14. Januar 1981 (BGBl. I S. 61), zuletzt geändert nach Maßgabe des Art. 11 durch Art. 1 und 2 des Zehnten Gesetzes zur Änderung des Luftverkehrsgesetzes vom 23. Juli 1992 (BGBl. I S. 1370)
OWiG	Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz) vom 24. Mai 1968 (BGBl. I S. 481), zuletzt geändert am 22. August 2002 (BGBl. I S. 3387)
PStG	Personenstandsgesetz
SächsAG-BAföG	Sächsisches Ausführungsgesetz zum Bundesausbildungs-förderungsgesetz vom 7. Januar 1993 (SächsGVBl. S. 16), geändert durch Artikel 29 der Verordnung vom 10. April 2003 (SächsGVBl. S. 94, 97)
SächsArchGebVO	Sächsische Archivgebührenverordnung vom 8. Februar 1996 (SächsGVBl. S. 82)
SächsArchivBenVO	Sächsische Archivbenutzungsverordnung vom 24. Februar 2003 (SächsGVBl. S. 79)
SächsArchivG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (GVBl. S. 449), zuletzt geändert durch Art. 1 des Gesetzes zur Änderung verschiedener Vorschriften des Sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 370, berichtigt durch Bekanntmachung vom 16. Dezember 1999 (GVBl. S. 7), geändert durch Gesetz vom 12. März 2002 (GVBl. S. 108)
SächsDO	Disziplinarordnung für den Freistaat Sachsen vom 28. Februar 1994 (GVBl. S. 333)

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)
SächsFFG	Gesetz zur Förderung und der Vereinbarkeit von Familie und Beruf im öffentlichen Dienst im Freistaat Sachsen (Sächsisches Frauenförderungsgesetz) vom 31. März 1994 (GVBl. S. 684)
SächsFöDaG	Gesetz über Fördermitteldatenbanken im Freistaat Sachsen vom 10. Juni 1999 (SächsGVBl S. 273)
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)
SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675), zuletzt geändert durch Gesetz vom 28. Juni 2002 (GVBl. S. 205)
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-BegleitG 2003 und 2004 vom 11. Dezember 2002 (GVBl. S. 312)
SächsLaJuHiG	Landesjugendhilfegesetz in der Fassung der Bekanntmachung vom 29. September 1998 (GVBl. S. 506)
SächsLVOPol	Verordnung über die Laufbahn der Polizeibeamten des Freistaates Sachsen (Laufbahnverordnung der Polizeibeamten) vom 22. November 1999 (GVBl. S. 799)
SächsMG	Sächsisches Meldegesetz in der Fassung der Bekanntmachung vom 11. April 1997 (GVBl. S. 377), geändert durch Art. 4 des Gesetzes zum 4. Staatsvertrag rundfunktrechtlicher Staatsverträge vom 16. März 2000 (GVBl. S. 89)
SächsPersVG	Sächsisches Personalvertretungsgesetz in der Fassung der Bekanntmachung vom 25. Juni 1999 (GVBl. S. 430)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (GVBl. S. 466)
SächsPresseG	Sächsisches Gesetz über die Presse vom 3. April 1992 (GVBl. S. 125), geändert durch Art. 30 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)

SächsSchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz vom 28. Juni 2001 (GVBl. S. 426)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453), zuletzt geändert durch Gesetz vom 6. Juni 2002 (GVBl. S. 168)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVwKG	Verwaltungskostengesetz des Freistaates Sachsen vom 15. April 1992 (GVBl. S. 164)
SächsWG	Sächsisches Wassergesetz in der der Fassung der Bekanntmachung vom 21. Juli 1998 (GVBl. S. 393), zuletzt geändert durch Gesetz vom 14. November 2002 (GVBl. S. 307)
SäHO	Haushaltsordnung des Freistaates Sachsen in der Fassung der Bekanntmachung vom 10. April 2001 (GVBl. S. 153)
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. 3322)
SGB III	Sozialgesetzbuch (SGB) Drittes Buch (III) - Arbeitsförderung – vom 24. März 1997 (BGBl. I S. 594, zuletzt geändert durch Gesetz vom 23. Dezember 2002 (BGBl. I S. 4621)
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Gesetz vom 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	Zehntes Buch Sozialgesetzbuch - 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)
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen - Signaturgesetz – i. d. F. des Artikel 1 des Gesetzes vom 16. Mai 2001 (BGBl. I S. 876)
SigV	Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074)

StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) vom 20. Dezember 1991 (BGBl. I S. 2272), zuletzt geändert durch Gesetz vom 11. Oktober 2002 (BGBl. I S. 3970)
StVG	Straßenverkehrsgesetz in der Fassung vom 5. März 2003 (BGBl. I S. 310)
StVZO	Straßenverkehrs-Zulassungs-Ordnung, zuletzt geändert am 11. September 2002 (BGBl. I S. 3574)
VAHRG	Gesetz zur Regelung von Härten im Versorgungsausgleich vom 21. Dezember 1983 (BGBl. I S. 105), zuletzt geändert durch Artikel 30 des Gesetzes vom 25. Juli 1991 (BGBl. I S. 1606)
VerpflichtungsG	Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 2. März 1974 (BGBl. I S. 469), zuletzt geändert durch Änderungsgesetz vom 15. August 1974 (BGBl. I S. 1942)
VwVAusfBNotO	Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz zur Ausführung der Bundesnotarordnung vom 13. Januar 1999 (Sächsische Justizministerialblätter Nr. 1/1999 S. 14)
VwVfG	Verwaltungsverfahrensgesetz
VwVPersAktenB	Verwaltungsvorschriften des Sächsischen Staatsministeriums des Innern über die Führung und Verwaltung von Personalakten der Beamten (Verwaltungsvorschrift Personalakten Beamte) vom 11. Dezember 1998 (SächsABl. vom 14. Januar 1999 S. 10)
WHG	Gesetz zur Ordnung des Wasserhaushalts
WoGG	Wohngeldgesetz in der Fassung der Bekanntmachung vom 1. Februar 1993 (BGBl. I S. 183), neugefasst durch Bek. vom 23. Januar 2002 BGBl. I S. 474, geändert durch Gesetz vom 19. Juli 2002 (BGBl. I S. 2690)
ZPO	Zivilprozeßordnung, zuletzt geändert am 23. Juli 2002 (BGBl. I. S. 2850, ber. 4410)

Sonstiges

a. E.	am Ende
a. F.	alte Fassung
AfL/ÄfL	Amt/Ämter für Landwirtschaft
AfNS	Amt für Nationale Sicherheit
AKG	Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen e. V.
ÄndVO	Änderungs-Verordnung
AOK	Allgemeine Ortskrankenkasse
ARoV	Amt zur Regelung offener Vermögensfragen
ASD	Allgemeiner Sozialer Dienst
AZR	Ausländerzentralregister
BAGE	Amtliche Sammlung der Entscheidungen des Bundesarbeitsgerichts
BAnz.	Bundesanzeiger
BayObLG	Bayerisches Oberstes Landesgericht
BayVBl.	Bayerische Verwaltungsblätter
BayVGH	Bayerischer Verwaltungsgerichtshof
BA	Bundesanstalt für Arbeit
BAG	Bundesarbeitsgericht
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Der Bundesbeauftragte für den Datenschutz
BfF	Bundesamt für Finanzen
BFH	Bundesfinanzhof
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BGS	Bundesgrenzschutz
BHW	Beamtenheimstättenwerk
BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse

BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium der Finanzen
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BML	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BMWA	Bundesministerium für Wirtschaft und Arbeit
BND	Bundesnachrichtendienst
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStBl.	Bundessteuerblatt
BStU	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
BT-Drs.	Bundestags-Drucksache
BVA	Bundesversicherungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts
BZR	Bundeszentralregister
CD-ROM	Compact disc-read only memory
CR	Computer und Recht [Zeitschrift; früher auch “CuR”]
DKFZ	Deutsches Krebsforschungszentrum
DRK	Deutsches Rotes Kreuz
DSMeld	Datensatz für das Meldewesen
DVBl	Deutsches Verwaltungsblatt
DVO	Durchführungsverordnung
ed-	erkennungsdienstlich
EG	Europäische Gemeinschaft
EGN	Einzelgesprächsnachweis
EOSS	Evolutionär orientierte Steuer-Software (Gemeinsamer Pro-

	grammierverbund auf Länderebene mit dem Endziel, bundeseinheitliche IT-Programme zu definieren)
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
FDGB	Freier Deutscher Gewerkschaftsbund (DDR)
FDJ	Freie Deutsche Jugend (DDR)
FTP	File transfer protocol
Gauck-Behörde	Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
GKR	Gemeinsames Krebsregister
GKV	gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GMBl.	Gemeinsames Ministerialblatt, hrsg. vom Bundesministerium des Innern
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
GWZ 1995	Gebäude- und Wohnungszählung 1995
HessVGH	Hessischer Verwaltungsgerichtshof
HIV	human immunodeficieny virus (Aidserreger)
HTTP	Hypertext Transfer Protocol
IKK	Innungskrankenkasse
IM	Inoffizieller Mitarbeiter (des MfS/AfNS)
INPOL	Polizeiliches Informationssystem des Bundes und der Länder
ISD	Internationaler Suchdienst Arolsen
ISDN	Integrated services digital network
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KIN-S	Kommunales Informationsnetz - Sachsen
KPI	Kriminalpolizeiinspektion

KV	Kassenärztliche Vereinigung
LARoV	Landesamt zur Regelung offener Vermögensfragen
LfF	Landesamt für Finanzen des Freistaates Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LG	Landgericht
LKA	Landeskriminalamt Sachsen
LKV	Landes- und Kommunalverwaltung (Zeitschrift)
LPDK	Lehrpersonaldatenbank
LRA	Landratsamt
LSG	Landessozialgericht
LUA	Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen
LÜVA	Lebensmittelüberwachungs- und Veterinäramt
LVA	Landesversicherungsanstalt
MdI	Ministerium des Innern (DDR)
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MedR	Medizinrecht (Zeitschrift)
MfS	Ministerium für Staatssicherheit
MPU	Medizinisch-Psychologische Untersuchung
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
ÖbV	Öffentlich bestellter Vermessungsingenieur
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OSA	Oberschulamt
OVG	Oberverwaltungsgericht
PASS	Polizeiliches Auskunftssystem Sachsen
PersR	Zeitschrift Personalvertretungsrecht
PersV	Die Personalvertretung (Zeitschrift)
PIN	Personal identification number (Persönliche Identifikationsnummer)

PKZ	Personenkennzahl
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegTP	Regulierungsbehörde für Telekommunikation und Post
RG	Reichsgericht
RGBl.	Reichsgesetzblatt
RP	Regierungspräsidium
RPA	Rechnungsprüfungsamt
SächsABl.	Sächsisches Amtsblatt
SächsDSB	Sächsischer Datenschutzbeauftragter
SächsJMBl.	Sächsisches Justizministerialblatt
SächsOVG	Sächsisches Oberverwaltungsgericht
SächsVBl.	Sächsische Verwaltungsblätter
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SAKD	Sächsische Anstalt für Kommunale Datenverarbeitung
SED	Sozialistische Einheitspartei Deutschlands (DDR)
SLFS	Sächsisches Landesamt für Familie und Soziales
SK	Sächsische Staatskanzlei
SLBG	Sächsische landwirtschaftliche Berufsgenossenschaft
SLT	Sächsischer Landkreistag e. V.
SMAD	Sowjetische Militäradministration
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz
SMK	Sächsisches Staatsministerium für Kultus
SMS	Sächsisches Staatsministerium für Soziales
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft
SMWA	Sächsisches Staatsministerium für Wirtschaft und Arbeit
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
SSG	Sächsischer Städte- und Gemeindetag e. V.
StaLA	Statistisches Landesamt Sachsen
StUFA	Staatliches Umweltfachamt
StUFÄ	Staatliche Umweltfachämter

TB	Tätigkeitsbericht
TCP/IP	Transmission control protocol/Internet protocol
TdL	Tarifgemeinschaft deutscher Länder
THA	Treuhandanstalt
TK-Anlage	Telekommunikationsanlage
TU	Technische Universität
TÜ	Telefonüberwachung
TÜV	Technischer Überwachungsverein
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VIZ	Zeitschrift für Vermögens- und Investitionsrecht
VO	Verordnung
VwV	Verwaltungsvorschift
VZR	Verkehrszentralregister
WiJu	Wirtschaftliche Jugendhilfe
WWW	World Wide Web
ZTR	Zeitschrift für Tarifrecht

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 Dank

Die Bemühungen der Behörde des Sächsischen Datenschutzbeauftragten galten dem Schutz des Persönlichkeitsrechts, der Privatsphäre. Ich danke allen Abgeordneten des Sächsischen Landtages, den Mitarbeitern der Ministerien und der anderen staatlichen Verwaltungsstellen, den kommunalen Gremien und Amtsträgern, den Hochschulen und den Kammern, nicht zuletzt den gesetzlichen Krankenkassen und den öffentlichen Unternehmen und Stiftungen für die gute Zusammenarbeit und für manches vertrauensvolle Wort. Meine Arbeit hätte ohne ihr Problembewusstsein, ohne Offenheit für Argumente und ohne eine große Portion Kollegialität nicht gelingen können.

Dieser Tätigkeitsbericht ist - wie die Vorberichte - ein Gemeinschaftswerk aller meiner Mitarbeiter. Wie in jedem Jahr habe ich auch diesmal eine Dankesschuld zu erfüllen: Es war einfach schön zu erleben, wie fachkundig, fleißig und unkompliziert meine Kolleginnen und Kollegen zusammenarbeiten, um allen öffentlichen Stellen bei den oft schwierigen juristischen und technischen Problemen, die eine moderne und - hoffentlich! - effiziente Datenverarbeitung im rechtsstaatlichen Gefüge bereitet, mit gutem Rat und manchem Fingerzeig zu helfen.

Der Landtagsverwaltung - geleitet durch den Herrn Landtagspräsidenten - habe ich wiederum für ein weiteres Jahr der kollegialen Unterstützung zu danken.
Besonderer Dank gilt in diesem Jahr dem Sächsischen Innenministerium, das uns als Hochwasser-Vertriebenen schnell und freundlich eine ausreichende Dienstunterkunft gewährt hat, die wir kurz vor Weihnachten wieder verlassen konnten.

1.2 Personalnot

Auch in diesem Jahr kann ich meinen Tätigkeitsbericht erst nach der Sommerpause des Parlaments vorlegen. Denn vom Stichtag des 31. März 2003 an hat es eben doch einige Monate gedauert, den Bericht zu erstellen. Diese Verspätung ist auf die zahlenmäßig unzureichende Personalausstattung meiner Behörde zurückzuführen. Wir sind einfach zu wenige, um die anfallende Arbeit, eben ein natürlicherweise gestiegenes Aufkommen an schwierigen Anfragen, sachgerecht und fristgerecht erledigen zu können. Ich habe in meinem 10. Tätigkeitsbericht - wie ich meine, in der gebotenen Deutlichkeit - auf diesen Missstand hingewiesen. Eine Reaktion darauf ist weder seitens des Landtages noch seitens der Staatsregierung erfolgt.

Ich teile förmlich mit, dass ich nicht einmal die aufgrund von Eingaben notwendigen und gebotenen Kontrollen durchführen konnte, von anlassfreien und überraschen-

den Routinekontrollen - die in mancher Behörde nun wirklich nötig wären - ganz zu schweigen.

Weil ich keine offizielle Reaktion auf meinen 10. Tätigkeitsbericht in diesem Punkt erfahren habe, wiederhole ich zur Vertiefung meinen damaligen Text mit der Bitte um Beachtung :

Die Ausgaben der öffentlichen Hand für Hard- und Software in der automatisierten Datenverarbeitung sind exponentiell gestiegen. Wir müssen uns vergegenwärtigen, dass jede Behörde, ja fast jeder Mitarbeiter im öffentlichen Dienst im Freistaat Sachsen von morgens bis abends personenbezogene Daten verarbeitet. Dann wird deutlich, dass lediglich 18 Mitarbeiter des Sächsischen Datenschutzbeauftragten nicht dazu in der Lage sein können, die ca. 250.000 Bediensteten in der Staatsverwaltung, in der Kommunalverwaltung, in der Hochschulverwaltung und in den Kammern und Stiftungen sowie in den Krankenkassen umfassend und effizient zu beraten und zu kontrollieren.

Es steht zu erwarten, dass die Novellierung des Sächsischen Datenschutzgesetzes meiner Behörde eine Reihe zusätzlicher Aufgaben übertragen wird. Spätestens dann muss eine angemessene Personalausstattung des Sächsischen Datenschutzbeauftragten erreicht werden. Darauf hat er einen gesicherten Anspruch, weil sein Amt, seine Aufgaben und Befugnisse auf verfassungsrechtlicher Grundlage (Art. 33 und Art. 57 der Sächsischen Verfassung) beruhen - und weil unsere Hinweise unnötigen Aufwand vermeiden.

1.3 Prozessbericht

In meinem 9. Tätigkeitsbericht (1) hatte ich kritisiert, dass gegen mich ein staatsanwaltschaftliches Ermittlungsverfahren eingeleitet worden war und mir zum Vorwurf gemacht wurde, den Vorgang einer rechtswidrigen Verarbeitung personenbezogener Daten durch den damaligen Justizminister öffentlich gemacht zu haben.

In dem sich anschließenden Strafverfahren wegen Geheimnisverrats (§ 353 b StGB) wurde ich durch das Landgericht Dresden von diesem Vorwurf freigesprochen. Die Sächsische Generalstaatsanwaltschaft legte hiergegen Revision ein. Inzwischen hat der Bundesgerichtshof meinen Freispruch letztinstanzlich bestätigt. Das Urteil ist in diesem Bericht im Original (unter 11/16.2.1) abgedruckt. Die zentrale Aussage des Gerichtes lautet wie folgt:
„Ein Amtsträger, der wie der Angeklagte zur Kontrolle der Gesetzestreue eines anderen Amtsträgers berufen ist, kann wichtige öffentliche Interessen nicht durch die Offenbarung eines Gesetzesverstoßes gefährden, wenn er die Öffentlichkeit - wie ersichtlich hier - auch als Verbündeten gewinnen will, um auf ein gesetzmäßiges Ver-

halten hinzuwirken. Damit verfolgte der Angeklagte selbst ein wichtiges öffentliches Interesse ...“

Der Bundesgerichtshof spricht allen Amtsträgern, die zur Kontrolle der Gesetzestreue anderer Amtsträger berufen sind (dies sind unter anderem die Datenschutzbeauftragten), das Recht zu, „die Öffentlichkeit als Verbündeten zu gewinnen“, um auf diese Weise auf ein gesetzmäßiges Verhalten der Behörden, ihrer Leiter und Bediensteten hinzuwirken. Diese Beteiligung der Öffentlichkeit liege gerade im öffentlichen Interesse.

Die klaren Worte des Bundesgerichtshofes haben nach meiner Einschätzung die Wirkmöglichkeiten der Datenschutzbeauftragten des Bundes und der Länder gestärkt und gesichert. Ich freue mich, dass das Verfahren die Position der unabhängigen, öffentlichkeitswirksamen Datenschutzkontrolle garantiert und ihre Rechte bekräftigt hat.

In der Gerichtsentscheidung wird schlaglichtartig festgestellt, dass der Öffentlichkeit in einer demokratischen Gesellschaft die zentrale Kontrollfunktion zukommt. Staatliches Handeln hat das Wohl des Einzelnen im Blick; das Gemeinwohl ist nicht mehr als das Wohl aller Einzelnen. Die staatlichen Funktionäre der „öffentlichen Verwaltung“ dienen dem Einzelnen und haben seine Freiheit zu garantieren, indem sie die Gesetze vollziehen. Sie haben dies grundsätzlich im Licht der Öffentlichkeit, also unter demokratischer Kontrolle zu tun.

Der einzelne Bürger hat Anspruch auf Beachtung seiner ungestörten und grundsätzlich abgeschotteten Privatsphäre. Während er auf seine Grundrechte vertrauen und sich grundsätzlich frei entfalten kann und soll - dies liegt nach der verbindlichen Rechtsprechung des BVerfG im Interesse einer freien Gesellschaftsordnung - muss der Staat sich für jeden grundrechtseinschränkenden Eingriff auf eine klare - öffentlich bekannte - Rechtsvorschrift stützen können und sein Handeln in der Medienöffentlichkeit, im öffentlichen Diskurs des Parlaments und vor öffentlich tagenden Gerichten begründen. Nicht der Einzelne muss sich für seine Freiheitsausübung - und damit für den Schutz seiner Daten - rechtfertigen, vielmehr muss der Staat sein Handeln öffentlich legitimieren. Dieser elementare Grundsatz ist - so muss ich leider auch in Gesprächen mit Verwaltungsjuristen feststellen - einigen im öffentlichen Dienst unbekannt; sie handeln zuweilen noch nach der Devise des Obrigkeitsstaates versunkener Zeiten.

1.4 Ausblick - Mahnungen zur formalen Gesetzesbindung

Juristische Anforderungen an die Verwaltung aus Sicht des Datenschutzes
Die sächsische Verwaltung hat sich in den vergangenen Jahren positiv entwickelt und

verkörpert den Rechtsstaat. Das häufig verschlungene Dickicht der Vorschriften wird zumeist durchschaut; auf ihre datenschutzgerechte Anwendung kann sich der Bürger grundsätzlich verlassen. Die Verwaltung hat nach der Wende Großartiges geleistet und auch die Folgen der Flut 2002 gemeistert. Das Grundverständnis für den Datenschutz hat in Sachsen weiter zugenommen; der Qualitätsstandard ist hoch. Böswilligkeiten oder bewusste Rechtsbrüche bilden eine absolute Seltenheit.

Die Komplexität der technischen Ausstattung, die Verlockung des Möglichen, der fehlende Widerstand der Zuständigen und die subjektiv empfundene „Belästigung durch die Gesetze“ verleiten aber manchen Amtsinhaber dazu, datenschutzrechtliche Bestimmungen zu verletzen. Meine Dienststelle entdeckt immer wieder solche Verstöße gegen das Grundrecht auf informationelle Selbstbestimmung. Offenbar sind die Versuchungen der Macht - und im gewaltfreien Raum ist nur Wissen Macht - groß. Die folgenden Ausführungen sollen helfen, diese Versuchungen weiter zu minimieren. Eine nun zwölfjährige Erfahrung auf dem Gebiet des Datenschutzes ist Gelegenheit, die Gründe zu nennen, die ich für die wesentlichen Ursachen für fehlerhafte, rechtswidrige Verarbeitungsvorgänge mit personenbezogenen Daten halte:

1.4.1 Grundrechtslage des Datenschutzes

Immer wieder wird die Bedeutung des Grundrechts (auf informationelle Selbstbestimmung) verkannt: Die Grundrechtslage bedeutet, dass der Mensch zur Freiheit geboren ist; zum Einzelnen gehört sein Freiheitsrecht, das ihm nicht etwa vom Staat verliehen wurde, sondern das aus der Tatsache herrührt, dass er ein Mensch ist. Denn Quell aller Grundrechte ist der in Art. 1 Abs. 1 des Grundgesetzes anerkannte Sachverhalt: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.“ Damit verbunden ist das Recht jedes einzelnen Menschen auf individuelle Entwicklung nach dem Wortlaut des Art. 2 Abs. 1 GG: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“ Jede Persönlichkeit ist anders; die Unterschiedlichkeit jedes Einzelnen ist gesellschaftspolitisch Ausgangspunkt und Ziel aller Bemühungen. Der freiheitliche Staat bietet jedem Raum auch für Extravaganz und Anders-Sein. Der Schutz dieses Freiraumes ist ein Staatszweck.

Die Unantastbarkeit der Würde des Einzelnen ist nicht änderbar (Art. 79 Abs. 3 GG), sie entzieht sich jeder Disposition; sie ist dem Einzelnen nicht von der Gemeinschaft, sozusagen „von oben“ zugebilligt oder zugeteilt, nein, sie steht jedem Menschen zu, weil er nach christlichem Verständnis ein Ebenbild Gottes und ein vernunftbegabtes, beseeltes Wesen ist. Die Würde ist das Naturrecht des Menschen.

Das hat Folgen. Man muss von jedem Politiker und von jedem Verwaltungsmitarbeiter erwarten, dass er die Konsequenzen der Grundrechtslage erkennt und bei all seinem Handeln beachtet.

Das Grundrecht auf informationelle Selbstbestimmung wird vom Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65,1 ff.) aus den vorgenannten Grundgesetz-Artikeln abgeleitet. Zu den Einzelheiten wird auf den Text der entscheidenden Passagen des - für alle staatliche Gewalt verbindlichen - Urteils verwiesen, der in diesem Tätigkeitsbericht unter (11/16.2.2) im Original abgedruckt ist.

Dieses Grundrecht auf informationelle Selbstbestimmung wird in Art. 33 der Sächsischen Verfassung wie folgt formuliert: „Jeder Mensch hat das Recht, über die Erhebung, Verwendung und Weitergabe seiner personenbezogenen Daten selbst zu bestimmen. Sie dürfen ohne freiwillige und ausdrückliche Zustimmung der berechtigen Person nicht erhoben, gespeichert, verwendet oder weitergegeben werden. In dieses Recht darf nur durch Gesetz oder auf Grund eines Gesetzes eingegriffen werden."

Aus der Tatsache, dass dieses Grundrecht jedem Menschen natürlicherweise zusteht und ihm nicht etwa durch einen gewährenden Akt des Staates zugebilligt wird, folgt, dass der Einzelne in seiner Berechtigung zur Privatheit grundsätzlich die Vorhand vor dem Staat hat. Der Staat ist nur ausnahmsweise gegenüber dem Bürger berechtigt, ihn anzufragen oder auszuforschen. Vielmehr ist es so, dass sich der Staat immer dann, wenn er Informationen über den einzelnen Menschen als gemeinschaftsbezogenes und - gelegentlich - sogar gemeinschaftsgebundenes Wesen regelgerecht in Anspruch nehmen und damit in das Grundrecht auf informationelle Selbstbestimmung eingreifen, also personenbezogene Daten erheben und weiterverarbeiten will, auf eine normenklare gesetzliche Vorschrift stützen können muss. Der Staat muss sich rechtfertigen, indem er sich auf eine demokratisch zustande gekommene Rechtsvorschrift beruft. Diese darf zum einen den Wesensgehalt des Grundrechts nicht antasten (Art. 19 Abs. 2 GG), zum anderen muss ein ordentlicher Rechtsschutz - und zwar für jeden Einzelnen, der von einer Datenverarbeitung durch die öffentliche Hand betroffen ist - bestehen (Art. 19 Abs. 4 GG). Im Grundsatz ist also der Einzelne frei, der Staat aber gebunden.

Es ist falsch danach zu fragen, ob dem Staat (als Inbegriff aller Inhaber öffentlicher Gewalt) etwa durch den Gesetzgeber eine bestimmte Verarbeitung personenbezogener Daten verboten sei und daraus zu folgern, dass dann, wenn ein solches Verbot nicht besteht, der Staat die Datenverarbeitung vornehmen dürfe. Richtig ist es vielmehr zu fragen, ob ein Gesetz dem Staat die Datenverarbeitung erlaubt. Dabei sind die gesetzlichen Formen zu beachten; sie schützen den Einzelnen vor willkürlicher, nicht vorhersehbarer Verarbeitung seiner Daten. Werden die Formen gewahrt, ist der Rechtsstaat gesichert. Daher ist vor allem nach dem formalen Verfahrensgang zu fragen.

Auf diesem richtigen Grundrechtsverständnis aufbauend kann man sich mit meiner Behörde über alle Probleme ernsthaft auseinandersetzen. Diese eben genannte Voraussetzung ist allerdings unerlässlich.

Weil der Einzelne die Verarbeitung der eigenen Daten durch öffentliche Stellen nicht bemerkt - das Freiheitsbedrohende wird zunächst üblicherweise heimlich vollzogen - soll es von Verfassungs wegen den unabhängigen Datenschutzbeauftragten als Kontrollorgan geben, der zumindest stichprobenhaft Rechtsschutz gewährt. Diese Kontrollen sind Tropfen auf einen heißen Stein; Aufgabe meiner Dienststelle ist es, die Tropfen zischen zu lassen, wenn sie verdampfen. Das Zischen weckt die öffentliche Kontrolle.

1.4.2 Handwerk der Juristen

Bei der Auslegung von Gesetzen werden immer wieder Defizite deutlich, so dass ich aus der Sicht des Datenschutzes folgende Vorgehensweise empfehle:

Am Anfang steht die Suche nach dem Gesetz, das den zu entscheidenden Fall trifft. Dabei geht das neuere dem älteren und das speziellere dem allgemeinen Gesetz vor.

Eine Gesetzesauslegung ist weder notwendig noch statthaft, wenn der Gesetzestext sprachlich klar und eindeutig ist. Ein klarer Gesetzestext kann und darf nicht weiter ausgelegt werden. Man muss allerdings den gesamten Text lesen.

Ist der Gesetzestext unklar oder können einem einzelnen Gesetzesbegriff unterschiedliche Inhalte zugrunde gelegt werden, so beginnt die Kunst der Auslegung; ihr Ziel ist es, den objektiv zum Ausdruck gekommenen Willen des Gesetzgebers zu erfassen. Die Grenze jeder Auslegung ist allerdings der Widerspruch zum Wortlaut der Norm. Grammatische, systematische, historische und teleologische Methoden ergänzen einander.

a) Zunächst muss der Kontext des Gesetzes geprüft, zum Beispiel in modernen Gesetzen danach gefragt werden, ob gesetzliche Begriffe etwa zu Beginn des Gesetzes oder in sog. Klammerdefinitionen näher erläutert werden. So erfolgt eine grammatikalische und nach dem Wortsinn eines ganz bestimmten verwendeten Begriffs suchende sprachliche Auslegung von der Systematik des Gesetzes her.

b) Daran kann sich anschließen eine Auslegung unter Beachtung der Begrifflichkeiten einer übergeordneten oder auch wesensverwandten Gesetzgebung, also beispielsweise eine Auslegung eines Landesgesetzes anhand eines Bundesgesetzes, das einen gleichen oder ähnlichen Sachverhalt regelt.

c) Hilft auch dies nicht weiter, so kommt die sog. historische Auslegung in Betracht, also die Suche danach, welche Auffassung die „Väter und Mütter des Gesetzes“ anlässlich der Gesetzesberatungen geäußert haben. Hier sind die sogenannten Materialien zum Gesetz zu erforschen, also Niederschriften über Ausschusssitzungen oder Reden in Plenardebatten zur Einbringung oder Begründung des Gesetzes. Wurde das Gesetz von der Regierung eingebracht, so hat es üblicherweise eine offizielle Begründung, die ebenfalls herangezogen wird.

d) Erst am Ende eines solchen Auslegungsprozesses kann - wohlgemerkt nur dann, wenn die bisherigen Schritte kein eindeutiges Ergebnis erbracht, sondern Widersprüchliches zu Tage gefördert haben - die Auslegung nach dem berühmten „Sinn und Zweck des Gesetzes“ erfolgen. Diese teleologische Auslegungsform ist deshalb erst so spät zu wählen, weil ja eigentlich das, was gesucht wird, nämlich der angeblich wirkliche Sinn des Gesetzes, häufig bei der Frage nach dem „Sinn und Zweck“ schon vorausgesetzt wird, wenn man etwa meint, vom Wortsinn, von der Systematik oder von der Historie absehen oder abweichen zu dürfen. Derjenige, der das Gesetz auslegt, ist immer in der großen Gefahr, einem Zirkelschluss zu unterliegen, wenn er zu früh danach fragt, was denn „Sinn und Zweck des Gesetzes“ ist. Anders gesagt: Wird ein abweichender „Sinn und Zweck“ einfach von dem, der ein bestimmtes Ergebnis erreichen will, unterstellt und blank definiert, so geschieht das, was nicht geschehen sollte: Das Gesetz wird nach Gutdünken zur Begründung für die eigene Meinung oder die mit der „Auslegung“ verfolgte Absicht genommen. Das gerade wäre aber ein Ergebnis, das den Wortlaut des Gesetzes dem subjektiven Auslegungsziel seines Anwenders unterordnen würde. Eine solche falsche Methodik widerspräche dem Grundsatz der Gesetzmäßigkeit der Verwaltung und dem Demokratieprinzip.

e) Falls die dem gemäß vorzuziehende mögliche Auslegung in einen Konflikt mit der Verfassung führen würde, folgt die sog. verfassungskonforme Auslegung, soweit diese durch den Wortlaut des Gesetzes gedeckt ist und die prinzipielle Zielsetzung des Gesetzgebers wahrt. Aus Respekt vor dem Gesetzgeber werden die von ihm gebrauchten Begriffe anhand der Grundentscheidungen der Verfassung und ihres Normengefüges in der Auslegung anerkannt, in der das Gesetz einen verfassungsgemäßen Inhalt hat.

1.4.3 Politisierung der Verwaltung

Wesentlicher Inhalt des Rechtsstaates ist der Befehl des Art. 20 Abs. 3 GG: „Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.“ Dieser rechtsstaatlichen Bindung und Kompetenz entspricht die Verwaltung leider aus der Sicht des Datenschutzes auf vielen Gebieten noch nicht: Das ist nicht etwa darauf zurückzuführen,

dass die Verwaltung grundsätzlich fehlerhaft und schlecht arbeiten würde - das ist nicht der Fall -, sondern darauf, dass sie gelegentlich sachfremden Einflüssen unterliegt: Wenn die Politik die „Kunst des Möglichen“ ist, so sollte die Verwaltung das „möglichst Unpolitische“, also das Regelhafte, eben das Gesetzmäßige, sein.

So ist immer wieder festzustellen, dass auch einfache Verwaltungsvorgänge dann „politisiert“, also als Einzelfälle in Form und Umfang der Datenverarbeitung vom formalen Recht entfernt werden, wenn dazu, aus welchen örtlichen Konstellationen auch immer, ein angeblicher Anlass besteht.

Wenn sich die Verwaltung doch nur auf die Ausführung der Gesetze beschränken würde!

Dies ist ihre wesentliche Aufgabe, die die Verfassung ihr zubilligt. Dennoch kommt es vor, dass statt der zur Entscheidung aufgerufenen Amtsträger vom Gesetz nicht vorgesehene Exekutivgremien eingesetzt werden, die - meist handverlesen, aber ohne ordentliche Verfahrensordnung - an ihrer Stelle politisch unangenehme oder unpopuläre Entscheidungen oder sogar Entscheidungen fernab der gesetzlichen Vorschriften durchpauken sollen.

Gremien werden auch dann gebildet, wenn z. B. Angst vor den Medien besteht oder wenn der politische Gegner - sei es die Opposition oder die Mehrheit - ausgebremst werden soll. Es entstehen dann „Nebenverwaltungen“ und gelegentlich auch „Überverwaltungen“.

Eine beliebte Strategie ist es auch, die Entscheidungen, für welche die untere Ebene zuständig ist, nach oben zu ziehen: Ein Fall, der angeblich von politischer Bedeutung ist, soll dann nicht mehr durch die eigentlich berufenen Amtsträger entschieden werden, sondern wird zur nächst höheren oder gar zur höchsten Stelle gegeben, um von dort entschieden zu werden. Die Folge besteht nicht nur darin, dass die Fach-, Rechts- oder Dienstaufsicht ausgehebelt (weil vorweggenommen und damit befangen gemacht) wird und die zuständigen Amtsträger frustriert sind. Der „Datenverarbeitungssalat“, der in diesen Fällen entsteht, ist - selbst aus Sicht der berufenen Entscheidungsträger - unerträglich.

Aus der Sicht des Datenschutzes ist auch ein Wort zur Ämterhäufung zu sagen: Das grundsätzlich, eben von ausdrücklichen Ausnahmen abgesehen, bestehende Nebentätigkeitsverbot im öffentlichen Dienst hat gute Gründe: Der Amtsträger soll sich mit voller Hingabe, also mit allen seinen persönlichen Kräften, seiner Funktion widmen. Daneben werden andere öffentliche oder private Tätigkeiten nur dann erlaubt, wenn sie das öffentliche Amt nicht berühren, wenn also keine Interessenkonflikte entstehen können. Je „höher“ das übertragene öffentliche Amt jedoch ist, umso häufiger werden diese guten Grundsätze verlassen: Die Nebentätigkeiten von Bürgermeistern, Landrä-

ten, Behördenleitern und Ministern (bei Letzteren bedarf es der Offenlegung gegenüber dem Parlament) werden zu wenig auf Inkompatibilität geprüft: Könnte es Konstellationen geben, in denen die eine Tätigkeit unter der anderen negativ beeinflusst oder gestört werden könnte? Wird die Zweckbindung von Daten - oft unmerklich - durch andere Zwecke unterlaufen? Wird das Wissen aus dem einen Amt unzulässigerweise für ein anderes Amt genutzt?
Wenn z. B. ein Minister personalverantwortliche oder aufsichtliche Funktionen über eine ihm nachgeordnete Stiftung auszuüben hat, sollte er aus meiner Sicht nicht im Verwaltungsrat dieser Stiftung sitzen. Es ist auch bedenklich, wenn er personenbezogenes Wissen, das er aus der Verwaltungsratstätigkeit gezogen hat, aufsichtsrechtlich nutzt. Aufsicht kann nicht ohne persönliche Distanz gelingen. Ebensowenig darf der Minister statt seiner selbst seinen Abteilungsleiter in den Verwaltungsrat berufen lassen. Ein Bürgermeister gehört nicht in den Aufsichtsrat eines ortsansässigen Unternehmens; dies ebensowenig, wie die Gemeinde ihr Fremdenverkehrsbüro in den Räumen der örtlichen Kurklinik unterbringen darf. Schon der böse Anschein von Befangenheiten ist zu vermeiden.

Hier sind Grundsätze der Ämtertrennung und des Datenschutzes eng, ja unauflösbar miteinander verwoben. Das Prinzip, öffentliche Stellen datenschutzgerecht, d. h. differenziert nach den unterschiedlichen gesetzlichen Zwecken der Verarbeitung personenbezogener Daten zu organisieren und personell zu besetzen, wird oft nicht genügend beachtet und gepflegt: Ämtertrennung ist ein Datenschutzprinzip.

Eine weitere Politisierung der Verwaltung entsteht dadurch, dass in der Verwaltung irgendwelche Leute „untergebracht“ werden. In derartigen Fällen melden sich meistens unsere - doch sonst so gestrengen - Personalisten nicht zu Wort. Manchmal sind sie auch nicht zuständig, weil es sich bei manchen Stellenbesetzungen um Bereiche handelt, in denen wirtschaftliche und politische, kulturelle und Gesichtspunkte der „Selbstvermarktung“ der in Betracht kommenden Körperschaften, Gremien und Funktionen von Bedeutung sind. Die Begehrlichkeit der politischen Parteien, häufig auch der Kuhhandel, mit dem Posten besetzt werden, ist aus Sicht des Datenschutzes ein schwerwiegender Fehler. Am Anfang stehen meist wenig transparente Datenverarbeitungsvorgänge, in die auch Personen, Berater oder Gremien eingebunden werden, die die Personalie gesetzesgemäß nichts angehen. Das gilt auch für den umgekehrten Vorgang: Die Entfernung missliebiger Mitarbeiter läuft leider manchesmal so ab, dass zunächst heimlich Informationen gesammelt werden - der Begriff der „Sachakte“ in Personalabteilungen bezeichnet den angeblichen Kunstgriff, die (sofortige!) Anhörungspflicht des § 119 des Sächsischen Beamtengesetzes zu umgehen - oder dass Beschwerden zum willkommenen und entsprechend aufgebauschten Anlass genommen werden. Und wenn eine Umsetzung oder Versetzung zu risikoreich erscheint, werden halt die Kompetenzen verkleinert. Das faire Verfahren des Arbeits- oder Disziplinarrechts darf nicht umgangen werden, auch wenn es viel Arbeit macht, denn die Datenverarbeitung hat klaren Regeln zu folgen. Die gerichtliche Überprüfbarkeit muss gewahrt bleiben.

Manche Vorgesetzte gefallen sich darin, abwägende oder abratende Juristen gern als „Verhinderer“ oder als „ewige Bedenkenträger“ zu bezeichnen (gern benutzt wird auch der dumme Spruch „Drei Juristen, vier Meinungen“). Derartige Chefs ersetzen die fehlende persönliche Autorität und die eigene Fach- und Rechtserkenntnis gern durch Forschheit und einen herablassenden Vorgesetztenton - eben ein Feigenblatt.

1.4.4 Führungspersönlichkeit

Schließlich gibt es klassische Führungsfehler, die nicht nur unklug sind, sondern die gesetzlichen Zuständigkeitsregeln und damit die rechtmäßigen Wege der Datenverarbeitung verlassen. Innerhalb der Hierarchie der Verwaltung gibt es „oben“ oder „weiter unten“ immer wieder Personen, die „nicht miteinander können“. Aber sie sind - eben wegen der Ordnung in der Hierarchie - aneinander gebunden und müssten eigentlich die Entscheidungsprozesse miteinander - offen und kollegial - erledigen. Diese Konstellation, aber auch die Befangenheit, ja Schwäche mancher Vorgesetzten, sich mit kühlem und fachkundigem Widerspruch „Untergebener“ auseinander zu setzen und selbst die sachlich besseren Argumente vortragen zu müssen, führt dazu, dass sie sich mit handverlesenen Jasagern umgeben. Die Entourage eines Schwachen ist meist noch schwächer, sie schwächt den Schwachen. Die Mitarbeiter eines Starken sind oft noch stärker, sie stärken den Starken.

Auf der anderen Seite finden sich leider immer wieder Emporkömmlinge, die es „klug“ unterlassen, mit der eigenen rechtlich sauberen Meinung hervorzutreten, obgleich sie dazu berufen oder verpflichtet sind.

In derartig geführten Verwaltungen herrscht der, der über Herrschaftswissen verfügt. Dort werden Informationen (sowohl von oben nach unten, als auch - Rache des kleinen Mannes - von unten nach oben) vorenthalten oder dosiert. Die Meinungsbildung verläuft in Etagen und in künstlich gepflegten Hierarchien. Es ist auch falsch, nur von solchen Rat anzunehmen, die die gleiche Gehaltsklasse haben; die „Etagendenker“ suchen nicht die sachliche Erledigung, sondern die eigene Spreizung - mancher Pfau schlägt sein Rad auch im kleinsten Raum. Offene Darstellungen, befreiende Meinungsäußerungen werden vermieden; Sachwissen wird nicht da offen und direkt abgefordert, wo es vorhanden ist. Wer mehr weiß, macht sich interessant. Das tötet nicht nur bei denen, die weniger Informationen erhalten, die Freude an der Arbeit, sondern führt zu verqueren und verquasten Datenverarbeitungsgängen, legt falsche Fährten, verändert die Gewichte und vergrößert den Aufwand - letztlich zu lasten des Betroffenen, der die verschlungenen Wege, die die ihn betreffenden Informationen nehmen, nicht mehr kennt; er versteht die Welt nicht mehr.

Berater, Stäbe, besondere Referenten, auswärtiger Rat etc. können aber ausnahmsweise doch notwendig sein. Ein Beispiel für eine notwendige Kommission war diejenige nach der Flut unter General a. D. v. Kirchbach - sie hat aber gerade keine Einzelfälle

bewertet, sondern strukturelle Fehler analysiert und Verbesserungsvorschläge vorgelegt. Solche Kommissionen dürfen aber nie dazu führen, dass ungesetzliche Verfahrenswege gegangen werden, Entscheidungsprozesse auf Sonderwegen zustande kommen und insbesondere die Zuständigen umgangen werden.

Führung lebt vom Widerspruch, von alternativen Vorschlägen, vom spannungsreichen Diskurs. In der Verwaltung ist Führung die oft mühsame Erarbeitung des effizientesten Weges zur fairen und gerechten Entscheidung des Einzelfalles. Jedem Vorgesetzten ist es - auf Dauer gesehen - eine Hilfe, sich dialektischen Prozessen zu unterwerfen. Jeder Vorgesetzte muss lernen - von wem sonst, als von seinen zuständigen Mitarbeitern (man nehme den Begriff wörtlich).

1.4.5 Freiwilligkeit

Art. 33 SächsVerf und § 4 SächsDSG betonen, dass jeder Betroffene über die ihn betreffenden Informationen selbst verfügen darf. Eine freiwillige Einwilligung (vorherige Zustimmung, nicht nachträgliche Genehmigung) kann daher, nimmt man das Selbstbestimmungsrecht ernst, Rechtsgrundlage der Datenverarbeitung durch die öffentliche Hand sein.

Die Frage ist nur, wann und auf welchen Gebieten das wirklich so ist. Denn der Grundsatz der Gesetzmäßigkeit der Verwaltung (Art. 20 Abs. 3 GG) gebietet, dass die Verwaltung sich bei jedem Akt des Eingriffes in Grundrechte, ja sogar bei jeder „wesentlichen“ Tätigkeit (siehe Wesentlichkeitsdoktrin des Bundesverfassungsgerichtes, BVerfGE 49, 89 [126]; 61, 260 [275]; 83, 130 [142, 151 f.]) auf ein Gesetz zu stützen hat, das die Aufgaben und Befugnisse der Verwaltungsstelle normenklar regelt. Dieser „Vorbehalt des Gesetzes“ betrifft die Verwaltung in ihrer Gesamtheit - allerdings darf der Gesetzgeber, dessen gesetzlicher Befehl den Ideen der Regierung und dem Willen der Verwaltung sowie aller Gerichte (außer den Verfassungsgerichten) vorgeht, ja sogar deren Tätigkeit abstrakt in Umfang, Verfahren und Ergebnis bestimmt, ganz bewusst Raum lassen für (rechtlich verbindliche) Normen, die durch Regierung (Rechtsverordnungen), Verwaltung (Satzungen; Verwaltungsvorschriften, die z. B. das Ermessen zugunsten des Bürgers binden) oder Gerichte (justitielle Selbstverwaltung) erlassen werden. Dieser Grundsatz vom „Vorrang des Gesetzes“ betont aber auch die „Vernormung“, d. h. die abstrakte Bindung der Verwaltung an Vorschriften und damit ihre Pflicht, jeden gleichen Sachverhalt auch gleich zu behandeln.

Dem widerspricht - und das springt sofort ins Auge - eine Verwaltungstätigkeit, die ihre Entscheidung am freien Willen des einen oder anderen Betroffenen ausrichten würde, nämlich danach, ob und wie weit er „mitmacht“, also freiwillig Informationen über sich liefert. Natürlich wird niemanden seine soziale Leistung ohne Antrag, also gegen seinen Willen gewährt. Und natürlich muss derjenige, der eine soziale Leistung

beantragt, der Verwaltung eine Menge Daten geben, damit diese die Leistungsvoraussetzungen prüfen kann. Insofern gilt der Grundsatz „Daten gegen Geld“. Aber auch bei der gewährenden Verwaltung müssen diese Leistungsvoraussetzungen abstrakt und stringent festgelegt sein; d. h. es muss von vornherein klar sein, welche personenbezogenen Daten „abgeliefert“ werden müssen, damit diese oder jene soziale Wohltat gewährt wird. Das bedeutet, dass die Verweigerung von Informationen deutlich negative Rechtsfolgen hat, aber auch, dass überschießende Informationen aus Rechtsgründen nicht erforderlich sind.
Wir stellen also fest, dass die Einwilligung in diesen Bereichen zwar nötig ist, dass aber der Wille des Betroffenen in diesen Fällen nicht wirklich „frei“ ist, denn seine Entscheidung, gewisse Informationen über sich und seine Verhältnisse zurückzuhalten, hat direkt spürbare Auswirkungen auf die Verwaltungsentscheidung.

Die Apologeten der Selbstbestimmung meinen diese folgenschwere rechtlich gebundene informationelle Selbstbestimmung auch nicht, wenn sie von Einwilligung sprechen. Vielmehr wollen sie üblicherweise entweder die Aufgaben oder die Befugnisse der Verwaltung über den gesetzlichen Rahmen hinaus erweitern, gleichsam im Zusammenspiel mit dem Betroffenen.

Ein negatives Beispiel ist die Einholung der Einwilligung zur Erhebung und Speicherung der DNA-Analyse bei Verurteilten oder gar bei Gefangenen, ohne eine richterliche Prognoseentscheidung - die macht nämlich Arbeit. Ein anderes Beispiel ist das „Angebot“ der Stadt Sebnitz, Bankdienstleistungen durch Gemeindepersonal in einer Außenstelle der Verwaltung erledigen zu lassen. Häufig wird die Freiwilligkeit auch entdeckt, um gesetzliche Bindungen oder Inkompatibilitäten zu unterlaufen.

Das widerspricht dem Datenschutz im Rechtsstaat.

Für eine wirklich freiwillige Entscheidung des Einzelnen, seine Daten preiszugeben oder eine besondere Verarbeitung seiner Daten zu erlauben, eignet sich das Über- und Unterordnungsverhältnis der Obrigkeit zu ihrem Bürger grundsätzlich nicht. Vielmehr muss jede staatliche, kommunale und sonstige Körperschaft des öffentlichen Rechts für vorhersehbar regelhafte, gleichförmige und gerechte Eingriffe und Gewährungen sorgen. So bleiben für die wirklich freiwillige Entscheidung des Betroffenen, ob er - sozusagen außer der Reihe - mit einer Datenverarbeitung einverstanden ist, nur die Bereiche übrig, in denen die Obrigkeit uns gleichgeordnet, eben wie ein anderer Bürger, gegenübersteht. Das ist in weiten Bereichen der Fiskalverwaltung so, also wenn das Finanzamt Kohlen kauft und den Kohlenhändler fragt, ob seine Daten auch fürs nächste Jahr gespeichert werden dürfen (das Beispiel ist lächerlich, aber so ist die Rechtslage); oder im Bereich öffentlicher Forschung, wenn die Universitätsklinik den Patienten fragt, ob die Studenten seine Leber ansehen dürfen. Auch hier bleibt die Entscheidung, Daten preiszugeben, nicht folgenlos, aber sie beeinflusst nicht die Rechte des Betroffenen (außer dem Recht auf informationelle Selbstbestimmung).

Da gibt es aber immer noch Personalstellen in der Verwaltung, die wollen z. B. über den klaren Wortlaut des § 31 SächsDSG hinaus weitere Personaldaten „freiwillig“ speichern, z. B. werden Polizeidienst-Bewerber um die Einwilligung gebeten, dass die einstellende Verwaltung in das Polizeiliche-Auskunfts-System-Sachsen (PASS) schaut, ob gegen den Bewerber „etwas“ vorliegt. Das SMI ist mit mir einig, dass hier - der Zugang zum öffentlichen Dienst ist ein Grundrecht - kein Raum für Freiwilligkeiten ist.

Krankenkassen haben sich an ihre Versicherten gewandt, um Entlassungsberichte aus Krankenhäusern zu erhalten, die ihnen gesetzlich nicht zustehen. Polizeidienststellen fragen Anrufer, ob sie mit der Aufzeichnung von Gesprächen einverstanden sind.

Wenn „es nicht geht“, kommen findige Verwaltungsleute auf die „Freiwilligkeit“. Fast immer ist das rechtlich verfehlt. Und fast immer ist es ebenso langwierig wie aussichtslos, diesen Kollegen ihre „Idee“ auszureden. Der Grundsatz lautet: Aufgaben und Befugnisse der hoheitsrechtlichen Verwaltung können auf der Basis einer Einwilligung des Betroffenen weder begründet noch modifiziert werden.

1.4.6 Fazit

Warum sage ich dies alles als Datenschutzbeauftragter? In den genannten Fallkonstellationen werden entweder ungeeignete, nicht erforderliche personenbezogene Daten verarbeitet, oder die richtigen Daten werden von Personen verarbeitet, die schlechterdings dazu nicht befugt sind oder jedenfalls nicht befugt hätten gemacht werden dürfen, oder diese beiden Fehler werden kumuliert. Die Datenverarbeitung verläuft dann eben nicht mehr in den vom Verwaltungsverfahrensgesetz oder von sonstigen Verfahrensvorschriften und klarer hierarchisch geordneter Zuständigkeit vorgesehenen und für jeden ablesbaren Bahnen, sondern sie verlaufen sozusagen auf doppelten Böden. Die Folge sind regelmäßig sogenannte Datenschutzskandale.

All solche Vorgänge schwächen die Kraft der Verwaltung und führen zur Unübersichtlichkeit und möglicherweise beabsichtigten Undurchschaubarkeit der Datenverarbeitung. Die Verantwortung für die Datenverarbeitung wird rechtswidrig verlagert, der Betroffene einem Machtspiel ausgesetzt.

Das Grundrecht auf informationelle Selbstbestimmung und die von ihm beherrschten Regeln der Datenverarbeitung fordern, dass die Verwaltung die Gesetze transparent umzusetzen und sich darin zu genügen hat.

2 Parlament

Aktenvorlage in Untersuchungsausschüssen

Ein Sächsisches Staatsministerium fragte mich, in welchem Umfang es seine Akten, die auch personenbezogene Daten oder Geschäftsgeheimnisse enthalten, einem Untersuchungsausschuss des Sächsischen Landtages vorzulegen hat.

In Beantwortung dieser Anfrage habe ich auf die Rechtsprechung des Bundesverfassungsgerichtes verwiesen. So werden im sog. Flick-Urteil des Gerichts (BVerfGE 67, S. 100 ff.) die wechselseitigen Rechte und Pflichten von Regierung und Parlament bei der Offenbarung von Akteninhalten verbindlich konturiert: Danach genießt das Recht des Parlaments auf Aktenanforderung Verfassungsrang. Es legitimiert damit das Parlament zur „Beteiligung am geheimen Wissen der Regierung“, denn ohne diese Beteiligung - so stellt das Gericht fest - vermag das Parlament weder das Gesetzgebungsrecht noch das Haushaltsrecht noch das parlamentarische Kontrollrecht gegenüber der Regierung auszuüben. Demzufolge hat das Gericht selbst Informationen, die durch den starken Schutz des § 30 AO privilegiert sind, nicht von der Verwertbarkeit durch parlamentarische Untersuchungsausschüsse ausgenommen. Als Konsequenz dieser Argumentation stellt das Bundesverfassungsgericht ferner den Grundsatz auf, dass der Schutz des Persönlichkeitsrechts (etwa aufgrund des Eigentumschutzes) erst recht dem Aktenherausgabeanspruch weichen muss, wenn Parlament und Regierung bereits Vorkehrungen für den Geheimschutz getroffen haben.

Weil letztere Voraussetzungen im Freistaat Sachsen erfüllt sind, bedeutet dies für die Sachbehandlung durch den Untersuchungsausschuss des Sächsischen Landtages, dass die Sächsische Staatsregierung befugt ist, ihre Akten nach Geheimhaltungsgraden zu klassifizieren; sie hat diese jedoch sodann dem Untersuchungsausschuss vorzulegen. Dort unterliegt der Vorgang mit den klassifizierten Informationen der Geheimhaltungsordnung des Sächsischen Landtages.

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. Datenschutz bei arbeitsmedizinischer Vorsorgeuntersuchung

Mit einer Eingabe hat mich ein Berufskraftfahrer veranlasst, auf die Frage des datenschutzgerechten Umgangs mit den Ergebnissen arbeitsmedizinischer Vorsorgeuntersuchungen einzugehen.

Für bestimmte Berufsgruppen des öffentlichen Dienstes sind arbeitsmedizinische Vorsorgeuntersuchungen empfohlen bzw. vorgeschrieben; der Arbeitgeber entspricht damit gesetzlichen Auflagen bzw. berufsgenossenschaftlichen Grundsätzen, schon deshalb, um bei Unfällen oder Krankheiten ausreichend abgesichert zu sein. (Solche besonderen Rechtsvorschriften enthalten die §§ 29 bis 35 Gefahrstoffverordnung, §§ 37 bis 41 Röntgenverordnung, §§ 67 bis 71 Strahlenschutzverordnung, §§ 10 bis 16 Druckluftverordnung sowie die Unfallverhütungsvorschrift „Arbeitsmedizinische Vorsorge“ VBG 100.) Allerdings kann grundsätzlich jede arbeitsmedizinische Untersuchung vom Beschäftigten abgelehnt werden. Ist eine Untersuchung für eine bestimmte gefährdende Tätigkeit rechtsverbindlich vorgeschrieben, darf der Beschäftigte dort nicht eingesetzt werden; daraus entstehen arbeitsrechtliche Konsequenzen.

Eine wesentliche Frage ist, ob und inwieweit der Arzt den Arbeitgeber nach einer durchgeführten Untersuchung, die zu einem pathologischen Befund geführt hat, informieren darf. Regelmäßig ist von einer stillschweigenden Einwilligung in Bezug auf die Weitergabe des Untersuchungsergebnisses an den Arbeitgeber auszugehen, wenn sich der Arbeitnehmer von einem Betriebsarzt untersuchen lässt. Der Betriebsarzt darf darauf gestützt jedoch nur eingeschränkt Daten mitteilen, nämlich ob gegen die Einstellung des Bewerbers gesundheitliche Bedenken bestehen oder nicht. Hingegen darf er grundsätzlich keine Einzelheiten zum Befund offenbaren. Die ärztliche Schweigepflicht gilt nämlich auch für arbeitsmedizinische Vorsorgeuntersuchungen; Diagnosen oder Befunde dürfen allenfalls mit Einwilligung des Patienten an den Arbeitgeber weitergegeben werden (vgl. § 8 Abs. 1 ASiG, § 4 Abs. 1 Nr. 2 SächsDSG). Der Betriebsarzt macht sich strafbar, wenn er unbefugt die ihm durch seine Tätigkeit bekannt gewordenen Daten des Arbeitnehmers dem Arbeitgeber übermittelt (§ 203 StGB).

Unbedenklich ist die Weitergabe der medizinischen Einschätzung nach folgenden streng arbeitsmedizinischen Kriterien:

- „keine gesundheitlichen Bedenken”,
- „befristete gesundheitliche Bedenken”,
- „dauernde gesundheitliche Bedenken”.

Hingegen greift die in der Praxis häufig verwendete Formel

- „keine Bedenken unter bestimmten Auflagen",

unter ausdrücklicher Nennung der Auflagen (z. B. das Vorschreiben einer Sehhilfe), in das o.g. Diagnosetabu insoweit ein, als sich aus der Art der Auflage auf die Natur des Befundes (im Beispiel wohl zumeist Kurzsichtigkeit) schlussfolgern lässt.

Jeder niedergelassene oder Krankenhaus-Arzt hat sich, möchte er die Daten weitergeben, zuvor der ausdrücklichen Einwilligung des Patienten zur Übermittlung dieses Ergebnisses an den Arbeitgeber zu versichern. Der Arzt hat dem untersuchten Patienten dessen Beruf er kennt, insbesondere den Zusammenhang zwischen dem erhobenen Befund und seiner beruflichen Tätigkeit zu erläutern.

Selbstverständlich hat der Arbeitnehmer das Recht, in eine Weitergabe diagnostischer Details nicht einzuwilligen. Soweit dies jedoch im Einzelfall zur Verletzung vertraglicher Nebenpflichten des Arbeitnehmers führt (vgl. § 7 Abs. 2 BAT-O), hat die Rechtsprechung eine Offenbarungspflicht des Betroffenen konstruiert: Arbeitnehmer im öffentlichen Dienst müssen bei Zweifeln an ihrer Diensttauglichkeit ihre Ärzte von der Schweigepflicht entbinden; eine Weigerung stellt eine Pflichtverletzung und damit möglicherweise einen Grund für eine fristlose Kündigung dar (BAG Urteil vom 06.11.1997 - 2AZR 801/96 - RDV 5/98, 217.). Dem ist datenschutzrechtlich mit einer sorgfältigen Abwägung Rechnung zu tragen. Nur wenn dem Datenschutzinteresse des Untersuchten ein anderes Schutzgut (z. B. die mögliche Vermeidung von Unfällen, d. h. Gefahr für Leib oder Leben) gegenübersteht und überwiegt, ist das Zurücktreten des Schutzes der Intimsphäre verhältnismäßig. Das kann z. B. dann der Fall sein, wenn bei einem Kraftfahrer oder Waffenträger ein Anfallsgefährdung (etwa infolge Bluthochdrucks) festgestellt wird.

5.1.2 Entfernung von Unterlagen aus der Personalakte

Ein Petent hat Einsicht in seine Personalakte genommen und festgestellt, dass eine vom Arbeitgeber in einem Personalgespräch ausgesprochene Missbilligung bereits seit 30 Monaten Teil der Akte war. Der Petent fragt nun, ob er ein Recht darauf habe, diese Missbilligung jetzt aus der Akte zu entfernen und vernichten zu lassen.

Die Gemeinsame Verwaltungsvorschrift der Sächsischen Staatskanzlei und der Sächsischen Staatsministerien zur Führung und Verwaltung von Personalakten für Angestellte, Arbeiter und die zu ihrer Ausbildung Beschäftigten im öffentlichen Dienst des Freistaates Sachsen vom 20. Juli 1999 (SächsABl. S. 866) besagt unter Nr. 2.1, dass die beamtenrechtlichen Bestimmungen zur Personalaktenführung sinngemäß anzuwenden sind, soweit die tariflichen Vorschriften keine eigenständigen Regelungen über die Aufbewahrungsdauer enthalten. (Von dem Beseitigungsanspruch nach § 13 Abs. 2 BAT-O war hier nicht auszugehen, da eine vorherige Anhörung stattgefunden

und die zutreffende Missbilligung lediglich den Sinn hatte, den Arbeitnehmer an die gewissenhafte Erfüllung seiner Vertragspflichten zu erinnern und sich die Missbilligung in ihrer Wirkung auch darin erschöpft hat.)

In diesem Fall war also von den beamtenrechtlichen Regelungen auszugehen:

Spricht der Vorgesetzte oder Dienstvorgesetzte einem Beamten gegenüber missbilligende Äußerungen (Zurechtweisungen, Ermahnungen, Rügen und dergleichen), die nicht Teil einer dienstlichen Beurteilung oder einer anderen die Leistung oder Eignung betreffenden Feststellung aus, so ist dies *keine* Disziplinarmaßnahme im Sinne von § 5 Abs. 2 SächsDO, es sei denn, sie ist ausdrücklich als solche bezeichnet.

Somit ist § 122 Abs. 1 Nr. 2 SächsBG sinngemäß anzuwenden. Nach dieser Vorschrift sind Unterlagen über Beschwerden, Behauptungen und Bewertungen, auf die die Tilgungsvorschriften des Disziplinarrechts keine Anwendung finden, *auf Antrag nach drei Jahren* zu entfernen und zu vernichten.

Durch erneute Vorwürfe vor Ablauf der 3-Jahres-Frist, die die in früheren Unterlagen gegen den Betroffenen erhobenen Vorwürfe oder geltend gemachten Bedenken weiterhin berechtigt erscheinen lassen, wird diese Frist unterbrochen.
In unserem Fall muss der Bedienstete noch sechs Monate warten, bis die Missbilligung aus der Akte verschwindet, falls er das wünscht.

5.1.3 Beförderungskonferenzen bei der sächsischen Polizei

Bei der sächsischen Polizei werden unter Federführung des Staatsministeriums des Innern und unter Beteiligung verschiedener polizeilicher Stellen so genannte „Beförderungskonferenzen“ durchgeführt. Diese sollten halbjährlich erfolgen. Ich habe hierin die Gefahr gesehen, dass die Teilnehmer dieser Beratungen Kenntnis von personenbezogenen Daten von Mitarbeitern außerhalb ihres Zuständigkeitsbereichs erhalten. Daher habe ich das Ministerium um Stellungnahme gebeten.

Das Ministerium teilte mir mit, dass die Beförderungskonferenzen aufgrund einer *Richtlinie über die Verleihung von Beförderungsämtern an Polizeivollzugsbeamte* durchgeführt worden seien. Es handelt sich hierbei um eine Vorschrift auf Erlassebene. Zweck der Beförderungskonferenzen war es hiernach, eine sachgerechte und einheitliche Praxis bei Beförderungen des auf viele Organisationseinheiten und Stellen sich erstreckenden Polizeibereichs zu erreichen. Die Beförderung selbst richtet sich nach § 13 der SächsLVOPol. Diese Verordnung sieht wie die allgemeine *Verordnung der Sächsischen Staatsregierung über die Laufbahnen der Beamten und Richter im Freistaat Sachsen* (Sächsische Laufbahnverordnung) die Beteiligung des Landespersonalausschusses bzw. von Aufsichtsbehörden bei der Beförderung vor. Darüber

hinaus sehen spezialgesetzliche Vorschriften eine Beteiligung anderer Stellen bei Beförderungen vor, wie die Mitbestimmung des Personalrates in § 81 Abs. 1 Nr. 2 SächsPersVG und der Frauenbeauftragten in § 20 Abs. 1 Nr. 1 in Verbindung mit § 8 Abs. 1 Nr. 2 SächsFFG. Im übrigen sind die Datenverarbeitungen streng an den Zuständigkeiten der personalverwaltenden Stellen zu orientieren, eine Beteiligung anderer Stellen ist nicht erforderlich. Für eine Datenverarbeitung durch Teilnehmer außerhalb deren jeweiligen Zuständigkeitsbereichs sah im Ergebnis zutreffend auch das Ministerium keine Rechtsgrundlage.

Dass es bei den Beförderungskonferenzen zu unerlaubten Datenverarbeitungen gekommen ist, konnte ich aufgrund der Stellungnahme des Innenministeriums nicht ausschließen. Nach meiner Anfrage ist die Richtlinie jedoch umgehend außer Vollzug gesetzt worden. Es finden keine Beförderungskonferenzen mehr statt. Das Ministerium hat mir zudem zugesagt, die vorgenannte Richtlinie zu überarbeiten. Dabei sollen die *Beförderungskonferenzen* keine Erwähnung mehr finden. Die angekündigte Neufassung der Richtlinie steht noch aus. Ich werde die Angelegenheit weiter verfolgen.

5.1.4 Aufbewahrung von Unterlagen über Erkrankungen - Arbeitsunfähigkeits-Bescheinigungen (Krankenscheine)

Bei Kontrollen von personalverwaltenden Stellen und durch mehrfache Anfragen hat sich gezeigt, dass immer noch Unsicherheiten bei der Aufbewahrung von Unterlagen über Erkrankungen, zu denen auch Arbeitsunfähigkeits-Bescheinigungen (Krankenscheine) zählen, bestehen.

Nach § 123 Abs. 2 SächsBG sind Unterlagen über Erkrankungen fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorganges abgeschlossen wurde, aufzubewahren. Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, sind unverzüglich zurückzugeben, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden.

Die Aufbewahrungsfrist von fünf Jahren gilt auch für die zur Registrierung von Abwesenheitszeiten durch Krankheit vorgelegten Arbeitsunfähigkeits-Bescheinigungen (Krankenscheine). Diese „kurze“ Aufbewahrungsfrist dient der Verwaltungsvereinfachung und bezweckt, die Personalteilakte (vgl. A I. Nr. 3 Buchstabe e VwVPersAktenB, vom 11. Dezember 1998, danach sind Unterlagen über Erkrankungen in Teilakten zu führen) von Vorgängen zu entlasten, die für die weitere Entwicklung des Dienstverhältnisses nicht mehr benötigt werden (wenn für dienstliche Zwecke nicht mehr auf den Einzelvorgang zurückgegriffen werden muss).

Die nach § 123 Abs. 2 Satz 2 SächsBG unverzüglich zurück zu gewährenden Unterlagen, sind die Unterlagen über die Art einer Erkrankung. Sie sind dem Betroffenen zuzusenden oder zu übergeben. Es ist streng darauf zu achten, dass geschützte Daten über Krankheit, Diagnosen, Behandlungen und Medikationen auf das für die Dauer der Abrechnung unumgänglich notwendige Maß beschränkt bleiben. Dadurch soll sichergestellt werden, dass sie nicht für dienstliche Zwecke genutzt werden, für die sie nicht vorgelegt oder erhoben worden sind. Das trifft auch auf Arbeitsunfähigkeits-Bescheinigungen zu, aus deren Daten auf eine spezielle Erkrankung zu schließen wäre (z. B. Arztstempel mit Facharztbezeichnung).

Ärztliche Unterlagen, die die Grundlage für eine dienstrechtliche Entscheidung bilden (z. B. Gewähr der gesundheitlichen Eignung, Beurteilung der Dienstfähigkeit bzw. Dienstunfähigkeit), werden dagegen nach ihrem bestimmungsgemäßen Zweck ggf. auf Dauer benötigt. Sie gehören dann *nicht* zu den zurückzugebenden Unterlagen im Sinne von § 123 Abs. 2 Satz 2 SächsBG. Diese Unterlagen sind verschlossen zur Personalgrundakte zu nehmen (vgl. A I. Nr. 2 Buchstabe f VwV PersaktenB).

5.2 Personalvertretung

Informationsrechte des Personalrates – Stellenbesetzungspläne der Dienststelle

Eine oberste Dienstbehörde wandte sich mit der Bitte um Prüfung an mich, ob es zulässig sei, dem Personalrat einen Stellenbesetzungsplan, der die Vor- und Zunamen der Beschäftigten, Funktionen und Vergütungsgruppe, den Aufgabenbereich sowie sonstige, für die Personalbedarfsplanung wesentliche Angaben (z. B. beabsichtigte Versetzungen, Abordnungen, Dauer von Erziehungsurlaub) enthalten sollte, zur Verfügung zu stellen. Der örtliche Personalrat verlangte nämlich die Datenübermittlung unter Hinweis auf eine Entscheidung des Bundesverwaltungsgerichts vom 23. Januar 2002, das eine genau solche umfassende Informationsweitergabe für die Personalvertretungen als erforderlich angesehen hat (Beschluss des BVerwG v. 23.1.2002 – Az.: 6 P 5/01; in Auszügen u. a. abgedruckt in ZTR 2002, 196 ff.).

Ich habe hierzu die Auffassung vertreten, dass dem Personalrat nach § 73 Abs. 2 SächsPersVG grundsätzlich die Möglichkeit gegeben werden muss, sein Überwachungsrecht auszuüben. Insoweit ist der Entscheidung des Bundesverwaltungsgerichts zu folgen. Der Personalrat benötigt einen Stellenbesetzungsplan, um in der Lage zu sein, Rechtsverstößen und Unbilligkeiten in der Dienststelle bereits im Vorfeld entgegenzuwirken. Dies ist auch nur bei dauerhafter Überlassung einer Stellenbesetzungsliste, die die erforderliche Gesamtübersicht bietet, möglich. *Vor- und Zunamen*, ggfs. *Titel* und die *Amtsbezeichnung* gehören zu einer solchen Stellenplanübersicht, denn der Personalrat muss auch wissen, um welche Mitarbeiter es im Stellenplan geht. Auch Datenfelder über die tatsächlichen *Bezüge*, *Dienstposten*, *Stelle/Planstelle* jeweils mit den dazugehörenden Vergütungs- bzw. Besoldungsgruppen als Bezugsgröße sind erforderliche Daten. Darüber hinaus enthält der Stellenplan regelmäßig keine weiteren auf die Mitarbeiter bezogenen Informationen.

Der Personalrat hat daher meiner Auffassung nach keinen Anspruch auf eine Übersicht, aus der sich zusätzlich zu den vorgenannten Daten vielfältige weitere Informationen aus Eintragungen in einem Freitext- oder einem vordefinierten Feld ergeben, wie z. B. der Aufgabenbereich der Mitarbeiter und deren Zuordnung zu einzelnen Organisationseinheiten, geplante Veränderungen wie Abordnungen und Erziehungsurlaube.

Dies trifft auf jeden Fall dann zu, wenn diese Daten schon auf andere Weise in der Dienststelle allgemein oder gegenüber dem Personalrat bekannt gemacht worden sind. Die Personalvertretung ist in der Lage über ihre Beteiligung und ihr Informationsrecht weitere erforderliche Daten fallweise und nach Notwendigkeit in Erfahrung zu bringen. Ein Hinzufügen weiterer Daten zu der Übersicht wäre auch nicht zulässig. Zu vermeiden ist nämlich das Erstellen ganzer Mitarbeiterprofile, deren Kenntnis über

die Aufgaben der Personalvertretung hinausgehen würde und damit für die Aufgabenwahrnehmung nicht erforderlich wäre.

Trotz der Verschwiegenheitspflicht der Personalvertretung ist die Weitergabe von in besonderem Maße gehäuften Informationen, wie bei einem Stellenbesetzungsplan, mit der entsprechenden Achtsamkeit durchzuführen. So sind bei großen Dienststellen gleich mehrere hundert Mitarbeiter betroffen. Für die Datensicherheit habe ich daher nachstehende, nicht abschließende Empfehlungen gegeben. Diese sind auf andere Datenverarbeitungen durch die Personalvertretung mit vergleichbarer Intensität übertragbar.

1. Der Personalratsvorsitzende und sein Stellvertreter erhalten eine Stellenplan-übersicht, zu der nur sie Zugang haben. Diese ist in einem gesicherten Behältnis aufzubewahren (andere Personalratsmitglieder können beim Vorsitzenden Einsicht nehmen).
2. Der Personalrat hat dafür Sorge zu tragen, dass keine Vervielfältigungen der Stellenplanunterlagen erfolgen.
3. Nachdem dem Personalrat eine aktualisierte Stellenplanübersicht zugeleitet worden ist, sind die alten Originalunterlagen an die zuständige Organisationseinheit (Haushaltsbeauftragter oder Personalverwaltung) zurückzugeben und dort unverzüglich zu vernichten. Das ist zu protokollieren.
4. Die Personalverwaltung kann vom Personalrat über die Datensicherungsmaßnahmen Auskunft verlangen.
5. Allgemein: Der behördliche Datenschutzbeauftragte sollte bei der Verarbeitung personenbezogener Daten verstärkt durch die Personalvertretungen als Berater in Anspruch genommen werden.

Aus Gründen einer einheitlichen und regelmäßigen Verfahrensweise habe ich darüber hinaus allgemein angeregt, dass Dienststellenleitung und Personalrat den jeweils wiederkehrenden Datenaustausch zwischen Personalrat und Dienststelle protokollarisch festlegen und dass die Beschäftigten hierüber informiert werden.

Was die automatisierte Verarbeitung der Beschäftigtendaten angeht, gelten im übrigen weiterhin die in 4/5.2.1 aufgestellten Grundsätze.

5.3 Einwohnermeldewesen

5.3.1 Zulässigkeit von Adressbüchern

Regelmäßig erhalte ich Petitionen, in denen sich Bürger darüber beschweren, dass ihre Daten in Adressbüchern aufgenommen worden sind oder aufgenommen werden sollen. Nach dem Sächsischen Meldegesetz (SächsMG) können Meldedaten der Einwohner an die Herausgeber von Adressbüchern weitergegeben werden. Der Bürger

hat allerdings die Möglichkeit, beim Einwohnermeldeamt gegen diese beabsichtigte Datenverarbeitung innerhalb einer bestimmten Frist Widerspruch nach § 33 Abs. 4 SächsMG einzulegen, wenn er nicht schon vorher eine Auskunftssperre nach § 34 SächsMG beantragt hatte und diese eingetragen worden ist. Der Hinweis auf die Widerspruchsmöglichkeit ist durch die Gemeinde ortsüblich bekannt zu machen. Diese erfolgt leider meist nur im Amtsblatt. Insofern werden die rechtlichen Grundlagen jedoch noch nicht eingehalten. Die Gemeinden haben über die Veröffentlichung im Amtsblatt hinaus verstärkt und zusätzlich in den Medien auf die melderechtlichen Möglichkeiten des Widerspruchs hinzuweisen, da Veröffentlichungen im Amtsblatt nach allgemeiner Lebenserfahrung weniger wahrgenommen werden, als Veröffentlichungen in der Tagespresse (vgl. 3/5.3.3.2; 10/5.3.2).

Aufgrund der mich immer wieder erreichenden Eingaben habe ich jedoch den Eindruck gewonnen, dass die Bürger nicht über die melderechtliche Zulässigkeit der Verarbeitung von Einwohnermeldedaten und über eine mögliche Weitergabe ihrer Daten informiert sind. Rechtspolitisch ist zu überlegen, ob auf die Weitergabe der zweckgebundenen Daten durch die Meldebehörde gänzlich verzichtet werden oder diese nur bei ausdrücklicher Einwilligung erfolgen kann. Hier ist gegebenenfalls der Gesetzgeber gefordert.
Für die Weitergabe von Daten an die Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen durch die Meldebehörde gelten übrigens die gleichen Widerspruchsmöglichkeiten. Auch hier ist eine nur geringe Akzeptanz auf Seiten der Bürger in Bezug auf die Übermittlung von Einwohnermeldedaten feststellbar. In diesem Zusammenhang verweise ich auf meine grundsätzlichen Ausführungen zu Gruppenauskünften an politische Parteien, Wählergruppe und andere Träger von Wahlvorschlägen in meinem 3. Tätigkeitsbericht in Nr. 5.3.3.3 sowie – vor dem Wahljahr 2004 – auf meinen 6. Tätigkeitsbericht in Nr. 5.3.8.

5.3.2 Auskünfte über Meldedaten an die Feuerwehr

In einem wegen seiner besonderen Umstände rührenden Fall wandte sich ein Ehepaar wegen einer erteilten Auskunft aus dem Melderegister an die Feuerwehr an mich. Zu dem Sohn der Eheleute war eine Auskunftssperre eingetragen. Die Auskunftssperre war wegen einer Inkognitoadoption, bei der ein Offenbarungs- und Ausforschungsverbot (§ 1758 BGB) besteht, vermerkt worden. Daher gingen die Adoptiveltern auch davon aus, dass aufgrund der Auskunftssperre eine Datenweitergabe generell ausgeschlossen sei. Die Feuerwehr erhielt die Daten und verwendete sie, um den Eheleuten einen Gebührenbescheid für die Inanspruchnahme eines Notfalltransports für ihr Adoptivkind zuzustellen. Dabei lag der Einsatz des Rettungsdienstes vor dem Adoptivzeitpunkt.

Meine Prüfung ergab, dass zwar die Übermittlung der Daten, insbesondere auch zum gesetzlichen Vertreter des Kindes, dem Grunde nach zulässig waren (§ 29 Abs. 1

SächsMG). Es handelte sich nämlich um eine Übermittlung innerhalb des öffentlichen Bereichs. Hier gilt eine Auskunftssperre gerade nicht. Die Meldebehörde wies auch auf die eingetragene Auskunftssperre hin. Nur ungenügend erfolgte in meinen Augen die gemäß § 29 Abs. 3 Satz 2 SächsMG vorzunehmende Prüfung. Nach der Vorschrift hat die Meldebehörde dann, wenn der Einzelfall Anlass für eine weitergehende Prüfung gibt, die konkrete Zulässigkeit der Datenübermittlung zu überprüfen. Im vorliegenden Fall hätte, bei bekannter Auskunftssperre, durchaus Anlass für eine weitergehende Prüfung der konkreten Datenweitergabe bestanden (In unproblematischen Fällen ist nur zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt.).

Letztendlich trug auch die empfangende Behörde, die Feuerwehr, Verantwortung für die Zulässigkeit der Datenweitergabe. Für diese war die Datenweitergabe nicht erforderlich. Sie wäre nur dann erforderlich gewesen, wenn das Adoptivelternteil zum Leistungszeitpunkt der Feuerwehr schon gesetzlicher Vertreter des Kindes gewesen wäre. Die Feuerwehr hätte die Meldedaten bezogen auf den konkreten Gebührenfall (und Zeitpunkt) abfragen müssen.

Meine Feststellungen in dieser Angelegenheit haben die Meldebehörde für vergleichbare Anfragen von Behörden sensibilisiert und bei eingetragenen Auskunftssperren nach § 34 Abs. 4 SächsMG zu zusätzlichen Maßnahmen veranlasst, die eine Wiederholung ausschließen sollen. Danach müssen Auskunftsersuchen von Behörden schriftlich gestellt werden und den Grund und Zweck der Anfrage sowie den maßgeblichen Zeitpunkt benennen. Durch den Sachgebietsleiter in der Meldebehörde wird nunmehr geprüft, ob das Auskunftsersuchen im Rahmen der Aufgaben der anfragenden Stelle liegt; gegebenenfalls wird der Nachweis schriftlich angefordert.

5.4 Personenstandswesen

In diesem Jahr nicht belegt.

5.5 Kommunale Selbstverwaltung

5.5.1. Katastrophenwarndienst via SMS oder Mail

Auf seiner Homepage wendet sich das Landratsamt Weißeritzkreis mit folgenden Worten an die Kreisbewohner: „Während der Hochwasserkatastrophe im Herbst 2002 wurden geeignete Alarmierungs- und Informationsmittel vermisst. Es gab zu wenig Sirenen und zudem existiert kein Sirenensignal für den Katastrophenschutz. Lautsprecherwagen waren ebenfalls viel zu wenig vorhanden. Somit funktionierte die Warnung der Bevölkerung nicht gut. Wir wollen nun einen anderen Weg beschreiten, der unseres Erachtens bundesweit einmalig ist: die Information über SMS / E-Mail.

Sie können ab sofort in dem entsprechenden Modul Ihre Handynummer eintragen http://weisseritzkreis.com.

„Der technische Stand lässt es zu, ganz gezielt zu informieren, so dass beispielsweise unterschiedlich betroffene Gebiete zielgenauer alarmiert werden können. Zudem ermöglicht das System auch die unmittelbare Benachrichtigung von Einsatzkräften in den jeweiligen Gemeinden."

Dieser Service ist gegenüber der Bevölkerung eine freiwillige Leistung, die durch die Landkreisverwaltung über die einschlägigen Regelungen des Sächsischen Katastrophenschutzgesetzes hinaus angeboten wird. Die zu ihrer Umsetzung erforderliche Datenerhebung habe ich geprüft und für zulässig erachtet. Zwar ist Katastrophenschutz grundsätzlich Ländersache, und der Landesgesetzgeber hat (ebenfalls bislang noch) darauf verzichtet, die Art und Weise der Informationsübertragung für Katastrophenfälle zu normieren. Gleichwohl erfüllen die Landkreise, soweit die Gesetze nichts anderes bestimmen, überörtliche Aufgaben in eigener Verantwortung (§ 2 Abs. 1 Satz 1 SächsLKrO). Um eine solche Aufgabe handelt es sich vorliegend, denn die Unterrichtung und Beratung der Einwohner über bedeutsame Angelegenheiten des Wirkungskreises gehört zum Wesen kommunaler Selbstverwaltung i. S. v. § 10 Abs. 1 SächsLKrO (vgl. § 11 Abs. 1 SächsGemO).

Dem Grunde nach bestehen daher also keine datenschutzrechtlichen Einwände gegen dieses sinnvolle Vorhaben. Die Freiwilligkeit der Datenübermittlung ist jedoch durch geeignete Mittel sicherzustellen. Im Weißeritzkreis ist dafür die folgende Formulierung gewählt und auf der Homepage gut sichtbar angebracht worden:

Wichtiger Hinweis zum Datenschutz:
Die von Ihnen eingegebenen Daten werden in einer Datei gespeichert. Die erfassten Daten werden ausschließ-lich für die Warnung und Information bei Katastrophenereignissen verwandt. Ein Zugriff Dritter auf diese Daten ist ausgeschlossen. Im Falle einer Verweigerung entstehen Ihnen keinerlei rechtliche Nachteile - Sie können dann lediglich nicht an unserem Warnsystem teilnehmen. Mit der Eingabe Ihrer Daten und dem abschließenden Klick auf den Button „Neu anlegen" auf der zweiten Seite der Anmeldemaske erklären Sie Ihre Einwilligung zum elektronischen Nachhalten Ihrer Daten (§ 4 Abs. 1 Sächsisches Datenschutzgesetz).

Mit diesem Hinweis habe ich mich einverstanden erklärt.

Es ist zu begrüßen, wenn der Einsatz neuer Kommunikationsmittel in künftigen Gefahrensituationen eine dadurch *raschere* Information ermöglicht und ein Zusammenwirken aller beteiligten Stellen den Schutz von Menschen und Sachgütern besser als bisher gewährleisten kann. Dass dies in datenschutzgerechter Weise erfolgen kann, wird am positiven Beispiel aus dem Weißeritzkreis gezeigt. Allerdings erinnere ich

daran, dass bei der Flut elektrische und elektronische Verbindungen ausgefallen sind. Die gute alte handgekurbelte Sirene wird durch Handys nicht ersetzt.

5.5.2 Bekanntmachung eines Hausverbots durch öffentlichen Aushang

Ich wurde darauf aufmerksam gemacht, dass im Eingangsbereich des Sozialamtes einer kreisfreien Stadt ein befristetes Hausverbot für eine mit Vor- und Zunamen sowie Anschrift bestimmte Person mit Aushang bekannt gemacht wurde. Dem Betroffenen wurde gleichzeitig per Brief das Hausverbot zugestellt. Der Aushang verursachte in der Gemeinde Aufsehen. Eine sächsische Zeitung behandelte den Vorgang in einem Artikel. Der Betroffene wurde dabei unter Nennung des Vornamens und mit dem ersten Buchstaben seines Nachnamens erwähnt. Die Auffassung der Behörde wurde in dem Pressebeitrag wiedergegeben.
Mir gegenüber begründete die Stadtverwaltung ihr Vorgehen mit der Uneinsichtigkeit des Betroffenen, der schon in der Vergangenheit mehrmals nicht als Antragsteller, sondern in unzumutbarer Weise in nicht amtsbezogenen Angelegenheiten gegenüber den Mitarbeitern der Sozialbehörde in Erscheinung getreten sei. Dem Behördenleiter sei es mit dem Aushang des Hausverbots darauf angekommen, die „Mitarbeiter unmittelbar … zu schützen“. Für den Zeitraum bis zur Zustellung des Hausverbotes habe man das Nichtbetreten des öffentlichen Gebäudes durch den Betroffenen unterbinden wollen.

Eine öffentliche Bekanntgabe des Hausverbots als Verwaltungsakt wäre nach § 41 Abs. 3 Verwaltungsverfahrensgesetz nur statthaft gewesen, wenn eine solche Bekanntgabe durch besondere Rechtsvorschrift zulässig gewesen wäre. Daran fehlt es. Teile der Rechtsliteratur vertreten die Ansicht, es handele sich bei einem behördlichen Hausverbot immer um eine Maßnahme mit öffentlich-rechtlichem Charakter. Die Stadt teilte mir hingegen mit, dass das Hausverbot kein Verwaltungsakt gewesen sei, sondern es habe sich um schlichtes Verwaltungshandeln auf zivilrechtlicher Grundlage gehandelt. Hierfür sprach die äußere Form des Hausverbotes. Nach der Rechtsprechung kann sich eine öffentliche Stelle in Ausübung ihres Hausrechts grundsätzlich auch auf die zivilrechtlichen Normen der §§ 859 ff., 903, 1004 BGB stützen (OVG Münster, Beschl. v. 8.10.1997, NJW 1998, 1425). Folgt man dieser Auffassung, beurteilt sich die Zuordnung des Hausverbots (zivilrechtlich oder öffentlich-rechtlich) nach der Rechtsnatur des beabsichtigten bestimmungsgemäßen Gebrauchs der Sache durch den vom Hausverbot Betroffenen. Nach meiner Einschätzung war der Ausspruch eines zivilrechtlichen Hausverbotes möglich. Die rechtliche Einordnung war aber bei der datenschutzrechtlichen Beurteilung im Ergebnis nicht entscheidend. Denn auch bei einem zivilrechtlichen Hausverbot wäre das Sozialamt als öffentliche Stelle im Sinne von § 2 Abs. 1 SächsDSG gehalten gewesen, mit dem Vollzug des Hausverbots einhergehende bzw. nachfolgende Datenverarbeitungen gemäß dem SächsDSG vorzunehmen und Verhältnismäßigkeitsgesichtspunkte zu beachten. Vor-

liegend war dies gerade nicht erfolgt. Für eine Datenübermittlung des Hausverbots mit Personenbezug durch die Bekanntgabe an alle das Gebäude betretende Besucher und Mitarbeiter gab es keine Rechtsgrundlage. Der Bürger muss grundsätzlich nicht damit rechnen, dass eine Behörde mit der er in einer privatrechtlichen Verbindung steht, den Inhalt rechtsgeschäftlicher Handlungen nach außen hin öffentlich macht und offenbart. Auch die besonderen Umstände des Einzelfalls rechtfertigten es nicht, dass eine Bekanntgabe in der vorgenommenen Weise erfolgte. Abgesehen von der durchaus in Zweifel zu ziehenden Geeignetheit der Maßnahme, dass nämlich ein Betroffener durch einen derartigen Aushang vom Betreten abgehalten (und nicht zusätzlich provoziert) wird, konnte nicht von einer Gefahr für Leib oder Leben (z. B. bei Allgemeingefährlichkeit) ausgegangen werden, die besondere Vorkehrungen gerechtfertigt hätten. Es hätte daher ausgereicht, dass das Hausverbot zur Sicherung des Betriebsablaufs vollzogen worden wäre. Hierzu hätte die Bekanntgabe an den Betroffenen mit dem Brief und eine ausschließlich interne Information an die Mitarbeiter des Amtes, die mit dem Betroffenen in Kontakt kommen könnten, Leiter von Organisationseinheiten sowie Mitarbeiter mit Sicherheitsaufgaben genügt. Dem Aushang kam hingegen durch die eindeutige Bezeichnung des Betroffenen mit Vor-, Zuname und Anschrift eine prangerähnliche Wirkung zu. Der Betroffene wurde hierdurch in unverhältnismäßiger Weise öffentlich bloßgestellt und in seinem Recht auf informationelle Selbstbestimmung verletzt.

Ich habe gegenüber der Stadtverwaltung die Unzulässigkeit der Datenverarbeitung deutlich gemacht. Das Sozialamt hatte den Aushang zwischenzeitlich schon wieder entfernt. Ich gehe davon aus, dass die Stadtverwaltung in zukünftigen Fällen die zu ergreifenden Maßnahmen sorgfältig abwägt.

5.5.3 Druck von Lohnsteuerkarten als Datenverarbeitung im Auftrag

Einer Stadtverwaltung wurde durch ein privates Unternehmen der Druck, der Versand und die Datenaufbereitung der jährlich auszureichenden Lohnsteuerkarten angeboten. Die Stadtverwaltung fragt, ob sie diese Leistung in Anspruch nehmen darf.

Nach § 39 EStG ist es Aufgabe der Gemeinden, den Bürgern, die Arbeitnehmer sind, rechtzeitig für jedes Kalenderjahr unentgeltlich eine Lohnsteuerkarte nach amtlich vorgeschriebenem Muster auszustellen und die persönlichen Daten einzutragen. Die Gemeinden sind, soweit sie die Lohnsteuerkarten auszustellen und zu übermitteln sowie Eintragungen vorzunehmen und zu ändern haben, örtliche Landesfinanzbehörde.

Die Lohnsteuerkarten sind gemäß Nr. 4 des jährlichen Merkblattes die Oberfinanzdirektion für die Gemeinden über die „Ausstellung und Übermittlung der Lohnsteuerkarten“ im allgemeinen Ausstellungsverfahren durch die Meldestellen der Gemeinden

selbst, oder durch ein beauftragtes Privatunternehmen auszustellen und zu drucken. Bei Versand der Lohnsteuerkarten durch ein Privatunternehmen muss die Gemeinde als versendende Behörde erkennbar sein und selbst den Tag des Versandes bestimmen. Von den Privatunternehmen dürfen deshalb Freistempler mit dem Firmennamen verwendet werden.

Datenschutzrechtlich handelt es sich bei der Beauftragung eines Privatunternehmens mit dem Ausdruck bzw. der Kuvertierung und Verteilung der Lohnsteuerkarten – bezogen auf den Auftragnehmer – um Datenverarbeitung im Auftrag. Hierbei sind die Regelungen des § 7 SächsDSG zu beachten. Danach bleibt der Auftraggeber (hier die Gemeinde) für die Einhaltung datenschutzrechtlicher Vorschriften (und somit des § 30 AO) verantwortlich. Die Gemeinde hat den Auftragnehmer hinsichtlich dessen Eignung *sorgfältig* auszuwählen.

Der Schutz des Steuergeheimnisses durch § 30 AO, § 355 StGB muss bei der Vergabe von Aufträgen außerhalb der Finanzverwaltung allerdings sichergestellt bleiben.

Die Beschäftigten (und ggf. der Unternehmer) des beauftragten Privatunternehmens sind deshalb durch die Meldestellen nach § 6 SächsDSG und § 1 Verpflichtungsgesetz zur gewissenhaften Erfüllung der Obliegenheiten förmlich zu verpflichten und auf die strafrechtlichen Konsequenzen von Pflichtverletzungen hinzuweisen. Dadurch werden sie Amtsträgern i. S. v. § 30 Abs. 1 i. V. m. § 7 AO gleichgestellt.

Im Übrigen halte ich es für erforderlich, den ordnungsgemäßen Ablauf der durchzuführenden Arbeiten durch einen Bediensteten der auftraggebenden Behörde überwachen zu lassen und im Fall der Versendung von Lohnsteuerkarten den zwischen den Gemeinden und dem Privatunternehmen zu schließenden Vertrag hinsichtlich der erforderlichen Bestimmungen durch das zuständige Finanzamt, zumindest stichprobenhaft, überprüfen zu lassen.

5.5.4 Plaudertaschen im Gemeinderat

In letzter Zeit häufen sich in Sachsen (gelegentlich bewusste) Fehler, Versäumnisse und Unsicherheiten der Gemeinderäte/Kreistage im Umgang mit personenbezogenen Daten. Man kann in diesem Zusammenhang nicht auf alle möglichen Konstellationen eingehen, sollte aber folgende Grundsätze in Erinnerung rufen:
Der Gemeinderat/Kreistag ist kein Parlament. Er ist ein demokratisch legitimiertes Hauptorgan der Gemeinde/des Landkreises. Ihm kommt lediglich die kommunalpolitische Führung im Sinne der politischen Vertretung der Bürgerschaft zu, Art. 28 Abs. 1 Satz 2 GG. Es gibt auf kommunaler Ebene keine Gewaltenteilung oder Gewaltenverschränkung; vielmehr ist der Stadtrat Teil der Stadtverwaltung, nämlich das Hauptorgan der Kommune. Die Datenübermittlung von den Fachämtern über den

Bürgermeister an den Stadtrat ist zwar eine Übermittlung im Rechtssinne, weil die einzelnen Stellen der Verwaltung, der Bürgermeister und der Gemeinderat jeweils unterschiedliche öffentliche Stellen sind und unterschiedliche gesetzliche öffentliche Aufgaben zu erfüllen haben. Wegen der letztlich im Grunde lückenlosen Kontroll- und Mitentscheidungsbefugnisse des Gemeinderates (im Grundsätzlichen ist das in der Gemeindeordnung, im Einzelnen in der Geschäftsordnung geregelt) besteht aber eine unter Berücksichtigung des Grundrechts auf informationelle Selbstbestimmung weitgehend lückenlose Übermittlungsbefugnis in Bezug auf alle personenbezogenen Vorgänge, die in der Verwaltung bearbeitet werden, sofern die Formalien für eine Ratsbefassung erfüllt sind.

Wenn der Bürgermeister nur die „Fraktionsvorsitzenden“ oder nur die „Obleute“ informiert, sollten die roten Lichter angehen: Denn derartige „Organe“ des Gemeinderates/Kreistages kennt die Gemeindeordnung/Landkreisordnung nicht; sondern nur den „Ältestenrat“, der aber keine inhaltlichen Entscheidungsbefugnisse hat, sondern lediglich in (formalen) Fragen der Tagesordnung und des Ganges der Verhandlungen den Bürgermeister berät. Der Gemeinderat/Kreistag ist eine homogene und in sich nicht unterteilte und unterteilbare öffentliche Stelle. Jedes Gemeinderats-/Kreistagsmitglied hat gleiche Rechte und gleiche Pflichten. Auf freiwilliger Basis kann naturgemäß jedes Gemeinderats-/Kreistagsmitglied ein anderes Mitglied mit seinen Kompetenzen, z. B. zur Akteneinsicht oder zur Entgegennahme oder Behandlung besonderer Informationen, z. B. von Stasi-Unterlagen, betrauen. Das bedeutet aber nicht, dass der Bürgermeister - ohne dass eine solche Beauftragung vorläge - selektieren dürfte, wem er Informationen gibt, und wem nicht. Insbesondere ist das „Fraktionsdenken“ in Gemeinderäten/Kreistagen fehl am Platze: Die Fraktionen sind letztenendes die „Kinder der Parteien“. Ihre Bildung ist nicht selten der Grund dafür, dass sich die Parteilichkeiten in die Gemeinderäte/Kreistage hinein fortsetzen und sogar fortentwickeln. Das ist regelmäßig schädlich für die kommunale Willensbildung. Es gibt auf kommunaler Ebene keine „roten“ oder „schwarzen“ Kanaldeckel. Vielmehr ist es Aufgabe des Hauptorgans, für eine objektive, neutrale und unparteiliche und ausschließlich sachbezogen agierende Verwaltung zu sorgen und ideologische Ausrichtungen und dergleichen außerhalb der Gemeinderats-/Kreistagsberatungen zu lassen.

Diese Gedanken sind für den einen oder anderen Gemeinderat oder für das eine oder andere Kreistagsmitglied nur schwer verdaulich. Sie meinen nämlich, sie hätten ein öffentliches Mandat ähnlich oder gar gleich dem eines Parlamentariers. Das ist nicht der Fall. Das ergibt sich u. a. aus den Regelungen des Strafrechts zur Schweigeverpflichtung: Gemäß § 203 Abs. 2 Nr. 4 (genau lesen!) StGB machen sich die echten Parlamentarier (Landtagsabgeordnete, Bundestagsabgeordnete, Abgeordnete des Europäischen Parlaments) nicht strafbar, wenn sie Amtsgeheimnisse ausplaudern. Ganz anders sieht es bei den Gemeinderats- und Kreistagsmitgliedern aus: Wird der gemäß § 205 StGB erforderliche Strafantrag gestellt, so können sie einem staatsanwaltschaft-

lichen Ermittlungsverfahren und anschließend einem strafrechtlichen Gerichtsverfahren unterzogen werden, wenn sie die ihnen obliegenden Schweigepflichten verletzen. Nicht nur derjenige, dessen Daten ausgeplaudert wurden, kann den Strafantrag stellen, sondern auch daneben der Bürgermeister/Landrat, der gemäß § 77 a Abs. 3 StGB eine gesetzliche Strafantragsbefugnis besitzt. Ist der Landrat/Bürgermeister selbst die Plaudertasche, so ist die Kommunalaufsichtsbehörde berufen, den Strafantrag zu stellen. Ich würde mir wünschen, wenn häufiger von dieser Antragsbefugnis Gebrauch gemacht würde, damit das gelegentlich anzutreffende gesteigerte Mitteilungsbedürfnis (früher nannte man das Schwatzhaftigkeit) auf kommunaler Ebene endlich ein Ende findet. Am Rande bemerkt: Kaum eine Strafvorschrift wird in Deutschland so häufig verletzt, wie die des § 203 Abs. 2 StGB - schauen Sie sich doch Kantinengespräche, abendliche Partei- und Party-Veranstaltungen oder bestimmte Interessentenkreise daraufhin einmal genauer an. Es ist ein Glück, dass Telefonate grundsätzlich nicht abgehört werden ...

5.5.5 Hundebestandsaufnahme bei Grundstückseigentümern

Das Steueramt einer westsächsischen Stadt wandte sich unter Bezugnahme auf die gemeindliche Hundesteuersatzung mit einem Erhebungsbogen an sämtliche Eigentümer von Hausgrundstücken im Gemeindegebiet und forderte diese mit Fristsetzung auf, die Namen der unter der Grundstücksadresse ansässigen Hundebesitzer mitzuteilen. Darüber hinaus sollten die Eigentümer Angaben über die Anzahl der gehaltenen Hunde, die Hunderassen und den zeitlichen Beginn der Hundehaltung machen. Gegenüber den Grundstückseigentümern wurde die Auskunftspflicht für die Angaben mit Hinweis auf § 93 AO begründet.

Die Datenverarbeitung war in mehrfacher Hinsicht unzulässig. Ich habe das zuständige Innenministerium auf den Vorgang aufmerksam gemacht und die Auffassung vertreten, dass zum einen die Grundsteuer-Adress-Daten der Grundstückseigentümer nicht zweckgemäß verwendet wurden, denn sie wurden nicht für Zwecke der Grundsteuer genutzt, sondern zu einem anderen Zweck, nämlich der Aufklärung von Hundesteuerverhältnissen. Dies war nach § 13 Abs. 3 SächsDSG nicht zulässig. Darüber hinaus überging die Gemeinde bei ihrer Vorgehensweise einen wesentlichen Verfahrensgrundsatz. Öffentliche Stellen können nicht voraussetzungslos Daten von Betroffenen bei Dritten erheben, sondern nur in den gesetzlich vorgesehenen Grenzen. Nicht alle Eigentümer sind selbst Hundehalter, so dass die Befragung mit dem Erhebungsbogen an die Eigentümer auch eine Datenerhebung bei Dritten darstellte. Diese war aber nach der von der Gemeinde als Rechtsgrundlage in Anspruch genommenen Vorschrift der Abgabenordnung nur unterstützend zulässig. So können nach § 93 Absatz 1 Satz 3 AO andere Personen als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder Erfolg verspricht. Dritte sollen mithin regelmäßig nicht in das

Besteuerungsverfahren einbezogen werden. Die Satzung habe ich daher als nicht im Einklang mit höherrangigem (Bundes-)Recht angesehen und das Ministerium gebeten, den Vorgang datenschutzrechtlich zu prüfen. Das Innenministerium ist meinen Bedenken im wesentlichen gefolgt und hat unverzüglich reagiert. Nach dessen Auffassung sind zunächst die potentiellen Hundehalter und deren volljährige Haushaltsangehörige zur Auskunft heranzuziehen, bevor weitere Dritte in Anspruch genommen werden können. Es hat die für die Stadt zuständige Rechtsaufsichtsbehörde angewiesen, der Gemeinde einen entsprechenden rechtlichen Hinweis zu erteilen. Die Durchführung der Hundebestandsaufnahme mit Hilfe der Grundstückseigentümer ist daraufhin eingestellt worden.

5.6 Baurecht; Wohnungswesen

5.6.1 Internet und Amtsblatt als Pranger bei Bauvorhaben

Durch einen Hinweis stieß ich auf eine Internet-Seite einer Gemeinde, auf der diese ihr Gemeindeblatt online veröffentlichte. In einer der Ausgaben erörterte der Bürgermeister der Gemeinde ein Straßenbauvorhaben, das von einer zahlenmäßig kleinen Bürgerinitiative in Frage gestellt wurde. In der Veröffentlichung verteidigte das Gemeindeoberhaupt das Bauvorhaben und benannte zwei Einwohner und Mitglieder der Bürgerinitiative mit Vor- und Zunamen bei für diese negativer Bezugnahme auf das „Gemeinwohl“ und die „Interessen Einzelner“. Daneben wurden in plakativer Weise die für die meisten Bürger - nach Prognose des Bürgermeisters - negativen Folgen bei einem Verzicht auf die Baumaßnahme dargestellt.
Zunächst: Es ist bedauerlich, wenn ein sächsischer Bürgermeister heute meint, mit dem bloßen Hinweis auf Mehrheitsentscheidungen des Stadtrates das „Gemeinwohl“ gepachtet zu haben. Das Gemeinwohl ist das Wohl aller Einzelnen, nicht mehr. Und diese „Interessen Einzelner“ dürfen im öffentlichen Schlagabtausch nicht deshalb diskriminiert werden, weil sie „einzeln“ sind. Der Bürgermeister sollte statt verfassungsrechtlichen Unfugs lieber Sachargumente vortragen. Weil diese ihm fehlten, er sich jedenfalls nicht imstande sah, sie vorzutragen, griff der Bürgermeister zum groben Keil - dem öffentlichen Pranger.

Den amtlichen Veröffentlichungen bei Gemeinden kommt regelmäßig ein starkes örtliches Interesse zu. In den Augen der Bevölkerung haben sie zudem ein hohes Maß an Glaubwürdigkeit und Objektivität, wie es die übrige Tagespresse nie erfährt. Es handelt sich eben um eine amtliche Veröffentlichung. Dem sollten sich Bürgermeister bzw. kommunale Amtsträger bewusst sein. Sie sind nach der Gemeindeordnung bzw. der Landkreisordnung in erster Linie Amtspersonen, repräsentieren die ganze Gemeinde bzw. den Landkreis.
Dementsprechend werden Bürger, die in personenbezogener Weise in der kommunalen Gemeinschaft durch offizielle Veröffentlichungen bzw. durch ein Gemeindeorgan

angegriffen werden, in besonderer Weise bloßgestellt und in ihren Grundrechten verletzt.

Die Informationsweise der Stadtverwaltung war in der durchgeführten Weise nicht erforderlich und stellte eine unzulässige Datenverarbeitung dar. Eine Kommune kann die Information ihrer Bürger nach § 11 SächsGemO, § 10 SächsLKrO nicht unbeschränkt betreiben. Sie ist an die Gesetze und das Verhältnismäßigkeitsprinzip gebunden. Die Darstellung der streitigen Interessen war im vorliegenden Fall problemlos ohne Herstellung eines Personenbezugs möglich. Die (sachliche) Auseinandersetzung mit gemeindlichen Angelegenheiten kann grundsätzlich in einem Gemeindeblatt erfolgen, doch sind bei der Verarbeitung personenbezogener Daten wegen der möglichen nachteiligen Wirkungen selbstverständlich die datenschutzrechtlichen Bestimmungen sorgsam zu beachten. Auch mittelbare Hinweise auf Privatpersonen sind zu unterlassen. Behörden müssen bürgerlichen Widerspruch dulden und ihm rein sachbezogen begegnen. Die Datenverarbeitung stellte einen Verstoß gegen § 15 SächsDSG dar. Auf meinen Hinweis hin änderte die Gemeinde unverzüglich die Internet-Ausgabe und verzichtete auf die namentliche Nennung der beiden Bürger. Ich habe daher von einer Beanstandung absehen können.

Bei einem weiteren Vorgang erhielt ich auf Nachfrage hin die Information, dass eine Gemeinde Informationen über einen sich mit ihr im Streit befindenden Investor im Gemeindeblatt veröffentlichte. Es handelte sich um eine mit grauem Hintergrund hervorgehobene und mit Fettdruck überschriebene Mitteilung. In dieser wurde der Investor mit Vor- und Zunamen im Zusammenhang mit Meinungsverschiedenheiten mit der Gemeinde benannt. Darüber hinaus enthielt die Nachricht die Information, dass der Betroffene seit einem bestimmten Zeitpunkt aufgrund eines ärztlichen Attests „komplett verhandlungsunfähig“ gewesen sei. Diese Information hatte die Gemeinde wiederum angeblich von einem unbekannten Dritten zugespielt bekommen. Selbst wenn es sich um eine zutreffende Angabe gehandelt haben mag, war die Datenverarbeitung nicht zulässig. Die Veröffentlichung und Datenübermittlung des Gesundheitsdatums war in diesem Fall ohne die Nennung des Namens des Betroffenen nicht sinnvoll möglich, aber schlichtweg auch nicht zur Erfüllung der gemeindlichen Unterrichtungspflicht nach § 11 SächsGemO im Sinne von § 15 SächsDSG erforderlich. Die Verletzung des Rechts auf informationelle Selbstbestimmung des Betroffenen war offenkundig. Aufgrund der besonderen Kooperation und Einsicht der Gemeindeverwaltung bin ich sicher, dass sich ein solches Vorkommnis in dieser Kommune nicht wiederholen wird.

Nochmals: Es gibt keine „Waffengleichheit“ zwischen Behörden und Bürgern: Was diese dürfen, darf die Obrigkeit noch lange nicht.

5.6.2 Weitergabe von Bürgereinwendungen gegen ein Bauvorhaben an den Investor

Ferner habe ich um die notwendigen Einwirkungen innerhalb der Staats- und Kommunalverwaltung gebeten, damit auch die Datenübermittlung, die ich beanstandet habe, sich nicht wiederholt. Die Wiederholungsgefahr bestand ganz offensichtlich, denn der Baudezernent der betreffenden Gemeinde hatte sich gegenüber der Presse wie folgt geäußert: „Das ist seit Jahren gängige Praxis. Wir geben die Einwände an das beauftragte Ingenieurbüro und dieses reicht die Unterlagen an den Investor weiter. Schließlich müssen die Unterlagen ja ausgewertet werden."

Eine Rechtsgrundlage für die Übergabe der Unterlagen an den Investor kann ich jedenfalls im Bauleitplanungsverfahren nicht erkennen und zwar aus folgenden Gründen:
Die Planungshoheit liegt in der Bauleitplanung bei der Gemeinde. Sie hat - gebunden an Recht und Gesetz - die Bürgereinwendungen im Einzelnen auszuwerten und unter planungsrechtlichen und tatsächlichen Gesichtspunkten - neutral - zu bewerten. Diese Prüfung nach § 3 Abs. 2 Satz 4 BauGB kann die Kommune nach § 4 b BauGB zwar einem Dritten übertragen. Gegenstand dieser partiellen Verfahrensprivatisierung ist aber lediglich die *Vorbereitung* der planerischen Abwägung, weil die Bewertung selbst nach § 1 Abs. 6 BauGB Aufgabe der Gemeinde bleibt, die sie - unübertragbar - selbst zu erledigen hat. Der Akt der Verwaltungsprivatisierung, der hier gesetzlich vorgesehen ist, belässt folglich die volle Verantwortlichkeit bei der Gemeinde, die bei der Abwägung den Grundsatz der Verhältnismäßigkeit zu beachten hat. Gleiches gilt auch in der vorhabenbezogenen Bauleitplanung, siehe § 11 Abs. 1 Nr. 1, 3. Halbsatz BauGB. Der Dritte als Projektmittler hat deshalb lediglich verwaltungsinterne, also vorbereitende Arbeiten, zu erledigen. Er ist deshalb kein beliehener Unternehmer.

Dieser Dritte muss fachkundig sein. Dies ist bei einem „Investor" (was auch immer sich hinter diesem Begriff zu verbergen vermag) üblicherweise nicht der Fall. Diese Fachkunde setzt vielmehr eine Spezialisierung, z. B. als Planungs- oder Architekturbüro voraus.

Der Dritte darf kein eigenes wirtschaftliches Interesse am Zustandekommen einer bestimmten Planungsversion haben. Die Grundsätze der Befangenheit von Ratsmitgliedern sind vielmehr sinngemäß zu berücksichtigen. Und die Möglichkeit des § 4 b BauGB darf diese Regeln nicht unterlaufen. Denn wenn schon ein Ratsmitglied von der Meinungsbildung ausgeschlossen ist, so muss auch ein „Dritter" dann von der - immerhin häufig maßgeblichen - Vorbereitung der Entscheidung ausgeschlossen sein, wenn er selbst ein persönliches Interesse am Zustandekommen des Planungsvorhabens verfolgt. Der Dritte muss also so neutral wie möglich sein, um seiner eigentlichen Rolle als Mediator genügen zu können (siehe dazu z. B. Battis u. a. BauGB, 8. Auflage, München 2002, § 4 b Rdnr. 6).

Jedenfalls lässt sich feststellen, dass das Baugesetzbuch weder in § 11 noch in § 12 die Einschaltung des Vorhabenträgers in die Datenverarbeitung der Einwendungen vorsieht.

Deshalb dürfen die personenbezogenen Daten der Einwender nicht einer vom Investor beherrschten (z. B. von ihm bezahlten) Gesellschaft oder gar ihm selbst übermittelt werden.

In diesem Punkt sind Verfahren im Bauplanungsrecht eben anders zu bewerten als z. B. Planfeststellungsverfahren (siehe § 73 Abs. 6 Satz 1 VwVfG) oder Verfahren nach dem Immissionsschutzgesetz (siehe § 10 Abs. 6 Satz 1 BImSchG und § 12 Abs. 2 Satz 1 BImSchV). Denn dort sieht der Gesetzgeber ausdrücklich die Datenübermittlung vor oder er setzt sie voraus, weil die Einwendungen mit dem Vorhabenträger oder Antragsteller - natürlich nach rechtsstaatlicher Vorbereitung im Sinne rechtlichen Gehörs - zu erörtern sind.

In diesen Fällen, in denen die Daten einem Privaten zu übermitteln sind, müssen die Daten der Einwender frühestmöglich von der Gemeinde anonymisiert werden. Dazu zwingt der Grundsatz der Verhältnismäßigkeit, also die Datensparsamkeit, die als datenschutzrechtliches Prinzip immer zu beachten ist. Zumindest muss eine Pseudonymisierung der Daten und - soweit möglich - eine Aggregierung der Daten versucht werden. Aus der Sicht des Einwenders geht es ja darum, dass er seine persönlichen Verhältnisse der Gemeinde, also einer aus seiner Sicht neutralen und gesetzlich gebundenen Institution oder deren neutralem und sachverständigen Beauftragten zuweist und nicht dem privatrechtlich agierenden und datenschutzrechtlich relativ ungebundenen Investor, der seine privaten Interessen - so löblich sie im Einzelfall sein mögen - gegen die Interessen der Einwender durchsetzen will. Der Betroffene will in seiner demokratischen Willensbildung und in seiner gesetzlich gewollten, rechtsstaatlich organisierten Verfahrensbeteiligung nicht durch einen Investor beeinflusst oder gar bedrängt werden („Wild-Ost“ ist zu vermeiden).

Von diesem vorgenannten Grundsatz darf es nur dann Ausnahmen geben, wenn es im konkreten Fall auf die Person des betroffenen Einwenders und auf die von ihm konkret dargelegten Belange ankommt. Hier sind Abwägungen im Einzelfall anzustellen, nämlich genau zu überlegen, ob die konkrete personenbezogene Datenübermittlung geeignet, erforderlich und auch - wenn z. B. Pressionen zu befürchten sind - zumutbar ist, um die gesetzlich gebotene Erörterung angemessen vorzubereiten bzw. die beiderseitigen planungsrechtlichen Beteiligungsrechte zu verwirklichen.

Nach alledem ist es gesetzlich nicht zulässig, Bürgereinwendungen im förmlichen Bauleitplanungsverfahren einem Investor zuzuleiten oder durch das Planungsbüro zuleiten zu lassen.

Diesem Rechtsstandpunkt hat das SMI Folgendes entgegengehalten:

„Die Vorschrift des § 4 b BauGB erlaubt die Beauftragung eines Dritten mit der *Vorbereitung und Durchführung* von Verfahrensschritten nach §§ 2 a bis 4 a BauGB, darunter fällt auch die Bürgerbeteiligung nach § 3 BauGB. Die Übertragung ist insbesondere auch im Rahmen eines städtebaulichen Vertrages gemäß § 11 Abs. 1 Satz 2 auf den Vertragspartner oder im Zusammenhang mit einem Vorhaben- und Erschließungsplan nach § 12 BauGB auf einen Vorhabensträger möglich.

Die Aufgabenübertragung auf den Dritten ist dabei nicht materieller Natur, sondern lediglich funktional. Der Dritte ist dabei schlichter Verwaltungshelfer der Gemeinde, hoheitliche Befugnisse stehen ihm nicht zu. Die zu erfüllende Aufgabe bleibt im Kern staatlich, somit bleibt die alleinige Entscheidungsverantwortung der Gemeinde hinsichtlich der Abwägung der Belange der Bürger durch eine Übertragung von Verfahrensschritten unberührt. Zu den übertragbaren Aufgaben kann jedoch auch die Zusammenstellung und Bündelung der aus der Beteiligung erhaltenen Informationen gehören, also weitestgehend die Vorbereitung der gemeindlichen Abwägung. Selbstverständlich ist der von der Gemeinde beauftragte Dritte als Verwaltungshelfer verpflichtet, mit den an ihn übermittelten personenbezogenen Daten verantwortungsvoll umzugehen und sie nur zweckentsprechend zu verwenden.

Eine vor der Zuleitung der Daten an den Investor erfolgende Anonymisierung der Daten bzw. eine Datenaggregation wäre jedoch in keiner Weise geeignet, eine ordnungsgemäße Abwägung und sachgerechte Entscheidung zu ermöglichen. Es muss im Einzelnen nachvollziehbar sein, in welcher Art und Weise mögliche bauplanerische Entscheidungen den Einwender beeinträchtigen oder begünstigen. Dies ist nur unter Berücksichtigung auch der personenbezogenen Daten des Betroffenen möglich. Allein die statistische Zusammenstellung von typischen Einwendungen kann für den Abwägungsprozess im Sinne von § 1 Abs. 6 BauGB nicht genügen. Eine fehlerfreie Abwägung wäre auf dieser Basis kaum zu bewerkstelligen. Die Qualität der planerischen Entscheidung, die in unmittelbarer Abhängigkeit zur Vollständigkeit der Informationsgrundlagen steht, wäre damit auf jeden Fall ganz entscheidend beeinträchtigt. Darüber hinaus wäre auch das Ziel der Verfahrensbeschleunigung und -vereinfachung durch Übertragung der Durchführung von Verfahrensschritten auf Dritte nach § 4 b BauGB verfehlt.

Grundsätzlich soll im Interesse einer allen Beteiligten gerecht werdenden kooperativen Konfliktlösung im Sinne von § 4 b BauGB ein neutraler Dritter beauftragt werden, der dann quasi als Mediator tätig wird. Streitig wird allerdings in der Fachliteratur die - soweit erkennbar noch nicht judizierte - Frage behandelt, ob als Dritter im Sinne von § 4 b BauGB auch ein Investor mit der Durchführung der Verfahrensschritte, u. a. zur Beteiligung der Bürger nach § 3 BauGB, beauftragt werden kann. Mit Hinweis auf die eventuell fehlende Interessenneutralität wird diese Frage teilweise verneint. Von

anderen Autoren wird differenziert und dem Investor zwar die Vorbereitung, nicht aber die Durchführung von Verfahrensschritten zugesprochen.

Dem Wortlaut des § 4 b BauGB nach ist eine solche einschränkende Auslegung jedoch nicht vorzunehmen. Demzufolge ist es - mit zahlreichen anderen Literaturstimmen - sachgerecht, einen Investor als Dritten nicht per se auszuschließen. Gleichwohl sind in einem solchen Fall die Einwirk- und Aufsichtspflichten der Gemeinde strengeren Voraussetzungen unterworfen. Entscheidend ist, ob und in welchem Umfang die Gemeinde durch eigene Mitwirkung sicherstellt, dass die Aufbereitung des Abwägungsmaterials interessenneutral vorgenommen wird.

Auf Grund der genannten Ausführungen ist aus unserer Sicht die Übergabe schriftlicher Bürgereinwendungen durch die Gemeinde an den Investor zulässig, soweit durch die Gemeinde eine förmliche Übertragung der Durchführung des Verfahrens zur Bürgerbeteiligung auf der Grundlage der aufgeführten Rechtsgrundlagen an den Investor vorher erfolgt ist und die Gemeinde dabei ihren Einwirk- und Aufsichtspflichten gerecht wird.

Ob und inwieweit diese Voraussetzungen im konkreten Einzelfall erfüllt sind, ist anhand des näheren Sachverhalts durch das Regierungspräsidium zu beurteilen und wird in dessen Stellungnahme einfließen."

5.7 Statistikwesen

5.7.1 Statistik im Verwaltungsvollzug: Nutzung der Daten über Beiträge zur Handwerkskammer

Eine mit der Kammerbeitrags-Satzung unzufriedene Innung hatte die Handwerkskammer gebeten, ihr eine Zahlentabelle zur Verfügung zu stellen, in der zu acht Gewinn(= Gewerbeertrags)-Größenklassen jeweils die Anzahl der kammerangehörigen Betriebsstätten (Unternehmen?), davon die mit Rechtsträgern in der Rechtsform der GmbH, sowie die Anzahl der der anfragenden Innung angehörenden Betriebe eingetragen sein sollten.
Nachdem die Kammer das zunächst mit dem recht hergebracht formulierten Hinweis, sie sei „den rechtlichen Gesetzmäßigkeiten unterworfen", und mit der pauschalen Begründung abgelehnt hatte, *die Handwerksordnung und die entsprechenden Datenschutzgesetze stünden* der Erteilung der erbetenen Auskünfte entgegen, weil *im Bereich der sensiblen Handwerkskammerbeiträge das Interesse des einzelnen dem allgemeinen Interesse vorgehe,* hat sich die Innung, als ihr dann noch im Hinblick auf § 13 Abs. 1 SächsDSG erläutert worden war, die von ihr gewünschten Daten könnten nicht der gesetzlichen Aufgabe der Innung - nämlich der Förderung der gemeinsamen gewerblichen Interessen der Innungsmitglieder - dienen, an mich gewandt.

Hier verschanzte sich eine öffentliche Stelle erkennbar hinter dem Datenschutz - oder doch zu recht ?

Betrachten wir zunächst die *Übermittlung*: Die Kammer durfte der Innung ohne weiteres die von dieser gewünschten Tabellenwerte *übermitteln*, sofern die Tabellenwerte nicht niedriger als drei waren. Die allgemeine Regel lautet, anders ausgedrückt: Es müssen die Angaben zumindestens dreier Personen (statistikrechtlich ausgedrückt: Erhebungseinheiten) zusammengefasst sein, dann ist es bei aggregierten Daten ausgeschlossen, dass *eine* bestimmte Angabe *einer* Person zugeordnet werden kann, dann also kein personenbezogenes Datum in den mittels der Tabelle gemachten Angaben enthalten (vgl. Simitis/Dammann Rdnr. 16 zu § 3 BDSG). Man kann sich diese Faustregel am vorliegenden Fall folgendermaßen veranschaulichen: Gibt es nach der in Fachkreisen vorhandenen ungefähren Einschätzung in einer bestimmten Gewinn-Größenklasse nur zwei innungsangehörige Betriebe, so kann derjenige, der weiß, dass er selbst oder ein bestimmter Dritter in diese Klasse fällt, folgern, dass ein einziger anderer, der möglicherweise dafür in Frage kommt, ebenfalls in diese Klasse zu fallen, auch tatsächlich so viel (oder auch so wenig) Gewinn erzielt hat (Tabellenfeldwert 2) oder gerade doch nicht (Tabellenwert 1).

Da ersichtlich war, dass dem Anliegen der Innung auch damit gedient war, wenn die Tabellenfeldwerte 0, 1 und 2 unterdrückt, also etwa durch ein * dargestellt wurden, bedurfte es keiner Prüfung, ob zur Beantwortung der Anfrage vielleicht doch auch *personenbezogene* Daten durch die Handwerkskammer an die Innung übermittelt werden dürften.

Voraussetzung war allerdings aus Datenschutzgründen noch ein weiteres, nämlich die Befugnis der Handwerkskammer, die ihr vorliegenden Daten zur Erstellung der von der Innung gewünschten Statistik zu *nutzen*. Diese *Nutzung* war nach allgemeinen Regeln genau dann erlaubt, wenn

(a) die Handwerkskammer - wie vorausgesetzt - die Daten ohnehin zur Erfüllung ihrer Aufgaben bereits vorliegen hatte und wenn außerdem

(b) die durch die Statistik gewonnenen Daten für die Erfüllung der Aufgaben der Handwerkskammer (oder auch der über die Handwerkskammer die Rechtsaufsicht ausübenden staatlichen Stelle) dienlich waren § 7 Abs. 1 SächsStatG (etwas enger § 12 Abs. 3 Satz 1, letzter Fall SächsDSG).

Unter der Voraussetzung, dass die Kammerbeiträge in Abhängigkeit vom Gewerbeertrag bzw. Gewerbebetriebs-Gewinn bestimmt werden dürfen, diente es also erkennbar der Aufgabenerfüllung der Handwerkskammer, wenn sie Mitgliedsbetrieben oder deren Vereinigungen im Hinblick auf die Ausgestaltung der Regelung der Kammerbeiträge die von diesen erwünschte Auskünfte erteilte (sofern eben dabei die o. g. Untergrenze des Tabellenfeldwertes, nämlich die Zahl 3 eingehalten wurde).

Gegen das letztere wandte die Handwerkskammer dann, inzwischen gewissermaßen juristisch aufgewacht, ein, dass § 113 Abs. 2 Satz 7 HandwO mit seinem Verbot, die gemäß § 113 Abs. 2 Satz 3 bis 5 HandwO für Zwecke der Beitragsfestsetzung übermittelten Daten für andere Zwecke als den der Beitragsfestsetzung zu speichern oder zu nutzen, der von der Innung gewünschten Datenzusammenstellung entgegenstehe.

Diesem - zweifellos pfiffigen - Einwand war folgendes entgegenzuhalten:
Nach allgemeinen datenschutzrechtlichen Regeln gehört zu dem Verwaltungszweck „Beitragsfestsetzung“, also zur Anwendung des Beitragsrechtes auf die einzelnen Fälle (Kammerangehörigen), als Annex-Zweck die Gewinnung eines statistischen Überblickes, also von Erkenntnissen nicht zum einzelnen Fall, sondern zu dem, was das Sächsische Statistikgesetz in § 1 Abs. 1 Satz 1 als „Massenerscheinung“ bezeichnet. Datenschutzrechtlich besagt diese Regel, dass die statistische Nutzung zu Zwecken des Verwaltungsvollzuges im Einzelfall erhobener Daten *nicht* als *Zweckänderung* gilt. Oder anders ausgedrückt: Der Betroffene muss damit rechnen, dass die Behörde sich seiner Daten nicht nur für die Zwecke der Regelung seines Einzelfalles bedient, sondern auch als Baustein dafür, um einen Gesamtüberblick über die Verhältnisse auf dem betreffenden Gebiet zu gewinnen. Genau diese Regel spricht § 12 Abs. 3 Satz 1, letzter Fall SächsDSG aus, und etwas erweitert eben § 7 Abs. 1 SächsStatG.

Die Einengung der Nutzungsbefugnis, die § 113 Abs. 2 Satz 7 HandwO bewirken soll, geht nicht so weit, dass sich die Nutzungsbefugnis auf die individuelle Beitragsfestsetzung beschränkt. Denn die individuelle Beitragsfestsetzung ist möglich nur auf Grundlage einer Beitragsordnung, welche die Beitragsfestsetzung regelt. Weil Recht im Rechtsstaat ja nicht blindlings gesetzt werden soll, ist die Beitragsfestsetzung von den Beteiligten im Hinblick auf ihre Zweckmäßigkeit und Rechtmäßigkeit zu beurteilen, und dies kann nur geschehen, wenn man, sofern dies sinnvoll erscheint, auch statistische Werte heranziehen kann. Mittelbar, so lässt sich im Anschluss an diesen Gedankengang wohl formulieren, hat Statistik durchaus etwas ähnliches wie Verfassungsrang.

Fazit: Die Handwerkskammer musste die Statistik anfertigen und der Innung übermitteln. Man fragt sich, warum die Handwerkskammer das nicht schon von sich aus als Service für die Innungen anbietet.

5.7.2 Besucherbefragung durch Gerichte

Die ordentliche Gerichtsbarkeit in Sachsen wollte für die Besucher der Gerichtsgebäude Fragebögen auslegen und für deren - natürlich freiwillige - Ausfüllung in den Gerichtsgebäuden Werbung machen. In dem Fragebogen würde man unter anderem angeben sollen, in welcher Eigenschaft man „heute“ das Gericht besucht habe (Merkmalsausprägungen unter anderem Angeklagter, Rechtsanwalt, Pressevertreter), in was für einer Angelegenheit (z. B. Insolvenzsache, Familiensache, Betreuungssa-

che, Grundbuchsache), wie oft man das Gericht schon aufgesucht habe, und zwar in derselben oder in anderer Sache; auch nach Wochentag und Tageszeit des letzten Gerichtsbesuches, der Wartezeit (mit oder ohne Termin) und dem Grad der Freundlichkeit, Hilfsbereitschaft, Fachkunde und Verständlichkeit des Gerichtsbediensteten bei diesem Termin sollte man gefragt werden. Schließlich würde man angeben sollen, ob man die Bearbeitung des eigenen Anliegens als eher schleppend oder eher zügig empfunden habe, und noch einiges andere mehr, wie namentlich das Alter in Jahren und das Geschlecht. Außerdem wollte man ein Freitextfeld für Anregungen und Hinweise anbieten.

Die Aktion war schon in der Presse angekündigt („die Justiz soll sich ganz dem Bürger zuwenden"), als ein Justizmitarbeiter sie zum ersten Mal mit meiner Behörde besprach und sich sehr wunderte, dass die ihm vom SMJus erteilte Auskunft, die Aktion falle nicht unter irgendwelche Vorgaben des SächsStatG, sich als falsch herausstellte, da dieses Gesetz keineswegs nur für wiederkehrende statistische Erhebungen gilt (vgl. etwa nur § 11 Abs. 1 SächsStatG), wie man ihm gesagt hatte. (Empfehlung: Innerhalb der Staatsverwaltung in Statistikrechtsfragen das StaLA oder das Referat 16 des SMI fragen.)

Sofern die Befragung wie geplant von der Justiz selbst durchgeführt würde, gäbe es, das habe ich im einzelnen dargelegt, gegenüber dem Statistikrecht kein Entrinnen: Der Anwendung des Sächsischen Statistikgesetzes steht nicht entgegen, wenn die Daten von Gerichten oder anderen Justizbehörden gesammelt werden, das ergibt sich aus § 2 Abs. 1 Nr. 5, § 3 Abs. 2 Nr. 6 SächsStatG. Auch ließe sich die Erhebung zwanglos unter § 1 Abs. 1 Satz 1 SächsStatG subsumieren, denn es sollte ja ein *Informationsbedarf* der ordentlichen Gerichtsbarkeit gedeckt werden. Dieser war zwar nicht der Informationsbedarf des Freistaates Sachsen als ganzem, sondern nur eines Teiles seiner ‚Stellen' - dies reicht jedoch für die Geltung des SächsStatG aus, wie z.B. § 7 Abs. 1, § 11Abs. 1 des Gesetzes zeigt.

Auch nach der im Verlauf von der Justizverwaltung erwogenen Weglassung derjenigen Fragen, deren Beantwortung verhältnismäßig leicht einen Personenbezug herstellbar machten, und auch nach einer Umstellung der Altersangabe auf Schrittweiten (z. B. „ über 80 Jahre") wäre die Erhebung noch nicht von der Art gewesen, dass sie gemäß den von mir im 5. Tätigkeitsbericht unter 5.7.3 gemachten Darlegungen als wegen *vollständiger von vornherein bestehender Anonymität* außerhalb des Anwendungsbereiches des Statistikrechtes, namentlich des Sächsischen Statistikgesetzes, liegend anzusehen gewesen wäre.

Auch eine andere, eine außerhalb des Statistikrechtes liegende Rechtsgrundlage war für die geplante Befragung nicht ersichtlich. § 11 Abs. 1 SächsDSG war nicht anwendbar. Denn diese Vorschrift, die als Erhebungserlaubnis verstanden eine Generalklausel darstellt, tritt im Anwendungsbereich des Statistikrechtes gegenüber dessen Spezial-

vorschriften zurück. Genau dies war hier der Fall. Denn der Informationsbedarf, dessentwegen die Daten erhoben werden sollten, war ein gerade durch die Feststellung von *Massenerscheinungen* im Sinne von § 1 Abs. 1 Satz 1 SächsStatG zu deckender Informationsbedarf - auch wenn die *Massenerscheinungen* ‚heruntergebrochen' werden sollten auf einzelne Gerichte bzw. Gerichtsgebäude. Eine gesetzlich ausdrücklich vorgesehene Aufgabe der Justiz, an welche § 11 Abs. 1 SächsDSG anknüpfen könnte, war für die Beschaffung der Daten nicht ersichtlich.
Eine Rechtsgrundlage hätte sich auch nicht daraus gewinnen lassen, dass man die Befragung als *Organisationsuntersuchung* eingestuft hätte. Denn § 12 Abs.3 SächsDSG stellt keine Erlaubnis einer Primärerhebung der Daten von Nichtbediensteten dar (sondern nur die Erlaubnis der Nutzung von Daten, die zu Zwecken des normalen Verwaltungsvollzuges erhoben worden sind). Und die in § 31 Abs. 1 SächsDSG erhaltene Erlaubnis, *zur Durchführung organisatorischer Maßnahmen* Daten zu verarbeiten gilt nur für die Daten von Bediensteten *(Bewerbern und Beschäftigten)*.

Da demnach die geplante Befragung unter das Sächsische Statistikgesetz fallen musste, hätte sie - ungeachtet des Fehlens einer Auskunftpflicht (vgl. § 6 Abs. 3 Satz 3, Abs. 6 Satz 2, § 11 Abs. 1, § 7 Abs.6 SächsStatG) - einer Rechtsgrundlage bedurft, also gemäß § 6 Abs. 1 SächsStatG eines Gesetzes, da einer der Fälle, in denen das SächsStatG eine Rechtsverordnung oder eine Satzung ausreichen lässt, nicht gegeben gewesen wäre.

Wie üblich (vgl. z. B. 9/5.7.3) habe ich die Justizverwaltung auf die Möglichkeit hingewiesen, die Durchführung der Befragung auf einen Dritten zu übertragen, der sie im Verhältnis zu den Befragten auf rein privatrechtlicher Grundlage durchführt, insbesondere auch eine Hochschule. Dabei ist wichtig, dass die Übernahme der Befragung nicht nur zum Schein erfolgen darf: Die Durchführung der Befragung muss den Aufgaben der betreffenden Hochschule entsprechen, die Befragung muss auch für eine Gestaltung durch die Hochschule zum Teil offen sein, wobei es sich in diesem Falle wohl eher um eine Auftragsforschung, finanziert durch Drittmittel, handeln würde. Wie üblich bei der Auftragsforschung kann der Auftraggeber natürlich im wesentlichen vorgeben, was er untersucht bekommen möchte. Wegen der Anforderung, die an eine solche Privatisierung einer amtlichen Statistik gestellt werden, konnte ich auf 4/5.7.3 und 5/5.7.5 verweisen. Danach darf die Justiz nach Durchführung der Erhebung (Befragung) durchaus als Auftraggeber in Erscheinung treten, sie darf also Ergebnisse zusammen mit der durchführenden Hochschule präsentieren. Dabei ist es vermutlich sogar von Vorteil, wenn die Justiz darauf verweisen kann, dass sie die Befragung durch Fachleute und nicht selbst durchgeführt hat. Vorher muss sich die Justiz allerdings zurückhalten und, was das Erscheinungsbild der Befragung betrifft, darauf beschränken, die Sammlung der Daten im Gerichtsgebäude zuzulassen. Dabei trägt sie die Verantwortung dafür, dass es bei der Datensammlung - zivilrechtlich - korrekt zugeht: Durch Übertragung der Befragung auf eine Hochschule oder eine andere im Verhältnis zu den Befragten privatrechtlich tätige Stelle entfallen Schranken für das

Erhebungsprogramm. Aber die Aufklärung darüber, was mit den Daten geschieht, muss nach den Maßstäben des *zivilrechtlichen Datenschutzrechtes* einwandfrei sein, dafür trägt die öffentliche Stelle, welche die Durchführung in ihrem Organisationsbereich duldet, - in diesem Fall also die Justiz - Verantwortung.

Ich hätte keine Einwände dagegen, wenn - zu Kostenersparniszwecken - in den Gerichtsgebäuden von der Hochschule oder einem privaten Auftragnehmer aufgestellte Behältnisse, in welche die ausgefüllten Fragebögen einzuwerfen wären, nach Abschluss der Befragungs-Zeit von der Justizverwaltung gänzlich verschlossen und von ihr zur Hochschule transportiert würden. Selbstverständlich erhielte die Justiz keinerlei Einzeldatensätze von der Hochschule, sondern ausschließlich Zahlen, Tabellen. Die Justizverwaltung als Auftraggeber kann frei wünschen, welche Auswertungen sie haben möchte.

Die Justizverwaltung hat sich daraufhin dafür entschieden, die Befragung nicht selbst durchzuführen, sondern dem Fachbereich Rechtspflege der Fachhochschule der Sächsischen Verwaltung (Meißen) die Befragung mitsamt Auswertung als Diplomarbeits-Thema vorzuschlagen, weil eine echte Vergabe eines Forschungs-Auftrages an eine etwa auf dem Gebiet der Soziologie, Kommunikation oder Psychologie tätige Hochschule zu kostspielig sei. Nach Zustimmung des Fachbereiches sei abzuwarten, ob sich ein Interessent findet, an den das Thema vergeben werden kann. Die Justizverwaltung werde sich also darauf beschränken, die Befragung im Gerichtsgebäude nach den oben genannten Regeln zuzulassen.

Damit lassen sich vermutlich bestimmte Einzelfragen wie die Verbesserung von Vordrucken oder Technisches wie die telefonische Erreichbarkeit, die räumliche Orientierung im Gebäude, die Terminplanung, Parkplatzfragen und dergleichen nicht für alle Gerichte der ordentlichen Gerichtsbarkeit beantworten. Aber dazu sollte man, so habe ich empfohlen, lieber gezielte Betroffenenbefragungen durchführen, etwa bei Anwälten, Sachverständigen oder auch Fachleuten (etwa für Wegweisergestaltung), und außerdem Qualitätszirkel einrichten.

Der Gesetzgeber hat halt nicht vorgesehen, dass sich staatliche Einrichtungen nach Gefallen oder Nicht-Gefallen organisieren. Der Populismus ist keine Verfassungskategorie. - Ich bin sicher, dass jeder Gerichtspräsident weiß, ob sein Gericht in Quantität und Qualität den Pflichten genügt. Dass er zu Einzelproblemen die eine oder andere Umfrage nutzt, sollte man ihm aber letztlich nicht verwehren.

5.7.3 Privatisierung der Durchführung kommunaler Statistiken

Nach wie vor kommt es zu Fehlern, wenn sich Kommunen bei der Durchführung amtlicher Statistiken der Hilfe Privater bedienen, obwohl ich mich bereits mehrfach

in meinen Tätigkeitsberichten ausführlich zu dieser Thematik geäußert habe (vgl. im 4. Tätigkeitsbericht zu Nr. 5.7.3., im 5. Tätigkeitsbericht zu Nr. 5.7.5 sowie im 6. Tätigkeitsbericht zu Nr. 5.7.5.).

So hatte die Große Kreisstadt Riesa im November 2002 durch Schüler an 40 v. H. aller Riesaer Haushalte Fragebögen verteilt, denen ein Anschreiben des damaligen Oberbürgermeisters beigefügt war, in dem die Befragung erläutert und zur Teilnahme aufgerufen wurde. Die ausgefüllten Bögen waren von den Schülern eingesammelt worden, konnten aber auch im Rathaus abgegeben werden. Die Unterlagen hat dann ein Ingenieurbüro erhalten und ausgewertet.

Nachdem ich durch eine Eingabe auf den Vorgang aufmerksam gemacht worden war, habe ich der Stadtverwaltung Riesa mehrfach meine datenschutzrechtlichen Einwände gegen die Fragebogenaktion mitgeteilt. Insbesondere habe ich auf die fehlende Satzung als Rechtsgrundlage der Durchführung der Haushaltsbefragung hingewiesen. Die Stadt Riesa zeigte sich jedoch in keinster Weise einsichtig. Im Rahmen einer Kontrolle bei dem beauftragten Ingenieurbüro musste ich zudem feststellen, dass sich die streitgegenständlichen Fragebögen noch allesamt in den Räumen des Ingenieursbüros befanden, obwohl die Stadt Riesa mir zuvor mitgeteilt hatte, dass nach Rücksprache mit der beauftragten Ingenieurgesellschaft mitgeteilt werden könne, dass diese über keine Einzeldatensätze mehr verfüge (wenn die Verwaltung es mit der Wahrheit nicht genau nimmt, stellt sie sich außerhalb des Rechts).

Hierauf beanstandete ich die durchgeführte Haushaltsbefragung wegen Verstoßes gegen datenschutzrechtliche Vorschriften (§ 26 SächsDSG).

Begründung:

(1) Die beginnend mit der Aushändigung der Fragebögen durchgeführte Datenverarbeitung wurde ohne die hierzu erforderliche Rechtsgrundlage vorgenommen und war somit schon aus diesem Grunde unzulässig.

Bei der von der Stadt Riesa durchgeführten Umfrage handelte es sich um eine amtliche Statistik im Rechtssinne, nämlich die Erhebung und Weiterverarbeitung von Daten über Massenerscheinungen zu Planungszwecken (vgl. § 1 Abs. 1 Satz 1 SächsStatG). Dabei ist nach geltendem Recht weder die regelmäßige Erhebung noch die Veröffentlichung der Statistik und genausowenig auch eine Auskunftspflicht Voraussetzung für das Vorliegen einer Kommunalstatistik.

Als Kommunalstatistik bedarf eine solche Erhebung gemäß § 8 Abs. 1 Satz 2, 1. Halbsatz SächsStatG einer Satzung als Grundlage, an deren Vorbereitung gemäß Abs. 3 der Vorschrift das Statistische Landesamt und der Sächsische Datenschutzbeauftragte zu beteiligen sind.

Diese Erfordernisse gelten auch dann, wenn die Teilnahme an der Befragung wie hier freiwillig ist (vgl. § 6 Abs. 6 Satz 2, § 11 Abs.1 SächsStatG; 5/5.7.4).

(2) Etwas Anderes ergibt sich auch nicht aus dem Umstand, dass die Stadt die Durchführung der Statistik weitgehend einem privaten Unternehmen übertragen hat. Die Stadt hat die Statistik nämlich nicht in vollständig privater Form durchgeführt, also so, dass für den Befragten kein Bezug zu einer öffentlichen Stelle als Auftraggeber erkennbar gewesen wäre. Durch die an die betreffenden Haushalte versandte Bitte des Oberbürgermeisters um Unterstützung und Teilnahme an der Befragung war aber gerade der Bezug zur öffentlichen Stelle hergestellt. Damit war die Statistik zu einer amtlichen geworden.

(3) Die von der Stadt Riesa vertretene Auffassung, eine Kommunalstatistiksatzung sei nur dann erforderlich, wenn die Datenerhebung und –verarbeitung von einer „amtlichen Statistikstelle“ durchgeführt werde, ist abwegig.

§ 8 SächsStatG regelt die Voraussetzungen, unter welchen eine Kommunalstatistik durchgeführt werden darf. Daraus folgt, dass eine Kommunalstatistik immer einer Satzung als Ermächtigungsgrundlage bedarf, selbst dann, wenn die Erhebung ohne Auskunftspflicht erfolgen soll. § 9 SächsStatG regelt lediglich die Frage der Zuständigkeit für die Durchführung der angeordneten Kommunalstatistik, nämlich dahingehend, dass keine andere kommunale Stelle als eine kommunale Statistikstelle mit der Durchführung von Statistiken betraut werden darf, begründet also damit innerhalb der gesamten Kommunalverwaltung eine ausschließliche sachliche Zuständigkeit der kommunalen Statistikstelle für die Durchführung amtlicher Primärstatistiken.

(4) Die hierzu einschlägigen Beiträge in meinen Tätigkeitsberichten waren der Stadt Riesa nach eigenen Angaben bekannt. Die Stadt Riesa hat in diesem Fall demnach wider besseres Wissen gehandelt, als sie die Befragung ohne entsprechende Satzung durchführen ließ. Desgleichen ist festzuhalten, dass die Mitteilung der Stadt Riesa, das beauftragte Ingenieurbüro verfüge über keine Einzel-Datensätze mehr, nicht der Wahrheit entsprach. Der Stadt Riesa musste bekannt sein, dass sich die Fragebögen, welche Einzel-Datensätze beinhalten, noch beim Ingenieurbüro befinden.

Weil keine Satzung vorlag, waren die im Zuge der Befragung erhobenen Daten zu löschen, da die Speicherung rechtswidrig erhobener personenbezogener Daten unzulässig ist, was insoweit nicht aus Statistikrecht, sondern aus allgemeinem Datenschutzrecht folgt (§ 12 Abs. 1 Nr. 1 SächsDSG), welches im vorliegenden Falle wegen des vorhandenen Personenbezuges der Daten zusätzlich anzuwenden ist. Der Personenbezug der mittels des Fragebogens erhobenen Daten ergibt sich daraus, dass die Kombination der Merkmalsausprägungen zu den Erhebungsmerkmalen „Geburtsjahr“ und „Geschlecht“, in Verbindung überdies mit der Anzahl der Personen im Haushalt, mittels des Datensatzes des Melderegisters eine Identifizierung vieler Haushalte ermöglichte, zumal die Einzelbögen bestimmten statistischen Bezirken des Gemeindegebietes („Verkehrsbezirk“) zugeordnet waren.

Die Stadt Riesa hat mir gegenüber erklärt, an ihrer - wie dargelegt - in mehrerer Hinsicht unzutreffenden Rechtsauffassung festzuhalten; die Daten würden jedoch - ohne Anerkennung einer Rechtspflicht - durch eine von der Stadt beauftragte Fachfirma vernichtet.
Ob und wie sich die Rechtsaufsicht, die ich über die Beanstandung unterrichtet habe, zur Vorgehensweise der Stadt Riesa verhält, ist noch offen, eine Reaktion steht bislang noch aus.

5.8 Archivwesen

5.8.1 Sächsische Archivbenutzungsverordnung

In seiner Ende März 2003 (GVBl. S. 79) verkündeten Verordnung über die Benutzung der staatlichen Archive (SächsArchivBenVO) hat das SMI meinen Forderungen und Vorschlägen, die ich im Hinblick auf den ursprünglichen Entwurf geäußert habe, sehr weitgehend Rechnung getragen.

(1) Entfallen ist erfreulicherweise die zunächst vorgesehene Verpflichtung des Nutzers, den Namen und die Anschrift desjenigen Dritten anzugeben, „in dessen Auftrag" er das Archivgut benutzen will. Damit sollte eine *Erhebungsbefugnis* geschaffen werden, gegen die ich mich schon 2/5.8.3 im Hinblick auf eine für ein Kreisarchiv erlassene Benutzungsordnung gewandt hatte. Die Gründe, warum eine solche Erhebungsbefugnis gegen höherrangiges Recht (§ 11 Abs. 1 SächsDSG) und damit zugleich gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz verstieße, nämlich gegen die Regel, dass personenbezogene Daten nur insoweit erhoben werden dürfen, als ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist, musste ich, um das SMI zu überzeugen, noch schärfer herausarbeiten:
Die Datenerhebung wäre weder erforderlich, um
(a) den rechtmäßigen Zugang zum Archivgut sicherzustellen, noch um
(b) aufgrund dieses Vorganges rechtmäßig Gebühren zu erheben.

(1.1) Ersteres ergibt sich aus Folgendem:
Rechtmäßig ist die Gewährung von Zugang zum Archivgut gemäß § 9 Abs. 1 SächsArchivG dann, wenn der Nutzer ein berechtigtes Interesse an der Nutzung glaubhaft macht und kein Ausschlussgrund nach Abs. 2 Satz 1 und 2 dieser Vorschrift vorliegt. Die Daten eines Dritten dürfen bei demjenigen, der den Antrag auf Nutzung stellt, unter dem erstgenannten (positiven) Gesichtspunkt also nur dann erfragt werden, wenn dies notwendig ist, um das den Genehmigungsantrag stützende berechtigte Interesse an der Nutzung feststellen zu können.

Es ist nicht ersichtlich, dass das Vorliegen von Ausschlussgründen nach Verhältnissen des Dritten („Auftraggebers") zu beurteilen wäre. Denn für einen Archivbenutzer gibt

es keine - zumindest keine für sein Rechtsverhältnis zum Archiv erheblichen, namentlich keine immaterialgüterrechtlich zu begründenden - Übermittlungsverbote, sieht man von den in diesem Zusammenhang nicht interessierenden Einschränkungen für Veröffentlichungen (§ 10 Abs. 4 Satz 2, 2. Halbsatz SächsArchivG) ab. Die Archivverwaltung hat also nach dem Gesetz keine Handhabe, die Nutzungsgenehmigung zu verweigern, weil der Antragsteller eine Beziehung zu einem Dritten hat, dem, wenn er selbst aufträte, die Nutzung gemäß § 9 Abs. 2 Satz 1 und 2 SächsArchivG versagt werden könnte oder versagt werden müsste.

Ich habe daher vorgeschlagen, folgende Vorschrift in die VO aufzunehmen:

> *Name, Vorname und Anschrift eines Auftraggebers können angegeben werden, wenn die zu der beantragten Nutzung berechtigenden Umstände nicht in vollem Umfang in der Person des Antragstellers, aber möglicherweise in der von dessen Auftraggeber vorliegen; der Auftrag ist dem Archiv vorzulegen.*

Mit solch einer Regelung wird die Nennung des Dritten (Auftraggebers) dem Antragsteller freigestellt; die Archivbehörde *gibt* dem Antragsteller in diesen Fällen *Gelegenheit,* den Auftraggeber zu nennen und den Nachweis der Beauftragung zu führen (vgl. schon 2/5.8.3).
Diese Regelung ist nicht in die VO aufgenommen worden, sie drückt aber etwas aus, was sich aus dem Archivgesetz und dem allgemeinen Datenschutzrecht ableiten lässt. Dabei dürfte die Notwendigkeit eines solchen Rückgriffes auf in der Person eines Auftraggebers liegende Umstände wohl nur im Falle des Antrages auf Zugang zu die eigene Person betreffenden Daten (§ 6 SächsArchivG) - nämlich wenn der Betroffene etwa einen Rechtsanwalt oder einen Verwandten bevollmächtigt - sowie in dem Falle bestehen, dass eine auf § 10 Abs. 4 SächsArchivG gestützte Schutzfristenverkürzung gewünscht wird, der Antragsteller selbst sich aber auf ein Forschungsvorhaben berufen muss, in dem er nur eine beschränkte Rolle spielt: Hier verlangt das Gesetz ja, dass das bestimmte Forschungsvorhaben der Behörde bekannt ist, und bei der Beurteilung der Seriosität eines Forschungsvorhabens ist im wesentlichen auf die Leitung eines solchen Projektes, weniger auf die in ihm tätigen Hilfskräfte abzustellen, die eher unbekanntere Größen darstellen.

(1.2) Wie demnach die Regeln über die Gewährung von Zugang zum Archivgut keine ausreichende Grundlage dafür sind, in jedem Falle Angaben über einen ‚Auftraggeber' des Nutzers zu erheben (oben a), lässt sich eine solche generelle Erhebungsbefugnis aber auch nicht mit gebührenrechtlichen Erwägungen (oben b) begründen:

(1.2.1) Da der Antragsteller, wie schon dargelegt, in der Weitergabe von aus der Benutzung des Archivgutes gewonnenen Informationen der Archivbehörde gegenüber frei ist, kann die Einschaltung eines ‚Auftragnehmers' nicht unter kostenrechtlichen Gesichtspunkten missbräuchlich sein. § 2 Abs. 1 Nr. 2 SächsArchGebVO, wonach

Schuldner der Nutzungsgebühren unter anderem auch derjenige ist, *in dessen Interesse die Leistungen der staatlichen Archive in Anspruch genommen werden*, halte ich dementsprechend für einen Verstoß gegen das Abgabenrecht. Ich darf der Einfachheit halber aus meinem 2. Tätigkeitsbericht zitieren: „Es gibt keine Veranlassung, die für die Archivbenutzung anfallenden Gebühren in dem Falle eines für den Auftraggeber tätigen Benutzers statt bei diesem bei dem Auftraggeber zu erheben. Gebührenschuldner ist ausschließlich der unmittelbare Benutzer, nicht dessen Auftraggeber. Es ist nach allgemeinem gebührenrechtlichen Regeln nicht Sache des Archives, als einer Behörde, sich um das finanzielle Innenverhältnis zwischen Benutzer und Auftraggeber zu kümmern. Darüber hinaus wird die Frage nach einem Auftraggeber des Benutzers womöglich zur Offenlegung eines eventuell aus rechtlichen Gründen gerade geheimzuhaltenden Auftragsverhältnisses veranlassen". Wer im eigenen Namen auftritt und in seiner Person die Voraussetzungen für den Zugang zu dem betreffenden Archivgut erfüllt, ist meiner Auffassung nach im Verhältnis zu Behörde alleiniger Kostenschuldner. Er und nur er ist als Veranlasser und Begünstigter Gebührenschuldner - nach der allgemeinen Regel, wonach Gebührenschuldner derjenige ist, der einen öffentlichen Aufwand veranlasst hat oder durch diesen Aufwand begünstigt worden ist (P. Kirchhof in: Isensee/Kirchhof Handbuch des Staatsrechtes IV § 88, Rdnr. 196). Gebühren sind nach dem verfassungsrechtlich bestimmten - „doppelgliedrigen" - Gebührenbegriff Ausgleich für einen Vorteil oder Auferlegung von Kosten, die der Pflichtige verursacht hat und für die er eine Verantwortung trägt (K. Vogel, Vorteil und Verantwortlichkeit. Der doppelgliedrige Gebührenbegriff des Grundgesetzes, in: Festschrift für Willi Geiger zum 80. Geburtstag, 1989, S. 518 ff., 533 oben).

(1.2.2) Das bedeutet konkret vor allem, dass § 2 Abs. 1 Satz 1, 2. Fall SächsVwKostG (wie auch die ähnliche Formulierung in § 13 Abs. 1 Nr. 1, 2. Fall BundesVwKostG) meiner Auffassung nach nicht so zu verstehen sind, dass dann, wenn die Gebühr nicht wegen (individuell) veranlassten Aufwandes, sondern wegen eines durch Amtshandlung verschafften Vorteiles erhoben wird, die individuelle Zurechnung (Regel A) oder auch nur die Bemessung des Vorteiles (Regel B) über das Benutzungsverhältnis hinaus ausgedehnt werden darf, und zwar auf Vertragspartner des Benutzers bzw. dessen Rechtsbeziehungen zu Vertragspartnern.
Durch Regel A machte man den Vertragspartner des Benutzers zum Gebührenschuldner, und zwar unter Berufung auf § 2 Abs. 1 Nr. 2 SächsArchGebVO. Durch Regel B würde lediglich das Ausmaß der Vorteile, die der Benutzer erlangt, auf der Grundlage seines - womöglich der eigenen Nutzung erst mit zeitlichem Abstand folgenden - vertraglichen Verhältnis mit einem Dritten bestimmt.

Regel A - und damit auch § 2 Abs. 1 Nr. 2 SächsArchGebVO - halte ich für unzweifelhaft rechtswidrig. Der Dritte - der ja vielfach seinen Sitz außerhalb des Geltungsbereiches der VO haben und innerhalb des Geltungsbereiches auch nicht einmal gehandelt haben wird, so dass sich schon deshalb überhaupt kein gebührenrechtlicher Anknüpfungspunkt für Sächsischen Recht ergeben kann - ist kein (zusätzlicher) Gebührenschuldner.

Aber auch Regel B ist vom geltenden Gebührenrecht nicht gedeckt. Die in der bundesrechtlichen Regelung verwendete ältere Formulierung, der zufolge Gebührenschuldner (auch) „derjenige“ ist, „zu dessen Gunsten die Amtshandlung vorgenommen wird“, die wohl aus der Preußischen Verwaltungsgebührenordnung von 1926 (zitiert nach Vogel a.a.O. S. 524 zu Fußnote 37) übernommen worden ist, drückt diese Beschränkung auf die unmittelbare Rechtsbeziehung des Benutzungsverhältnisses aus; die Formulierung lässt ein finales Moment, ähnlich wie bei der zivilrechtlichen „Leistung“, anklingen. Man könnte sagen: Der Vorteil fließt nicht einfach zu, er wird *zugewandt,* und dafür wird vielfach der Ausdruck „Leistung“ verwendet, nicht nur in der Rechtssprechung (z. B. jüngst BVerfG Urt. v. 19. März 2003 - 2 BvL 9/98, NJW 2003, 715, 715 rSp, 717) und der Literatur (vgl. Vogel a.a.O. S. 533), sondern auch etwa in § 1 Abs.1 SächsArchGebVO.

Dieser Gedanke der *beschränkten Vorteils-Beziehung* lässt sich aus dem Gebühren-Begriff ableiten: Die Erhebung von Gebühren als Ausgleich für einen Vorteil setzt voraus, dass der Vorteil ein *individueller* Vorteil ist (Vogel a. a. O. S. 533 unten). Individueller Vorteil ist aber (so Vogel a.a.O S. 533/534 einleuchtend) nur derjenige, von dem der Hoheitsträger den, der nicht zur Gebührenzahlung bereit ist, ausschließen darf. Diese Ausschluss-Berechtigung ist individuell, nämlich grundrechtsträgerbezogen, zu beurteilen.

Damit wäre es nicht vereinbar, wenn der Vorteil des Benutzers danach bemessen würde, wie sich dessen Verhältnis zu Dritten entwickelt. Folgerichtig muss man das Verhältnis des Benutzers zu Dritten bei der Bemessung des Vorteiles ganz außer Betracht lassen.

(1.3) Es liegt auf der Hand, dass das die nachteilige Folge haben könnte, dass gebührenrechtlich diejenige Benutzung bessergestellt wäre, bei der nicht der Benutzer selbst, sondern Dritte Vervielfältigungen von Abbildungen von Archivgut in Verkehr bringen. Dieser Nachteil ist jedoch dem Gebührenrecht auch aus folgendem Grunde immanent: Zumindest über das nächste, d.h. das dritte Glied in einer Verwertungskette könnte der Benutzer nicht mehr zu Auskünften gezwungen werden, weil die Archivverwaltung ihn nämlich nicht verpflichten kann, seinen Vertragspartner zur Auskunft über einen Vertrag zu verpflichten, den der mit einem Dritten über eine Weiterverwendung geschlossen hat. Dies betrifft auch das bloße Ausmaß dieser Weiterverwendung. Schon der Vertragspartner des Benutzers wäre der Archivverwaltung gegenüber nicht zu Auskünften verpflichtet.

Folgerung ist, dass die Gebührenordnung zweckmäßig so zu gestalten ist, dass die Gebühr nach einem mittleren Vorteilsmaßstab, unter Einschluss der abstrakten Verwertungsmöglichkeiten, zu berechnen ist, wenn als Benutzungszweck das Abfassen einer publizierbaren Abhandlung genannt wird oder wenn es sich um Archivgut handelt, dessen Abbildung nicht nur den Benutzer interessieren könnte. Eine solche

generalisierende, pauschalisierende Betrachtungsweise ist im Gebührenrecht bekanntlich erlaubt (vgl. BVerfG a. a. O. S. 717 lSp.). Der Benutzer trüge damit das unternehmerische Risiko für die Inanspruchnahme der Leistungen der Archivverwaltung. Das dürfte nicht unangemessen sein.
Meine Vermutung ist, dass es sonst nirgendwo im Abgabenrecht eine Berücksichtigung des Verhältnisses des Benutzers zu Dritten zum Zweck der Bemessung des Vorteiles gibt.

(1.4) Gegen dieses Ergebnis spricht nicht, dass es im Steuerrecht zusätzliche Haftungsschuldner gibt. Im Gebührenrecht hat der Fiskus nicht den Absicherungsbedarf wie im Steuerrecht: Die Verwaltungsleistung kann zurückbehalten werden bzw. Zug um Zug gegen Gebührenentrichtung erbracht werden, während demgegenüber die Steuertatbestände in der Regel an Vorgänge anknüpfen, die von Hause aus ohne jede staatliche Beteiligung stattfinden.

(1.5) Für dieses Ergebnis spricht auch, dass das Handeln *im Interesse eines Dritten* hinsichtlich der möglichen rechtlichen Beziehungen zwischen den beiden Beteiligten von so unterschiedlicher Natur sein kann, dass die Bestimmtheit der Vorschrift zweifelhaft sein könnte, und vor allem aber, dass dies Verhältnis der Berücksichtigung durch die Behörde faktisch leicht entzogen werden könnte, weil es, wie dargelegt, erst nach Abwicklung des Verwaltungsvorganges (Archivbenutzung) oder mit jemandem begründet werden könnte, dessen Handeln sich ausschließlich außerhalb des Freistaates Sachsen abspielt.

(1.6) Nicht betroffen von dieser Frage sind wohlgemerkt diejenigen Fälle, in denen gegenüber der Archivbehörde lediglich ein Bote (z. B. Anwaltsgehilfe) oder ein weisungsabhängiger Amtsträger auftritt und die Benutzung zugleich für jeden gleichartigen Arbeitnehmer oder Bediensteten mitbeantragt wird. In diesen Fällen ist Antragsteller ausschließlich der Arbeitgeber bzw. die Behörde. Dasselbe gilt für den Fall des Auftretens eines Bevollmächtigten, also den Fall der Stellvertretung, in dem der Vertreter den Antrag im Namen des Vertretenen stellt. Für das Vorliegen der Antragsvoraussetzungen wie für die Festsetzung der Gebührenschuld kommt es ausschließlich auf die Person des Vertretenen an. Dies folgt aus allgemeinen Regeln, ist auf meine Anregungen hin aber vorsorglich in § 2 Abs. 2 Satz 3 Nr. 2 der VO zum Ausdruck gebracht worden.

(2) Zum Teil habe ich auch auf eine Erweiterung der Erhebung von Daten der Archivbenutzer gedrungen: Da nämlich, wo die Archivbehörde gesicherte Feststellungen darüber zu treffen hat, ob der Antragsteller die - gesteigerten - Voraussetzungen für die Gewährung von Zugang zu Archivgut mit personenbezogenen Daten erfüllt, also von Archivgut, für das die dem Schutz des Persönlichkeitsrechts dienenden Schutzfristen (§ 10 Abs. 1 Satz 3 und 4 SächsArchivG) noch nicht abgelaufen sind.
Hier gilt die Pflicht, sich auszuweisen (§ 2 Abs. 3 Satz 1, 1. Halbsatz

SächsArchivBenVO), in den Fällen, in denen sich die Daten - in einem zu präzisierenden Sinne, vgl. nachstehend 5.8.2 - auf die Person des Antragstellers beziehen müssen, zusätzlich das Erfordernis einer schriftlichen Begründung (§ 2 Abs. 3 Satz 2 der VO), die wiederum in den Fällen der Verkürzung der Schutzfrist zugunsten von Vorhaben der wissenschaftlichen Forschung, (also § 10 Abs. 4 und 5 SächsArchivG), die in § 3 der VO genannten näheren Angaben zum Forschungsvorhaben enthalten muss.

Ergänzend gilt die wie von mir gewünscht präzisierte Pflicht, nach § 2 Abs. 2 Satz 4 der VO Veränderungen mitzuteilen.

(3) Zu § 2 Abs. 2 Satz 3 Nr. 3 SächsArchivBenVO ist das SMI meinem Vorschlag, nämlich

> *In der Benutzungsgenehmigung sind alle Personen aufzuführen, welchen zugunsten eines bestimmten Vorhabens Einsicht gewährt oder Auskunft erteilt wird*

wird leider nur zum Teil gefolgt.

(4) Den jeweiligen *Benutzungszweck* hätte man, anders als ursprünglich geplant, nur in bestimmten Fällen (nämlich gemäß § 6 Abs. 1 Satz 2, Abs. 3 Satz 2 SächsArchivG, gemäß Nr. 3, sowie Nr. 7 bis 9 des Gebührenverzeichnisses zur SächsArchGebVO oder im Falle der Benutzung durch eine öffentliche Stelle) erheben dürfen. Wohl um eine entsprechende, komplizierte Regelung zu vermeiden, hat man lieber gänzlich auf eine Erhebung eines „Benutzungszweckes“ verzichtet.

(5) Im Falle des § 10 Abs. 3 Satz 2 SächsArchivG, also eines Einsichtsbegehrens derjenigen Stelle, welche die Unterlagen abgegeben hat, muss die Archivbehörde feststellen, ob die Unterlagen, für welche die Schutzfristen noch nicht abgelaufen sind, nicht bei der abgebenden Stelle hätten gesperrt, gelöscht oder vernichtet werden müssen.

In diesem Zusammenhang muss die abgebende, jetzt Einsicht begehrende Stelle u. U. auch Namen Betroffener nennen (statt bloßer Aktenzeichen), also unzweifelhaft personenbezogene Angaben machen. Solange die von mir schon in anderem Zusammenhang gegenüber dem SMI befürwortete Erlaubnis zur Schutzfristverkürzung für besondere behördliche Zwecke (öffentliche Sicherheit) immer noch fehlt, ist dies für die Archive der einzige Fall einer datenschutzrechtlich problematischen Gewährung von Akteneinsicht an Behörden. Ich habe daher vorgeschlagen, die Vorschrift

> *Im Falle des § 10 Abs. 3 Satz 2 SächsArchivG hat die den Antrag stellende öffentliche Stelle die betreffenden Personen oder den betroffenen Personenkreis sowie diejenigen Vorschriften zu bezeichnen, aufgrund deren sie die Daten vor Abgabe an das Archiv verarbeitet hat, und darzulegen, dass die Unterlagen bei ihr nicht hätten gesperrt, gelöscht oder vernichtet werden müssen*

einzufügen, und bleibe bei meiner Auffassung, dass es zweckmäßig gewesen wäre, wenn man eine solche Darlegungslast zugunsten der Archivbehörden in die VO aufgenommen hätte.

Die Sächsische Archivbenutzungsverordnung gilt, der Ermächtigungsgrundlage in § 16 Nr. 2 SächsArchivG entsprechend und wie auch ihr vollständiger Name zum Ausdruck bringt, ausschließlich für Benutzung der *staatlichen* Archive. Die Rechtsträger anderer Archive können einschlägige Satzungen erlassen (§ 13 Abs. 3 Satz 2, § 14 Abs. 2 SächsArchivG). Diese Satzungen bzw. die Praxis der Archive lassen sich anhand der nunmehr existierenden SächsArchivBenVO bzw. der vorstehenden Überlegungen überprüfen.

5.8.2 Noch einmal: Anspruch auf latent-eigene Daten nach § 6 SächsArchivG

Weiterhin (9/5.8.4) werden zum Zweck der Suche nach (mutmaßlichen) Vätern, die zu DDR-Zeiten an sächsischen Hochschulen studiert haben, Auskunftsverlangen an Universitätsarchive und entsprechende Anfragen an mich gerichtet. Außerdem ist das SMI als oberste Archivbehörde (§ 3 Abs. 2 SächsArchivG) der von mir (10/5.8.3) begründeten Anerkennung eines Anspruches gegen Archivbehörden auf Auskunft betreffend latent-eigene Daten entgegengetreten - allerdings naheliegenderweise nicht aus Datenschutzgründen.
Beides gibt Anlass, Folgendes klarzustellen und zu präzisieren:

Der Rechtsstandpunkt, den ich seinerzeit im Hinblick auf die Väter-Suche (9/5.8.4) eingenommen habe, ist nicht etwa dadurch überholt, dass, wie 10/5.8.3 ausgeführt, der archivrechtliche Auskunftsanspruch auch insoweit anzuerkennen sein kann, als die Daten einen *latenten Zusatz-Bezug* auf in den Unterlagen nicht selbst genannte Auskunftssuchende aufweisen. Denn der von der allgemeinen Schutzfrist für personenbezogenes Archivgut (gem. § 10 Abs. 1 Satz 3 SächsArchivG), also von einem Übermittlungsverbot, befreiende Anspruch auf Auskunft über eigene Daten (gem. § 6 Abs. 1 und 3 SächsArchivG) steht nicht jedem zu, auf den ein latenter Zusatz-Bezug der Daten besteht. Anspruchsbegründend wirkt vielmehr nur derjenige latente Zusatz-Bezug, der sich innerhalb des Verarbeitungszweckes (Verwaltungszweckes) ergibt, zu dessen Erreichung die Akten angelegt bzw. die in ihnen enthaltenen Daten (vor Abgabe an das Archiv) verarbeitet worden sind. Im konkreten Vergleich: Bauakten ist die Beziehung des Grundstückes zu Nachbargrundstücken (10/5.8.3) immanent. Die Hochschulverwaltung bzw. die von hier zu Studenten geführten Akten haben mit Abstammungsfragen (Vaterschaftsfeststellung) demgegenüber nichts zu tun.

Das bedeutet: Zwar bestimmt § 2 Abs. 3, letzter Fall SächsArchivG, dass die Aufbewahrung von Unterlagen durch die Archivbehörden auch der Sicherung berechtigter

Belange betroffener Privatpersonen dient. (Damit schließt das Archivrecht nahtlos an das formell zum Datenschutzrecht gehörende, materiell jedoch außerhalb des Datenschutzrechtes liegende Löschungsverbot zugunsten schutzwürdiger Interessen des Betroffenen, § 19 Abs. 4 Nr. 1 SächsDSG, an.) Die Belange bzw. Interessen sind jedoch nur in den Grenzen geschützt, die durch den jeweiligen Verwaltungszweck gezogen werden. Die datenschutzrechtlich begründete Zweckbindung wirkt also auch insofern (vgl. ferner § 10 Abs. 3 Satz 2 SächsArchivG) im Archivrecht fort.

Damit sind die Grenzen für einen als auskunftsanspruchsbegründend anzuerkennenden latenten Zusatz-Bezug gesteckt.

Die Frage einer Aufnahme einer Bestimmung in das SächsArchivG, die, nach dem Vorbild anderer Archivgesetze, unter bestimmten Voraussetzungen anderen öffentlichen Stellen und privaten Dritten einen zweckändernden Zugang zu fristengeschützten personenbezogenem Archivgut gewährt, bleibt davon unberührt.

Das Archivreferat des SMI sollte seinen Standpunkt überdenken. Die Rechte, die im Hinblick auf in der Archivbehörde „beerdigte" Akten bestehen, können nicht geringer sein als diejenigen, die im Hinblick auf Daten bestehen, die sich in „lebenden" Akten der Verwaltung befinden; instruktive Beispiele für latenten, durch die zweckimmanenten Rechtsbeziehungen begründeten Zusatz-Bezug, der den Anspruch auf Datenzugang begründet, finden sich 4/9.4.1 und 5/9.4.1.

5.8.3 Veröffentlichung von Fotografien von politischen Veranstaltungen aus DDR-Zeiten

Ein Kreisarchiv legte mir ein reichliches Dutzend nach 1950 entstandener Fotos aus seinen Beständen vor, die ein Historiker in einer Untersuchung über *die Etablierung totalitärer Herrschaft in einem sächsischen Landkreis in den 1933 bis 1961* veröffentlichen wollte.

Bei der Entscheidung über die Überlassung von Reproduktionen von Lichtbildern, die zu ihrem Archivgut gehören (vgl. § 2 Abs. 1 i. V. m. Abs. 2 SächsArchivG), haben die Archivbehörden neben den Vorschriften des Archivrechtes auch §§ 22 f. KUG zu beachten.

Daraus ergaben sich im Einzelnen folgende Überlegungen für die Verwendung der seinerzeit, wie es hieß, „als *Pressefotos* angefertigten" Bilder von Kundgebungen, Sitzungen von Parteigremien (etwa eifriges Studium von Unterlagen unter dem Spruchband „Werdet mutige und unerschrockene Kämpfer wie Stalin es war"), Verleihungen politischer Ehrungen und Besuchen höchster Partei-Prominenz:

1. Die allgemeinen Schutzfristen des § 10 Abs. 1 Satz 1 und 2 SächsArchivG waren gemäß § 10 Abs. 2 Satz 2 SächsArchivG auf die Bilder nicht anwendbar. Aber die dem Persönlichkeitsschutz dienenden Fristen nach § 10 Abs. 1 Satz 3 und 4 SächsArchivG waren zu beachten, sofern nicht die Ausnahmevorschriften des Abs. 2 eingriffen.

   Daraus ließ sich ableiten, dass die Bilder in folgenden Fällen für den Abdruck freigegeben werden durften:

   (1) Im Falle der Einwilligung des Abgebildeten oder nach seinem Tode derjenigen seiner Angehörigen, § 22 KUG; diese spezielle Einwilligungs-Regelung muss meiner Meinung nach auch im Archivrecht Anwendung finden, also eine Datenübermittlung durch die Archivbehörde rechtfertigen. § 10 Abs. 4 Satz 3 SächsArchivG scheint diese Auffassung zu bestätigen, zugleich aber auch ihr entgegenzustehen: Er bestätigt die Auffassung insofern, als er die Einwilligung zur Grundlage der behördlichen Übermittlung macht. Andererseits sieht § 10 Abs. 4 Satz 3 SächsArchivG die Einwilligung als Grund der Erlaubtheit einer Übermittlung nur für „Akten“ vor; das ist jedoch eine durch keinen vernünftigen Grund gebotene Beschränkung auf eine bestimmte Art von Archivgut, so dass die Vorschrift einer ergänzenden Anwendung des § 22 KUG nicht entgegensteht.

   (2) Der Abgebildete ist seit mindestens zehn Jahren tot: § 10 Abs. 1 Satz 3 SächsArchivG, § 22 Satz 3 KUG.

   (3) Der Abgebildete ist bei Ausübung seines öffentlichen Amtes abgebildet, § 10 Abs. 2 Satz 3, 1. Halbsatz SächsArchivG, wobei gemäß dem 2. Halbsatz dieser Vorschrift i. V. m. § 4 Abs. 2 Satz 2 und 3 SächsArchivG ausreicht, wenn es sich wie bei den Bildern in diesem Fall um Tätigkeit als Funktionsträger der SED, der Blockparteien, der Nationalen Front oder des Kreiskomitees der antifaschistischen Widerstandskämpfer handelt.

   Dem könnte entgegenstehen, dass jedenfalls vom Ausgangsgrundsatz her das KUG bzw. das Recht am eigenen Bild als Teil des allgemeinen Persönlichkeitsrechtes auch amtsträgerbezogen auf die Ausübung ihrer Amtstätigkeit schützt (Wenzel, das Recht der Wort- und Bildberichterstattung, 4. Aufl. 1994, Rdnr. 7.2); mit anderen Worten: Der Amtsträger ist in Ausübung seiner Amtstätigkeit noch nicht ohne Weiteres als Person der Zeitgeschichte einzustufen (Münchener Kommentar - Schwerdtner, Rdnr. 176 zu § 12 BGB).
   Ein solcher Schutz besteht jedoch meiner Auffassung nach insoweit nicht, als der Amtsträger sein Amt durch einen Auftritt auf einer Veranstaltung ausübt, bei der es eingeladene Zuschauer oder zumindest einen eingeladenen Fotografen gibt, der ein zur Veröffentlichung bestimmtes Bild macht. Hier wird die Amtstätigkeit gerade in einer für die Wahrnehmung durch eine bereits hergestellte Öffentlichkeit bestimm-

ten, in einer diese Wahrnehmung bezweckenden Weise ausgeübt.
Abgesehen davon kann ein Recht am eigenen Bild im Hinblick auf Amtstätigkeit zumindest dann nicht mehr bestehen, wenn nicht nur der abgebildete Vorgang, sondern - wie vorliegend der Fall - zusätzlich auch das Abbilden selbst sowie die Verbreitung der Abbildung eine Ausübung von Amtstätigkeit gewesen ist. Denn der Fotograf war beim Aufnehmen von *Pressefotos* - und darum hat es sich ja ausnahmslos gehandelt - im Sinne des § 10 Abs. 2 Satz 3, 2. Halbsatz SächsArchivG Mitarbeiter einer vom Staat bzw. von der Partei gesteuerten Einrichtung: Die Presse in der DDR stand - mit Ausnahme der Kirchenpresse - unter ganz intensiver Kontrolle von SED und Staat, in Einzelfällen auch einer Blockpartei oder einer anderen von der SED gelenkten Massenorganisation (FDJ, FDGB), in der Zeit davor der SMAD.
Die Bilder sind daher eine *amtliche*, offizielle, zumindest offiziöse Dokumentation von Funktionärstätigkeit gewesen.

Insoweit auf den Fotografien Personen abgebildet sind, von denen nicht bekannt ist, dass sie Funktionen - auch ehrenamtliche - in einer gesellschaftlichen Organisation ausgeübt haben und im Hinblick auf diese Funktionen aufgetreten sind bzw. sich haben fotografieren lassen, ist diese Voraussetzung (3) nicht erfüllt. Wer in der DDR etwa wegen besonderer Arbeitsleistung oder wegen Widerstandes gegen das NS-Regime ausgezeichnet werden sollte, konnte sich schlecht dagegen wehren; er war insofern kein Funktionsträger. Entsprechendes müsste meiner Auffassung nach für Wehrpflichtige gelten, (einschließlich derjenigen, die sich, etwa um studieren zu dürfen, freiwillig länger verpflichtet haben?) Die waren eben keine Amtsträger.

2. Die bloße Teilnahme an einer öffentlich abgehaltenen Veranstaltung mit politischem Einschlag reicht nicht aus, um porträtartige Aufnahmen einzelner Teilnehmer zu rechtfertigen. § 23 Abs. 1 Nr. 3 KUG gilt nur für die die Versammlung repräsentierenden Personen, z. B. Redner, insbesondere in Aktion, im Übrigen dürfen nur Vorgänge ohne porträtartige Wirkung wiedergegeben werden (Steffen in Löffler, Presserecht, § 6 Rdnr. 138).

   Dagegen könnte man § 10 Abs. 2 Satz 1 SächsArchivG ins Feld führen, der alle Unterlagen, die bereits bei ihrer Entstehung zur Veröffentlichung bestimmt waren, von den Schutzfristen, also auch von den dem Persönlichkeitsschutz dienenden Fristen, ausnimmt. Das ist jedoch problematisch, wenn die Veröffentlichung rechtswidrig war oder nach den zum Beurteilungszeitpunkt (hier also 2002) geltenden Maßstäben (KUG) rechtswidrig gewesen wäre. Daher ist § 10 Abs. 2 Satz 1 SächsArchivG zumindest verfassungskonform so auszulegen, dass die Regeln des KUG ihm vorgehen.

3. Für eine Schutzfristverkürzung gemäß § 10 Abs. 4 Satz 2 SächsArchivG war kein Raum. Denn das Weglassen der Fotos in der geplanten Veröffentlichung hätte

dem Forschungszweck keinen Abbruch getan, auch wenn Bilder in historischen Abhandlungen dem Leser immer einen zusätzlichen, besonders unmittelbaren, anschaulichen Eindruck von den dargestellten Zeitläuften vermitteln können.

Dabei bestand die Möglichkeit, einzelne Personen, für die keine der vorstehend genannten, für sich jeweils hinreichenden Voraussetzungen einer erlaubten Bild-Wiedergabe bestanden, unkenntlich zu machen: Die vom Archiv abgegebene Reproduktion muss in solchen Fällen einen schwarzen Balken um die Augenpartie erhalten (der auch wirklich die Gesichtszüge unkenntlich macht), wie man es aus heutigen Presseveröffentlichungen kennt, oder die Gesichtspartie muss unscharf gemacht werden, und der Name darf in einer Bildunterschrift nicht erwähnt werden.

Bei der Anwendung dieser Regeln auf die einzelnen Bilder gab es natürlich Grenzfälle, was die Erkennbarkeit einzelner Personen betrifft. Bei der Abbildung eines Jugendlichen, der offenbar in Ausübung eines Amtes bei der staatlichen Jugendorganisation eine Rede gehalten hat, also als Funktionär aufgetreten ist, habe ich empfohlen, für den Fall, dass die betreffende Person nicht später im Rahmen des Untersuchungsgegenstandes noch einschlägig in Erscheinung getreten ist, wegen ihrer Minderjährigkeit von einer die Person erkennbar werden lassenden Veröffentlichung abzusehen (in Anwendung des Prinzips der §§ 20 Abs. 1 Nr. 6 und Nr. 7, 21 Abs. 1 Nr. 6 und Nr. 7 StUG).

5.9 Polizei

5.9.1 Grenzen polizeilicher Datennutzung bei Luftverkehrsüberprüfungsverfahren

Das SMWA äußerte mir gegenüber Zweifel an der Zulässigkeit eines Ersuchens des LKA, mit dem es die zuständige Luftfahrtbehörde, das Regierungspräsidium Dresden, gebeten hatte, „zur Aufrechterhaltung bzw. Intensivierung der Luftsicherheit die Personen, deren Zuverlässigkeit verneint oder widerrufen wird, unter Angabe der Verneinungsgründe mitzuteilen“. Es sollten also personenbezogene Informationen zur Gefahrenabwehr erhoben werden. Dieser Erhebungszweck ist jedoch durch die datenschutzrechtliche Spezialvorschrift des § 29 d Abs. 5 Satz 2 LuftVG nicht gedeckt. Diese Vorschrift legt nämlich fest, dass die aus einer luftfahrtrechtlichen Zuverlässigkeitsprüfung stammenden Daten einer strengen Zweckbindung unterliegen: Die Polizei darf die Daten nur für Strafverfolgungszwecke, nicht zur Gefahrenabwehr nutzen. Weitere Nutzungsmöglichkeiten sind durch den Wortlaut der Vorschrift explizit ausgeschlossen.

Das von mir zur Stellungnahme aufgeforderte aufsichtsführende SMI hat leider versucht, den klaren Gesetzeswortlaut zu ignorieren, indem es dem LKA zubilligte, die

Daten auch zur Gefahrenabwehr zu erheben; schließlich habe die polizeiliche Aufgabe der Prävention ja ebenfalls „Verfassungsrang“.

Diese Auffassung verkennt freilich Folgendes: Die Vorschrift des § 29 d LuftVG ist gerade die einschlägige und verfassungsgemäße Gefahrenabwehrvorschrift, denn sie gewährleistet, dass Gefahren für die Sicherheit des Luftverkehrs durch die Sicherheitsüberprüfung des Personals abgewendet werden. Eine Gefahr für den Luftverkehr ist deshalb bereits abgewendet, wenn die Zuverlässigkeit von Personen verneint oder widerrufen wird und damit diese Personen von schädigenden Einwirkungsmöglichkeiten ferngehalten werden.

Eine Nutzung der bei einer Sicherheitsüberprüfung angefallenen „Negativdaten“ eröffnete der Polizei zudem die Möglichkeit, ohne polizeilichen Gefahrenhintergrund „quasi auf Vorrat“ und anlassfrei Daten zu sammeln - ein eindeutiger Verstoß gegen das verfassungsrechtliche Übermaßverbot, weil der Polizei lediglich in den Vorschriften der §§ 46 und 47 SächsPolG die Möglichkeit eingeräumt wird, unter Beachtung der dortigen Voraussetzungen Datenbestände anderer Stellen im Rahmen eines Abgleichs zu nutzen.

Somit musste ich dem SMI nochmals verdeutlichen, dass das LKA die bei der Luftverkehrs-Sicherheitsüberprüfung angefallenen Daten nicht zur abstrakten Gefahrenabwehr, sondern einzig zur Aufklärung begangener Straftaten erhalten darf. Ich erwarte, dass die sächsischen Polizeidienststellen diese Rechtslage beachten; die Auslegung von Gesetzen, deren Wortlaut klar und eindeutig ist und die somit nicht auslegungsfähig sind, sollte das SMI unterlassen.

5.9.2 Verarbeitung von Daten strafunmündiger Kinder

Wie bereits im Vorjahr musste ich auch im Berichtszeitraum feststellen, dass durch die sächsische Polizei Daten strafunmündiger Kinder rechtswidrig verarbeitet worden sind. Während es bei dem in 10/5.9.2 geschilderten Fall um die rechtswidrige erkennungsdienstliche Behandlung von Kindern ging, musste ich diesmal Strafverfolgungsmaßnahmen bewerten, die gegen ein strafunmündiges Kind durchgeführt wurden: Ein achtjähriges Mädchen wollte eine Tüte Chips ohne Bezahlung aus einem Geschäft mitnehmen, wurde hierbei vom Personal ertappt und der Polizei übergeben. Auf dem Polizeirevier unterschrieb das Kind ein Protokoll, das von seiner Vernehmung angefertigt wurde und auf welchem sich vor seiner Unterschrift die Bemerkung „selbst gelesen, genehmigt und unterschrieben“ befand. Den Vorgang des Ladendiebstahls speicherte die Polizei in ihrer Datei „Vorkommnis-Bericht“ für die Dauer von zwölf Monaten. Neben der Speicherung in PASS wurde zu dem Vorgang eine Ermittlungsakte bei der Polizei angelegt, die daraufhin an die Staatsanwaltschaft abgegeben wurde. Dort erhielt der Vorgang ein Js-Aktenzeichen, was bedeutet, dass ein staatsanwaltschaftliches Ermittlungsverfahren eingeleitet war.

Das war alles falsch.

Meine datenschutzrechtliche Überprüfung ergab, dass die Verarbeitung personenbezogener Daten des offensichtlich schuldunfähigen Kindes *zu Zwecken der Strafverfolgung* unzulässig war. Denn Ermittlungshandlungen dürfen nicht durchgeführt werden, wenn der Ermittelnde zurzeit seines Handelns genau weiß, dass eine strafrechtliche Sanktionierung von Gesetzes wegen ausgeschlossen ist (§ 19 StGB). Die „Anhörung" eines offensichtlich schuldunfähigen Kindes unter 14 Jahren zu Strafverfolgungszwecken kann deshalb nur eine Zeugenvernehmung sein. Auch eine „Anhörung", die dem Zweck dient, festzustellen, ob das Kind als Werkzeug eingesetzt wurde, wäre als Zeugenvernehmung zu qualifizieren. Ich habe deshalb das SMI aufgefordert sicherzustellen, dass - gegebenenfalls gemeinsam mit dem SMJus - im Erlasswege klargestellt wird, dass die Einleitung eines Ermittlungsverfahrens gegenüber einem offensichtlich schuldunfähigen Kind unzulässig ist und die Polizei weder personenbezogene Daten des Kindes erheben, speichern oder an die Staatsanwaltschaft übermitteln darf.

Davon abgesehen ist auch die Verarbeitung personenbezogener Daten von offensichtlich schuldunfähigen Kindern *zum Zweck der Gefahrenabwehr* nur in Einzelfällen zulässig. Die Anhörung eines Kindes zu Gefahrenabwehrzwecken nach § 37 SächsPolG wäre nur zulässig, um festzustellen:
- ob eine rechtswidrige Tat vorliegt,
- wo das Kind wohnt,
- ob Aufsichts- oder Erziehungspflichten der Erziehungsberechtigten verletzt wurden,
- ob kindtypisches Fehlverhalten vorliegt.

Zu Gefahrenabwehrzwecken kann das Kind zunächst dahingehend informell - und später unverwertbar, weil ein Kind, selbst wenn es von Anfang an ordnungsgemäß über sein Aussage- oder Auskunftsverweigerungsrecht belehrt wurde, nicht verantwortlich entscheiden kann, ob und wie es seine Rechte wahrnimmt, dazu braucht es seine gesetzlichen Vertreter, in der Regel die Eltern (übrigens beide) befragt werden, ob überhaupt eine (strafbare) Tat vorliegt. Nur wenn dies hinreichend sicher feststeht, kann es - wenn es ohne seine Erziehungsberechtigten angetroffen wird - zu seinen Eltern und seinem Wohnort befragt werden, damit es den Eltern übergeben werden kann, bzw. diese nach § 45 Abs. 1 SächsPolG über den Vorfall informiert werden können. Danach müssten die personenbezogenen Daten des Kindes aufgrund § 49 Abs. 1 SächsPolG i. V. m. § 19 Abs. 1 SächsDSG gelöscht werden. Nur wenn es im Einzelfall konkrete Anhaltspunkte dafür gäbe, dass die Erziehungsberechtigten ihren Aufsichts- oder Erziehungspflichten nicht ausreichend nachkommen, könnten weitere Befragungen dieser Personen durch die Polizei zulässig sein, um herauszufinden, ob das Kind gefährdet ist, erneut strafbare Handlungen zu begehen (so sehen dies auch die KpS-Richtlinien in Nr. 2.7 vor). Ist dies nach Einschätzung der Polizei nicht der Fall, wäre die Speicherung personenbezogener Daten des Kindes durch die Polizei unzulässig (§ 43 Abs. 1 Satz 1 SächsPolG).

Aber selbst wenn das Kind aus Sicht der Polizei gefährdet wäre, weitere Straftaten zu begehen, ist bei der Verarbeitung personenbezogener Daten von Kindern zu polizeilichen Zwecken der Erziehungsaspekt zu beachten. Die Verarbeitung personenbezogener Daten von Kindern durch die Polizei kann nur der Individualprävention dienen, also der Verhinderung von künftigen strafrechtlichen Auffälligkeiten des Kindes. Dies kann bei Kindern nur durch erzieherische Maßnahmen erreicht werden. Erziehung verlangt jedoch in der Regel die Vermeidung „polizeilicher Sozialkontrolle“ beim Prozess des Erwachsenwerdens. Ziel ist die Verringerung von Stigmatisierung und das Eingehen auf die Probleme des Betreffenden mit konkreten Hilfsangeboten. Das geht nie ohne die Erziehungsberechtigten, notfalls auch im Zusammenwirken mit dem Jugendamt, der Schule etc. Zu dieser (arbeitsintensiven) Arbeit erwarte ich schon lange konkrete Vorschläge der Staatsregierung.

Erziehung und Jugendhilfe sind aber nicht Aufgabe der Polizei, sondern der Eltern und - erst wenn diese „versagen“ - Sache der Träger der Jugendhilfe (§ 2 SGB VIII). Erst wenn auch deren Einflussmöglichkeiten auf das Kind erschöpft sind, sollte es der Polizei - unter engen Voraussetzungen - erlaubt sein, Daten von Kindern zum Zweck der vorbeugenden Straftatenbekämpfung zu verarbeiten. Von der Polizei als „gefährdet“ erkannte Kinder - wozu auch gehört, dass die Eltern offensichtlich ihren Aufsichts- oder Erziehungspflichten nicht ausreichend nachkommen - sollten deshalb grundsätzlich zunächst den Trägern der Jugendhilfe gemeldet und nicht in den kriminalpolizeilichen Sammlungen gespeichert werden.

Weil das SMI mir inzwischen signalisiert hat, meine Empfehlungen in eine Neufassung der KpS-Richtlinien aufzunehmen, habe ich zunächst von einer förmlichen Beanstandung im vorliegenden Fall abgesehen.

5.9.3 Beanstandete Beantwortung einer parlamentarischen Anfrage

Aus Anlass einiger Eingaben hatte ich das SMI zu einer Stellungnahme zu der Frage aufgefordert, inwieweit die Nennung der Namen von Versammlungsanmeldern in einer Antwort der Sächsischen Staatsregierung auf eine Kleine Anfrage eines Abgeordneten erforderlich gewesen sein soll. Der Sachverhalt war folgender:

In seiner Beantwortung einer Kleinen Anfrage eines Abgeordneten hatte das SMI die Namen von Anmeldern verschiedener Demonstrationen gegen eine rechtsgerichtete Demonstration aufgeführt. Die der Beantwortung zugrunde liegende Kleine Anfrage enthielt aber keine Frage zu bestimmten Demonstrationsanmeldern oder gar noch deren Namen, sondern war auf die Erlangung allgemeiner, nicht personenbezogener Hintergrundinformationen (Störungen und Beeinträchtigungen der öffentlichen Sicherheit und Ordnung, Zahl der Straftaten, Zahl der Beteiligten der „Gegenmaßnahmen“) gerichtet.

Das von mir darum gebetene SMI konnte nicht darlegen, dass die Nennung der Anmelder der Gegendemonstrationen dem verfassungsmäßigen Gebot der Verhältnismäßigkeit genügte. Ich musste deshalb die Beantwortung der parlamentarischen Anfrage förmlich nach § 26 Abs. 1 SächsDSG beanstanden. Hierfür waren folgende Erwägungen maßgebend:

Artikel 58 SächsVerf kam als Befugnisnorm für den vorgenommenen Grundrechtseingriff nicht in Betracht, weil diese Verfassungsregel nur zur Anwendung gelangt, wenn „Fragen einzelner Abgeordneter oder parlamentarische Anfragen" nur unter Verwendung personenbezogener Daten beantwortet werden können. Die Kleine Anfrage des Abgeordneten umfasste aber wegen des allgemein gehaltenen Informationszieles kein Begehren, personenbezogene Daten in Erfahrung zu bringen. Oder anders ausgedrückt: Nicht gestellte Fragen müssen - und dürfen personenbezogen - nicht beantwortet werden. Rechtfertigungsversuche des SMI derart, man müsse parlamentarische Anfragen ja „vollständig" beantworten, lagen daher ersichtlich neben der Sache. Bereits aus diesem Grunde verstieß jede Nennung personenbezogener Informationen durch die Staatsregierung gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz.

Die Einwendungen des SMI veranlassten mich, allgemeine datenschutzrechtliche Klarstellungen vorzunehmen. Denn die Argumentation des SMI ließ auf ein Verständnis datenschutzbezogener und damit verfassungsrechtlicher Zusammenhänge schließen, das mit dem garantierten Schutz des Grundrechtes auf informationelle Selbstbestimmung nicht zu vereinbaren war.

Offenbar ging das SMI von der Annahme aus, dass Anmelder von Versammlungen, deren Namen nach dem Versammlungsgesetz für Zwecke des Verwaltungsverfahrens zu erheben sind, es hinnehmen müssen, jederzeit und in anderen Verwendungszusammenhängen durch öffentliche Stellen der Öffentlichkeit „bekanntgemacht" (besser: „vorgeführt") zu werden.

Der Anmelder einer Versammlung gibt seine Daten in einem Verwaltungsverfahren jedoch nicht öffentlich kund, sondern machte sie lediglich der Behörde zu dem Zweck bekannt, dass das Anmeldungsverfahren der Versammlung ordnungsgemäß abläuft; der Anmelder soll der Ordnungsbehörde ein Ansprechpartner sein, der als Adressat versammlungsrechtlicher Pflichten gilt und den Ablauf und die Einzelheiten der Versammlung mit der Ordnungsbehörde festzulegen hat. Nur darin liegt der gesetzmäßige Zweck der Datenerhebung und Datenverarbeitung. Nur er legitimiert eine - gesetzesgemäße - Datenübermittlung an die eventuell zu beteiligenden Behörden, z. B. Polizeidienststellen.

Es kann also keine Rede davon sein, dass der Anmelder einer Demonstration mit der Abgabe seiner Daten in einem Verwaltungsverfahren sich zugleich der Öffentlichkeit

preisgeben will. Er muss auch nicht damit rechnen, dass öffentliche Stellen seine Daten veröffentlichen. Er ist schließlich nicht mit denjenigen Personen identisch, die gegebenenfalls öffentlich zur Teilnahme an der von ihm angemeldeten Veranstaltung aufrufen. Bemühte Argumentationsversuche (des SMI), die Anmelder hätten sich mit ihrer Anmeldung selbst in das Rampenlicht der Öffentlichkeit gebracht und müssten daher einen reduzierten Grundrechtsschutz hinnehmen - gleichsam als „Person der Zeitgeschichte“ behandelt werden - können an dieser Rechtssituation nichts ändern. Etwas ganz anderes ist die allfällig zu vernehmende schöne politische Forderung, derjenige, der demonstriere, solle dies offen tun. Solcherart politisch Argumentierende sollten sich stets vor Augen halten, dass dieser politische Wunsch nicht identisch ist mit der gesetzlichen Befugnis, interne Verwaltungsdaten zu bestimmten Personen offen zu verbreiten.

Für ebenfalls abwegig hielt ich die weitere Argumentation des SMI, ein einmal in einem Verwaltungsverfahren auf dem Gebiet des Versammlungsrechts erhobenes Datum könne später beliebig (oft) verwendet werden; dies sei „kein Eingriff“: Selbst wenn sich die Personen bei der Anmeldung oder bei der Durchführung der Versammlung mit ihrem eigenen Namen zuvor selbst an die Öffentlichkeit gewandt hätten, so rechtfertigt dies nicht ohne weiteres die Übermittlung der Namen durch die Anmeldungsbehörde an das letztlich aufsichtsführende SMI und von dort an den Landtag also die Öffentlichkeit. Selbst wenn personenbezogene Daten schon einmal veröffentlicht waren, so rechtfertigt dies nicht die nochmalige Verwendung dieser Daten, d. h. den nochmaligen Grundrechtseingriff. Einfaches Beispiel: Was vielleicht vor Jahren in der Zeitung stand, darf von Behörden nicht ohne weitere Legitimation nochmals aktuell veröffentlicht werden. Es ist also der verfassungsrechtlich garantierte und von den Datenschutzgesetzen normierte Grundsatz zu beachten, dass jede Verarbeitung personenbezogener Daten, d. h. erst recht jeder weitere Verarbeitungsschritt, einer klar definierten gesetzlichen Grundlage bedarf.

Inwieweit meine Beanstandung bei der Beantwortung künftiger vergleichbarer parlamentarischer Anfragen Beachtung finden wird, kann ich zum jetzigen Zeitpunkt nicht abschätzen, weil mir die Staatsregierung bislang keine entsprechenden Zeichen gegeben hat.

5.10 Verfassungsschutz

In diesem Jahr nicht belegt.

5.11 Landessystemkonzept/Landesnetz

In diesem Jahr nicht belegt.

5.12 Ausländerwesen

5.12.1 Akteneinsicht im Visumverfahren

Eine Ausländerin hatte vor ihrer Einreise in die Bundesrepublik Deutschland bei der deutschen Auslandsvertretung in ihrem Heimatland ein Visum beantragt. Für die Erteilung des Visums war die Zustimmung der Ausländerbehörde in Leipzig notwendig. Das Visum wurde letztlich nicht erteilt. Über ihre Anwälte beantragte die Ausländerin Einsicht in die Akten der Ausländerbehörde Leipzig. Diese wurde mit Hinweis darauf verwehrt, dass die Entscheidung über die Visumerteilung die Deutsche Auslandsvertretung getroffen hatte und dass deshalb dort Akteneinsicht zu beantragen sei. Das Verwaltungshandeln der Auslandsvertretung unterfalle nicht den Regeln des Verwaltungsverfahrensgesetzes, weshalb ein Akteneinsichtsrecht nach § 29 VwVfG nicht gegeben sei.

Meine datenschutzrechtliche Bewertung ergab, dass zwar das Verwaltungsverfahrensgesetz für die Tätigkeit der Vertretungen des Bundes im Ausland nicht gilt (vgl. § 2 Abs. 3 Nr. 3 VwVfG). Hier ging es jedoch nicht darum, welches Recht die Auslandsvertretung einzuhalten hatte, sondern darum, ob die Betroffene gegenüber der Ausländerbehörde in Leipzig einen Anspruch auf Akteneinsicht hatte - was gemäß § 17 SächsDSG unzweifelhaft der Fall war:

Zwar sind für die Entscheidung über die Erteilung des Visums die vom Auswärtigen Amt ermächtigten Auslandsvertretungen (§ 63 Abs. 3 AuslG) zuständig; auch bedarf gemäß § 64 Abs. 4 AuslG i. V. m. § 11 Abs. 1 Nr. 3 DVAuslG das Visum lediglich der vorherigen Zustimmung der für den vorgesehenen Aufenthaltsort zuständigen Ausländerbehörde. Das ändert aber nichts daran, dass die Ausländerbehörde ihre Akten nach den Regeln des Verwaltungsverfahrens führt und auch zur Einsicht gegenüber den Betroffenen bereithalten muss.

Aber selbst wenn sich ein Akteneinsichtsrecht nicht bereits aus § 29 VwVfG ergäbe, hätte die Betroffene jedenfalls einen Anspruch auf Akteneinsicht aus § 17 SächsDSG. Denn in allen Fällen, in denen eine deutsche öffentliche Stelle nicht an die Vorschriften des Verwaltungsverfahrensrechts gebunden ist, gilt noch immer das jeweilige Datenschutzgesetz; für sächsische Behörden also das Sächsische Datenschutzgesetz.

Die Ausländerbehörde der Stadt Leipzig ließ sich von meiner Rechtsauffassung überzeugen und gewährte schließlich dem Rechtsbeistand der Petentin Akteneinsicht.

5.12.2 Einrichtung von so genannten Passabgleichstellen

Die Innenministerkonferenz hatte eine Arbeitsgruppe „Rückführung“ beauftragt, ein Verfahren zu entwerfen, mit dessen Hilfe die Identität von Ausländern geklärt werden kann, die nicht im Besitz eines Ausweisdokumentes sind. Im Rahmen dieses Verfahrens sollte im Einzelfall eine Zuordnung von bundesweit ca. 20.000 Ausweisdokumenten erfolgen, die bei den Ausländerbehörden und sonstigen öffentlichen Stellen aufbewahrt werden, weil ihr Inhaber nicht auffindbar ist.

Die Arbeitsgruppe hatte daraufhin vorgeschlagen, so genannte Passabgleichstellen (Landeszentralstellen) einzurichten. Diese Stellen sollten die Aufgabe haben, Ausweisdokumente von Ausländern, deren Inhaber nicht aufgefunden werden können, aufzubewahren und das Lichtbild sowie weitere Daten, die das Dokument über den Inhaber enthält, digital zu speichern. Zweck der Speicherung sollte sein, das Dokument dem berechtigten Inhaber zuordnen zu können, falls dieser bei einer Ausländerbehörde ohne Ausweispapiere registriert wird. Diese Zuordnung sollte zunächst durch einen digitalisierten Abgleich der bei der Landeszentralstelle gespeicherten Lichtbilder mit dem von der Ausländerbehörde übermittelten Lichtbild des Ausländers erfolgen, wobei auch eine Auswertung biometrischer Merkmale vorgesehen war. Bei Übereinstimmung mehrerer Bilder sollten weitere Daten verglichen und die Ausländerakte angefordert werden.

Um allen Landeszentralstellen die Speicherung des bundesweiten Bestandes an „herrenlosen“ Ausländer-Ausweisdokumenten zu ermöglichen, sollten die bei der Landeszentralstelle eines Landes gespeicherten Daten über einen sog. Zentralserver an die Landeszentralstellen der anderen Bundesländer verteilt werden. Die Ausgestaltung des Verfahrens sah ferner vor, dass die Aufgabe der Landeszentralstelle eine von der jeweiligen Landesregierung nach § 63 Abs. 1 Satz 2 AuslG bestimmte Ausländerbehörde wahrnehmen soll; die Aufgabe die sog. Zentralservers sollte durch eine Verwaltungsvorschrift des BMI nach § 63 Abs. 2 AuslG bestimmte Landeszentrale wahrnehmen.

Das Vorhaben habe ich einer datenschutzrechtlichen Bewertung unterzogen, deren Ergebnis ich dem SMI dargelegt habe:

Die dateimäßige Speicherung des Lichtbildes und weitere sich aus dem aufgefundenen Ausweisdokument ergebenden personenbezogenen Daten des Ausweisinhabers wäre unzulässig, weil die Ausländerbehörde in einer Datei nur solche Ausländer erfassen darf, mit denen sie im Rahmen einer in § 80 Abs. 1 Satz 1 Nr. 1 AuslG i. v. m. § 2 Abs. 1 AuslDatV genannten ausländerrechtlichen Maßnahme befasst war oder ist. Aufgefundene ausländische Ausweisdokumente aufzubewahren und dem Inhaber zuzuordnen ist jedoch keine solche ausländerrechtliche Maßnahme.

Auch könnte eine Speicherungsbefugnis nicht gemäß § 80 Abs. 1 Satz 1 Nr. 1 AuslG durch eine bloße Rechtsverordnung des BMI geschaffen werden. Voraussetzung wäre

nämlich, dass die Datei zur Aufgabenerfüllung der mit der Ausführung des Ausländergesetzes betrauten Behörde erforderlich ist. Das Gesetz weist der Ausländerbehörde aber nicht die konkrete Aufgabe zu, aufgefundene Ausweisdokumente von Ausländern aufzubewahren und zuzuordnen.

Selbst wenn man eine derartige Zuständigkeit der Ausländerbehörde annähme, habe ich Zweifel, dass die Führung einer Lichtbilddatei durch eine (zentrale) Ausländerbehörde erforderlich ist. Geeignet ist eine solche Datei nämlich nur, wenn sog. Suchbilder von ausweislosen Ausländern abgeglichen werden dürfen. Dies würde voraussetzen, dass die Ausländerbehörde ein Lichtbild eines Ausländers ohne Ausweispapiere anfertigen darf, um dieses zum Zweck der Identitätsfeststellung an die Landeszentrale zu schicken. Lichtbilder anzufertigen ist der Ausländerbehörde aber nur unter den engen Voraussetzungen des § 41 Abs. 2 Satz 1 AuslG i. V. m. § 81 b StPO erlaubt. Die Lichtbilder dürfen nur unter den Voraussetzungen des § 78 AuslG übermittelt und genutzt werden. Nach § 78 Abs. 1 und Abs. 2 AuslG wertet das BKA zum Zweck der Aufgabenerfüllung der Ausländerbehörde die erkennungsdienstlichen Unterlagen aus. Eine Nutzung der mittels erkennungsdienstlicher Maßnahmen gewonnen sog. Suchbilder durch eine (zentrale) Ausländerbehörde, die hierzu Verfahren zur Auswertung biometrischer Merkmale einsetzt, sieht aber das Gesetz bislang nicht vor.

Darüber hinaus werden alle Ausländer nicht erfasst, die Asyl nach dem Asylverfahrensgesetz beantragt haben und deren Identität nicht mehr durch die Ausländerbehörde, sondern durch das Bundesamt für die Anerkennung ausländischer Flüchtlinge gemäß § 16 AsylVfG festgestellt wird.

Schließlich gibt es auch keine Rechtsvorschrift, die die Übermittlung von Lichtbildern, die im Rahmen eines Asylverfahrens zur Identitätsfeststellung eines Ausländers angefertigt wurden, durch das Bundesamt an eine (zentrale) Ausländerbehörde erlaubte. Wenn also sog. Suchbilder nicht in jedem Fall, sondern nur unter engen Voraussetzungen angefertigt und von der Ausländerbehörde nicht mittels Abgleich anhand biometrischer Daten genutzt werden dürfen, erübrigt sich die Führung einer Lichtbilderdatei im vorgesehenen Rahmen. Der Bundesgesetzgeber müsste den Ausländerbehörden die Befugnis verleihen, entsprechende Suchbilder von ausweislosen Ausländern anzufertigen und zur Identitätsfeststellung mittels einer Auswertung biometrischer Merkmale nutzen zu dürfen.

Darüber hinaus bedarf auch die Nutzung der aus den Ausweisdokumenten entnommenen und digital gespeicherten Bilder einer gesetzlichen Befugnis. Diese kann sich nicht aus einer Rechtsverordnung ergeben, die zum Führen der Lichtbilddatei ermächtigt. Der Abgleich von Bildern anhand biometrischer Daten ist ein wesentlicher Eingriff in das Grundrecht auf informationelle Selbstbestimmung sowie das Recht am eigenen Bild, über dessen verfassungsmäßige Rechtfertigung allein der Gesetzgeber zu entscheiden hat.

Ebenso halte ich auch die Einrichtung eines sog. Zentralservers allein durch eine Verwaltungsvorschrift des BMI (mit Zustimmung des Bundesrates) nach § 63 Abs. 2 Nr. 2 AuslG für nicht zulässig, weil die dortigen Voraussetzungen nicht vorliegen und - wie oben ausgeführt - auch gar nicht vorliegen können. Notwendig ist vielmehr eine gesetzliche Vorschrift, die der Ausländerbehörde die Verarbeitung personenbezogener Daten, insbesondere von Lichtbildern zu Zwecken der Identitätsfeststellung, erlaubt. Für die beabsichtigte, für das gesamte Bundesgebiet zuständige, zentrale Ausländerbehörde wäre ein Staatsvertrag der Länder notwendig. Ein bloßes Verwaltungsabkommen reicht nicht aus, weil wesentliche Grundrechtseingriffe nur auf eine Rechtsvorschrift gestützt werden dürfen.

5.13 Wahlrecht

Elektronischer Antrag auf Erteilung eines Wahlscheines

Mit der Neuregelung des § 27 Abs. 1 Satz 2 BWO eröffnet der Verordnungsgeber die zusätzliche Möglichkeit, einen schriftlichen Antrag auf Erteilung eines Wahlscheines bei der Gemeindebehörde durch Telegramm, Fernschreiben, durch formlose E-Mail oder durch das Ausfüllen und Versenden einer von der Gemeindebehörde im Internet bereitgestellten Eingabemaske (virtuelles Formular) zu stellen. Erforderlich ist die Angabe der vollständigen Anschrift des Antragstellers.

Um die zweifelsfreie Identifikation des Antragstellers zu erleichtern und eine missbräuchliche Antragstellung per E-Mail zu verhindern, stimme ich mit dem Landeswahlleiter überein, dass neben vollständigem Namen und Anschrift als Zusatzinformationen auch das Geburtsdatum und – soweit bekannt – die Wählerverzeichnis- und Wahlbezirksnummer gefordert und diese als Zusatzangaben in einer entsprechenden Internet-Eingabemaske im Internet bereits berücksichtigt werden. Im Freistaat Sachsen geht man damit zwar über die nach der BWO vorgegebenen Pflichtangaben hinaus, die Zusatzinformationen sind jedoch regelmäßig erforderlich, die Antragsteller, die von E-Mail und Internet Gebrauch machen, zu identifizieren. Für die Sicherstellung des ordnungsgemäßen Wahlverfahrens ist dies insbesondere von Bedeutung, wenn Wahlschein und Briefwahlunterlagen an eine andere als die Wohnanschrift des Antragstellers gesendet werden sollen. In diesem Falle sollte nur dann auf die Angabe der Zusatzinformationen verzichtet werden, wenn die zweifelsfreie Identifikation des Antragstellers aus anderen Gründen gewährleistet ist. Auch im Interesse der Wahlberechtigten ist es wichtig, dass nicht z. B. ein Nachbar in fremdem Namen - aus welchem Grunde auch immer - einen Wahlscheinantrag stellt.

Im Freistaat Sachsen wurde nach diesen Grundüberlegungen das Muster einer Internet-Eingabemaske entwickelt, die die benötigten Daten als zusätzliche freiwillige Angaben vorsieht und auf deren Bedeutung zur eindeutigen Identifizierung des Antragstellers hinweist. Nur damit erfüllt das Verfahren die in § 9 Abs. 2 SächsDSG

genannten Anforderungen und Maßnahmen zur Gewährleistung des Datenschutzes bei der Bearbeitung personenbezogener Daten; die Grundsatzkriterien der Vertraulichkeit, Integrität, Verfügbarkeit wie der Authentizität. Entsprechendes gilt für die schon bisher mögliche Antragstellung per Telegramm oder Fernschreiben.

In Vorbereitung der Bundestagswahl am 22. September 2002 hatte der Landeswahlleiter bezüglich der Wahlscheinbeantragung per E-Mail in den Info-Briefen Nr. 4 vom 29. April 2002 (Ziffer 1 e) und Nr. 5 vom 12. Juni 2002 (Ziffer 11) und in einer der Besprechungen mit den Kreiswahlleitern wichtige Informationen zum Verfahren gegeben. Aus den Erfahrungsberichten zur Bundestagswahl geht zudem hervor, dass es beim Vollzug der Neuregelung des § 27 Abs. 1 Satz 2 BWO im Freistaat Sachsen keine Probleme gegeben hat. Wahleinsprüche lagen diesbezüglich nicht vor.

Im Rahmen der beabsichtigten Einführung elektronischer Bürgerdienste und E-Government scheint mir das ein gutes und wegweisendes Beispiel dafür zu sein, wie Bürgerservice und Datenschutz zweckmäßig und unaufwändig verbunden werden können.

Sollte sich der Verordnungsgeber in Sachsen zur im Jahre 2004 anstehenden Landtagswahl entschließen, die Antragstellung zur Erteilung von Wahlscheinen per E-Mail und Internet zu ermöglichen, wären auch hier den vorstehenden Ausführungen entsprechende Maßnahmen zur Gewährleistung der Identifikation und Datensicherheit zu ergreifen.

5.14 Sonstiges

5.14.1 Verwaltungsvorschrift Korruptionsvorbeugung

Im Sächsischen Amtsblatt vom 13. Juni 2002 war die Verwaltungsvorschrift der Sächsischen Staatsregierung zur Korruptionsvorbeugung in der staatlichen Verwaltung des Freistaates Sachsen (VwV Korruptionsvorbeugung) vom 21. Mai 2002 erschienen. (Die SPD hat mit der Landtagsdrucksache 3/7175 am 24. Oktober 2002 den Entwurf eines Anti-Korruptionsgesetzes in den Landtag eingebracht.)

Ich konnte diverse Veränderungen mit Datenschutzbezug anregen, die die Bestimmtheit und Klarheit dieser Verwaltungsvorschrift zu verbessern halfen.

So schlug ich u. a. vor, dass der Verantwortliche (und nicht nur Ansprechpartner) für die Anti-Korruption der Dienststellenleiter ist (zu Ziffer 4 a VwV Korruptionsvorbeugung). Die Befugnis, personenbezogene Daten zum Zwecke der Korruptionsvorbeugung mit Datenschutzbezug zu speichern, zu verändern und zu nutzen leitet sich nicht aus dem Strafrecht oder dem polizeilichen Gefahrenabwehrrecht ab, sondern sind

vielmehr auf § 12 Abs. 2 Nr. 3 und Abs. 3 SächsDSG zu stützen. Ich machte darauf aufmerksam, dass eine sorgfältige Personalauswahl in korruptionsgefährdeten Bereichen die Erhebung und Verarbeitung personenbezogener Daten voraussetzt (Ziffer 9 a VwV Korruptionsvorbeugung).

Ich hoffe, dass meine Anregungen aufgegriffen werden und zu datenschutzrechtlichen Verbesserungen in der Verwaltungsvorschrift und ihrem Vollzug führen.

5.14.2 Datenverarbeitung beim Kommunalen Versorgungsverband Sachsen; Datenerhebung zur Nachweisführung in Bezug auf Versorgungsleistungen

Mehrfach wandten sich Bürger an mich, weil sie durch das Handeln des Kommunalen Versorgungsverbandes Sachsen (KVS) ihr Recht auf informationelle Selbstbestimmung verletzt sahen.

In einem Fall hatte ein Bürger beim KVS einen Antrag nach § 5 Abs. 1 VAHRG auf Aussetzung der Kürzung der Versorgungsbezüge gestellt.

Der KVS teilte ihm daraufhin mit, dass er die bestehende Unterhaltspflicht für seine geschiedene Ehefrau nachzuweisen habe. Dabei sollten die Einkommens- und Vermögensverhältnisse der geschiedenen Ehefrau seit dem Ende der Ehezeit substantiiert – gegebenenfalls durch Einkommenssteuerbescheide der Ehefrau - belegt werden.

Mir gegenüber betonte der Bürger, dass er die Beibringung von Steuerunterlagen seiner geschiedenen Ehefrau für zu weitgehend und unverhältnismäßig halte. Darüber hinaus sei durch den KVS nicht erklärt worden, welche Unterlagen beigebracht werden sollen, wenn keine Einkommenssteuerbescheide verfügbar seien. Aus dem Scheidungsurteil ergebe sich seine Unterhaltspflicht gegenüber seiner geschiedenen Ehefrau. Diese Unterhaltspflicht müsse seiner Meinung nach auch nur dem Grunde nach vorliegen.

Der KVS vertrat die Auffassung, dass der Nachweis über die Unterhaltsverpflichtung nicht hinreichend erbracht und die Voraussetzungen für eine Aussetzung der Kürzung nicht hinreichend nachgewiesen worden seien und beschied den Antrag auf Aussetzung der Versorgungsbezüge nach § 57 BeamtVG ablehnend. Er vertrat die Ansicht, dass durch das vorliegende Scheidungsurteil zu Lasten der Versorgungsanwartschaften des Betroffenen für seine Ehefrau Rentenanwartschaften bei der Bundesversicherungsanstalt für Angestellte begründet worden seien. Über die gesetzliche Unterhaltsverpflichtung habe das Familiengericht nicht entschieden. Die inzwischen rechtskräftige Gerichtsentscheidung enthalte lediglich eine über das Quasi-Splitting

hinausgehende Regelung im Wege des schuldrechtlichen Versorgungsausgleichs. Die Unterhaltsverpflichtung sei im Übrigen auch nicht zwischen den Ehegatten auf andere Weise vereinbart worden. Bisherige Angaben des Beschwerdeführers zur Unterhaltspflicht nahm der KVS nach eigenen Angaben zum Anlass, um die Unterhaltspflicht im Einzelfall zu prüfen. So habe der Beschwerdeführer (Petent) gegenüber dem Verband zu anderer Zeit mitgeteilt, dass eine Unterhaltsverpflichtung gegenüber seiner geschiedenen Ehefrau nicht bestehe. Der KVS stellte sich auf den Standpunkt, dass der Petent bis zur erfolgten Entscheidung die notwendigen Nachweise nicht beigebracht habe, so dass eine Aussetzung der Kürzung nach § 5 VAHRG durch den KVS nicht habe erfolgen können.

Der Petent hat zwischenzeitlich Klage beim Arbeitsgericht erhoben. (Das Arbeitsgericht ist hier als Zivilgericht zuständig, da hier die Besonderheit gegeben ist, dass sich der pensionsberechtigte Petent in einem Angestelltenverhältnis befunden hat.) Über den weiteren Fortgang des arbeitsgerichtlichen Verfahrens ist mir nichts bekannt.

In dem vorliegenden Fall handelt es sich um eine beamtenversorgungsrechtliche Angelegenheit, die in Bezug auf den Umfang der Beibringung von Unterlagen durch den Versorgungsempfänger einen datenschutzrechtlichen Bezug aufweist.

Nach § 5 Abs. 1 i. V. m. § 9 Abs. 1 VAHRG wird eine Versorgung nicht nach § 57 BeamtVG gekürzt, solange der Berechtigte, hier die geschiedene Ehefrau des Petenten, einen Unterhaltsanspruch hat. Hieraus leitete der KVS zu Recht ab, dass er die Unterhaltspflicht als Tatbestandsmerkmal des § 5 VAHRG zu prüfen habe.

Er berief sich hierbei u. a. auf eine Entscheidung des Bundesverwaltungsgerichts (2 C 25.98; Urteil v. 22. Juli 1999) aus dem sich die Feststellungspflicht für den KVS ergibt. Für die Feststellung benötigt er Nachweise in Bezug auf den gesetzlichen Unterhaltsanspruch. Die Zahlung von Unterhalt selbst reicht als Nachweis nicht aus, denn diese kann auch ohne gesetzliche Verpflichtung erfolgen. In den Gründen des herangezogenen Urteils heißt es zudem in Bezug auf die Auslegung des § 5 VAHRG sinngemäß, dass es auf Nachweise der tatsächlich erbrachten Unterhaltsleistungen nicht ankomme, um die Aussetzung der Kürzung zu begründen. Insofern wäre eine Datenerhebung in Bezug auf eventuell laufende Zahlungen (z. B. durch Überweisungsbelege) auch nicht erforderlich und geeignet. Zudem ist auch die Höhe des Anspruchs unerheblich (so Palandt, Bürgerliches Gesetzbuch, 62. Aufl., Anh. zu § 1587 b [VAHRG], Rdnr. 2). Aus Vereinfachung und wegen der Praktikabilität habe man eine pauschalierende Regelung geschaffen, so das Bundesverwaltungsgericht an einer anderen Stelle in der Entscheidung. D. h. mit anderen Worten, dass die Unterhaltspflicht dem Grunde nach vorliegen muss. Eine Unterhaltspflicht kann sich aus §§ 1569 ff. BGB ergeben. § 1573 Abs. 2 BGB kam im vorliegenden Fall wegen der möglichen Erwerbslosigkeit der geschiedenen Ehefrau in Betracht. Diese Vorschrift setzt wiederum voraus, dass die geschiedene Ehefrau unterhaltsbedürftig ist (§ 1577

BGB). Für die Unterhaltspflicht entscheidend sind dabei die Einkommensverhältnisse der geschiedenen Ehepartner, die in einem Vergleich gegenüberzustellen sind. Insofern wäre die Erhebung und Verarbeitung von Einkommenssteuerbescheiden der geschiedenen Ehefrau grundsätzlich geeignet und erforderlich und aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Ansonsten müssten Nachweise für die Einkommensverhältnisse aus der Sphäre der Ehefrau beigebracht werden, die nach ständiger Rechtsprechung als Beleg für die Unterhaltsbedürftigkeit anerkannt werden. Die Beibringung solcher Unterlagen ist für den Petenten auch nicht unzumutbar, denn die geschiedene Ehefrau trifft eine Offenbarungspflicht, was die Unterhaltsbedürftigkeit/-pflicht beeinflussende Tatbestände, wie z. B. die Aufnahme einer Erwerbstätigkeit angeht und eine Beweislast gegenüber ihrem geschiedenen Ehegatten in Bezug auf die Unterhaltspflicht allgemein. Dies ergibt sich aus § 1580 BGB (vgl. Palandt, Bürgerliches Gesetzbuch, 62. Aufl., Einf. v. § 1569, Rdnr. 11 sowie § 1577, Rdnr. 38). Dabei ist hinsichtlich des Umfangs der Vorlegungspflicht abzustellen auf den Informationsbedarf des (auskunfts-) berechtigten Petenten. Anerkannt werden neben Einkommenssteuerbescheiden Verdienstbescheinigungen, Geschäftsunterlagen und Umsatzsteuerbescheide. (Zum Umfang der Vorlagepflicht: Wendl/Staudigl, Das Unterhaltsrecht in der familienrichterlichen Praxis, 3. Aufl., § 1 Rdnrn. 578 ff.)

Wird kein bzw. fast kein Einkommen erzielt, könnten zur Nachweisführung neben Eigenerklärungen des geschiedenen Ehegatten z. B. eine kostenfreie Antragsveranlagung (§ 46 Abs. 2 Nr. 8 EStG) durchgeführt bzw. nach behördlicher Übung – sofern ausreichend – eine Nichtveranlagungsbescheinigung bei der zuständigen Finanzbehörde beantragt werden (vgl. § 44 a EStG Abs. 1 Nr. 2, Abs. 2 Nr. 2).

Letztendlich entfiel die Notwendigkeit der Beibringung von Einkommensnachweisen im vorliegenden Fall nicht dadurch, dass das Familiengericht über die Scheidung der Eheleute entschieden hat, denn es enthielt keine Festlegungen zur gesetzlichen Unterhaltspflicht des Petenten gegenüber seiner geschiedenen Ehefrau. Die nach §§ 1587 ff. BGB erfolgende Entscheidung über den Versorgungsausgleich ist Teil des Scheidungsurteils. Der Versorgungsausgleich betrifft allein die Versorgungsrechte, die während der jeweils zu scheidenden Ehe erworben wurden. Nach den Vorschriften werden beamten- und beamtenähnliche Versorgungen ausgeglichen, indem zu Lasten der späteren Versorgung des Verpflichteten für den Berechtigten gesetzliche Anwartschaften begründet werden (Quasi-Splitting oder fiktive Nachversicherung), § 1587 a BGB. Der schuldrechtliche Versorgungsausgleich ist gegenüber dem dinglichen Versorgungsausgleich subsidiär. Er greift überall dort ein, wo ein öffentlich-rechtlicher Versorgungsausgleich aus rechtlichen oder tatsächlichen Gründen nicht möglich ist. Mit dem schuldrechtlichen Versorgungsausgleich wird ein nicht dinglicher Versorgungsanspruch der berechtigten geschiedenen Ehefrau begründet, der z. B. bei angemessener Eigenversorgung auf Null herabgesetzt werden kann (vgl. insbesondere

§ 1587 h BGB). Das Verhältnis zwischen Unterhalt und Versorgungsausgleich besteht dergestalt, dass sich nämlich die Unterhaltsbedürftigkeit des Berechtigten mindert, wenn dieser die durch den Versorgungsausgleich erhöhten Versorgungsleistungen bezieht. Das bedeutet, dass sich der nacheheliche Unterhalt des verpflichteten geschiedenen Ehegatten mindert. (Zur Begründung des Versorgungsausgleichs: vgl. Johannsen/Erich-Hahne – Eherecht, Kommentar, 3. Aufl. § 1587, Rdnrn. 18 ff.; zum Versorgungsausgleich hier: Schwab, Handbuch des Scheidungsrechts, 3. Aufl., VI Rdnr. 3; VI, Rdnr. 64.)

Im Ergebnis meiner Kontrolle habe ich dem Petenten mitgeteilt, dass die Erhebung von Daten durch den KVS in seiner Angelegenheit nicht im Widerspruch zu den gesetzlichen Vorschriften steht. Datenschutzrechtliche Verstöße oder gar beanstandungswürdige Datenverarbeitungsvorgänge konnte ich nicht feststellen.

5.14.3 Datenschutzverstöße in der zentralen Bußgeldstelle

Aufgrund einer Eingabe habe ich die Anforderung einer Auskunft aus dem Personalausweisregister einer Meldestelle durch die zentrale Bußgeldstelle in einem Bußgeldverfahren kontrolliert und bewertet.

1. Das Amtshilfeersuchen an eine Ausweisbehörde einer anderen Stadt war nach seinem Wortlaut unklar und missverständlich. Es war vor allem zweifelhaft, ob dieses Schreiben den Auskunftszweck nannte und nicht gegen den rechtsstaatlichen Verhältnismäßigkeitsgrundsatz verstieß. Die Belehrung des Zeugen in Bezug auf den Lichtbildabgleich auf dem Zeugenbefragungsbogen war ebenfalls in mehr oder weniger gutem Deutsch abgefasst und verwirrend. Merke: Erste Voraussetzung für ein rechtsstaatliches Vorgehen ist gutes Deutsch!

2. Die auskunftsersuchende Stadtverwaltung trägt die Verantwortung, dass die Voraussetzungen für die Datenübermittlung der angeschriebenen Ausweisbehörde vorliegen (§ 2 b Abs. 3 Satz 1 Personalausweisgesetz und § 22 Abs. 3 Satz 1 Passgesetz). Aus welchen Gründen die zentrale Bußgeldstelle tatsächlich nicht in der Lage war, die im Frontfoto sichtbare männliche Person des Fahrers durch Datenerhebung bei dem Betroffenen (und ohne Passbildabgleich) zu identifizieren (vgl. 4/5.9.9), ist aus der Bußgeldakte nicht ersichtlich. Nach § 2 b Abs. 3 Satz 3 Personalausweisgesetz hat die Behörde jedoch den Anlass des Ersuchens aktenkundig zu machen. Bei Rechtsstreitigkeiten, Kontrollen/Rückfragen durch die Staatsanwaltschaft, Gerichte oder den Datenschutzbeauftragten muss die Bußgeldstelle ihre korrekte Arbeitsweise im Ordnungswidrigkeitsverfahren nachweisen**.**

3. Gegen einen zweckändernden Gebrauch des Personalausweis-/Passregisters als ein allgemeines Auskunftsregister hat der Bundesgesetzgeber erhebliche daten-

schutzrechtliche Hürden errichtet. In § 2 b Abs. 3 Satz 2 Personalausweisgesetz ist festgelegt, dass das Auskunftsersuchen an das Ausweisregister nicht von jedem Bediensteten, sondern nur von vom Behördenleiter dafür besonders ermächtigte Bedienstete gestellt werden darf. Eine derartige Ermächtigung existierte nicht.

4. Dem datenschutzrechtlichen Grundanliegen des Gesetzgebers, den Missbrauch des Personalausweisregisters vorzubeugen, wurde auch nicht mit der „Aktion" in dem neuen EDV-Verfahren zur Bearbeitung von Ordnungswidrigkeiten entsprochen, mit der ein Standardschreiben „Fahrer-Ermittlung/Anforderung Lichtbild" bei der jeweiligen Meldestelle ausgelöst wird. Ein solches Schreiben ist auch nicht „ohne Unterschrift gültig". Im Schreiben sind weder die einschlägigen Rechtsgrundlagen angegeben, noch der konkrete Anlass für die Anfrage. Auf diese Weise werden mittels EDV-Verfahren nicht die genannten Datenschutzverstöße verhindert, sondern die Umgehung von Datenschutznormen erleichtert. Das verletzt das Gebot, durch technische, organisatorische und personelle Maßnahmen den Vollzug von Datenschutznormen zu gewährleisten (Grundsatz des Datenschutzes durch Technik, vgl. § 9 SächsDSG).

Nach der Aufklärung des Sachverhaltes bei den Verantwortlichen empfahl ich, zur Beseitigung der festgestellten Datenschutzmängel Folgendes zu veranlassen:

1. Durch den Leiter des Ordnungsamtes wird allein ein sorgfältig ausgewählter Personenkreis von Bediensteten in der zentralen Bußgeldstelle schriftlich ermächtigt, allein die Amtshilfeersuchen nach Passbildkopien anzufordern und zu unterzeichnen (§ 2 b Abs. 3 Satz 2 Personalausweisgesetz).

2. Die Prüfung der Verhältnismäßigkeit eines Bildabgleichs für jeden Einzelfall wird dienststellenintern festgelegt.

3. Die Dokumentation der Gründe und des Anlasses für das Auskunftsersuchen zur Übermittlung einer Passbildkopie mit dem EDV-Verfahren wird schriftlich geregelt (§ 2 b Abs. 3 Satz 3 Personalausweisgesetz).

4. Auf den Zeugenbefragungsbogen wird der Verfahrenshinweis auf den „Lichtbildabgleich" geändert und für den Zeugen klar und verständlich formuliert.

5. Die Sachbearbeiter der zentralen Bußgeldstelle, evtl. auch der Meldestelle, sind über die neue korrekte Verfahrensweise, insbesondere beim Vollzug der angesprochenen Abschnitte von § 2 b Personalausweisgesetz und § 22 Passgesetz zu schulen.

Angesichts dieser Ergebnisse meiner Kontrolle habe ich dem SMI vorgeschlagen, seinen Erlass über die „Einsichtnahme des Polizeivollzugsdienstes und der Bußgeld-

behörden in das Personalausweis- und Passregister vom 18. November 1999“ mit mir erneut zu beraten und diesen Erlass zu präzisieren. Ich strebe dabei an, dass der Abgleich von Frontfotos mit den Passlichtbildern nicht bei Lappalien erfolgt, dass er „angedroht“ werden soll, dass er nicht Teil eines Verwarnungsverfahrens, sondern nur Teil des Ordnungswidrigkeits-Ermittlungsverfahrens sein kann, dass er aber gegenüber einer Befragung Dritter das mildere Mittel ist. Die Vorlage des Frontfotos bei Nachbarn, Arbeitskollegen oder gar Vorgesetzten dürfte dem Betroffenen weniger lieb sein, als der „stille“ Abgleich mit seinem Passfoto, dass als Doppel bei der Passstelle liegt.

6 Finanzen

6.1 Wahrung des Steuergeheimnisses in Informations- und Annahmestellen (IA-Stellen) bei den Finanzämtern

In Sachsen werden die Finanzämter zur besseren Bewältigung des Besucheraufkommens sukzessive mit einer zentralen Anlaufstelle in Form eines Großraumbüros ausgestattet. Dort werden die Steuerpflichtigen in vergleichsweise einfachen Angelegenheiten betreut. Zweck ist u. a., dass die Befassung der Bearbeiter in den spezielleren Sachgebieten mit Routineangelegenheiten vermindert und damit eine effizientere Zeitauslastung in den Finanzämtern möglich wird.

Diese Verfahrensweise kann jedoch dann datenschutzrechtliche Fragen aufwerfen, wenn etwa Steuertatbestände in den so genannten IA-Stellen von Dritten mitgehört werden können. In einer Eingabe wurde eben dieser Umstand kritisiert. Wie bei der „Auskunft auf einem Bahnhof" habe das Gespräch auf dem betreffenden Finanzamt stattgefunden, da unbeteiligte Wartende in unmittelbarer Nähe hinter dem Petenten gestanden hätten.

Wie eine auf diesen Fall bezogene Stellungnahme des SMF klarstellt, haben alle Steuerpflichtigen weiterhin die Möglichkeit, auf einem Gespräch in einer separaten Räumlichkeit zu bestehen. In der Stellungnahme heißt es: „Sollte ein Steuerpflichtiger eine Beratung in der IA-Stelle nicht wünschen, sondern den für ihn zuständigen Berater sprechen wollen, so ist dies *selbstverständlich* möglich. Ein separater Besprechungsraum ... steht ebenfalls zur Verfügung; in der Informations- und Annahmestelle (IA-Stelle) sind die Beschäftigten der IA-Stelle angehalten, die Besucher auf diese Möglichkeit hinzuweisen." Sollte ein Bürger tatsächlich um die Wahrung des Steuergeheimnisses besorgt sein, stehen ihm somit mehrere Möglichkeiten zur Verfügung.

Wer daher das Steuergeheimnis § 30 AO durch die räumlichen Gegebenheiten beeinträchtigt sieht, sollte geltend machen, dass seine Angelegenheit in einem Büroraum oder einem Besprechungsraum durch einen Sachbearbeiter behandelt werden muss.

Aus meiner Sicht ist mit den getroffenen Maßnahmen ein ausreichender Datenschutz gewährleistet. Das Staatsministerium hat mir darüber hinaus versichert, dass in den IA-Stellen jeweils auf die räumlichen Verhältnisse abgestimmte Maßnahmen getroffen wurden. Hierzu gehören u. a. Trennwände, geräuschdämpfende Bodenbeläge und Decken sowie Hinweisschilder zur Wahrung eines ausreichenden Diskretionsabstandes. Hinzu kommen die erwähnten separaten Besprechungsräume. Das SMF hat bei der Oberfinanzdirektion zusätzlich veranlasst, dass die Beschäftigten der IA-Stellen noch einmal ausdrücklich auf die datenschutzrechtliche Problematik hingewiesen werden.

6.2 Automatisiertes Abrufverfahren bei Umsatzsteuerbetrugsfällen und entsprechenden Verdachtsfällen (ZAUBER)

Im Finanzbereich werden staatlicherseits zunehmend die Möglichkeiten erkannt, mit fortschreitender EDV-technischer Hard- und Softwareausstattung die Steuerverwaltung in ihren Bemühungen bei der Bekämpfung von Steuerverkürzung und Steuerhinterziehung zu unterstützen. Als besonders effektiv erscheinen dabei Datenbanken, auf die eine Vielzahl von Behörden online zuzugreifen imstande sind. Bei einer Kontrolle im Rechenzentrum der Finanzverwaltung des Freistaates ließ ich mir die Nutzung einer solchen Datenbank durch die sächsische Verwaltung vorführen. Bei dem kontrollierten Verfahren ZAUBER (Zentrale Datenbank zur Speicherung und Auswertung von Umsatzsteuer-Betrugsfällen und Entwicklung von Risikoprofilen) handelt es sich um eine Verbunddatei, die durch Dateneingaben der Mitarbeiter der Finanzämter in den Ländern gespeist wird. Verwaltet und gepflegt wird die Datenbank in ihrer Gesamtheit durch das Bundesamt für Finanzen. Für die Datenverarbeitungsvorgänge durch Amtspersonen der sächsischen Verwaltung bzw. in Sachsen bin ich zuständig.

Die Umsatzsteuer ist eine der wichtigsten Einnahmequellen von Bund und Ländern. Wegen der Besonderheiten der Steuerart treten im Unsatzsteuerbereich anteilig besonders viele Täuschungsfälle auf. Die Täter operieren nicht selten in mehreren Bundesländern. Die Datenbank soll die bundesweite Erfassung von Betrugsfällen im Bereich der Umsatzsteuer gewährleisten, aktuelle Ermittlungen in möglichen Umsatzsteuer-Hinterziehungsfällen unterstützen, die Schwerpunkte der Umsatzsteuerhinterziehung sowie neue Handlungsmuster und Vorgehensweisen bei der Umsatzsteuerhinterziehung erkennen helfen. Ich begrüße das dahinter stehende Anliegen, steuerrechtliche Verstöße besser aufdecken zu können und das Bemühen um mehr Steuergerechtigkeit.

Das Verfahren ZAUBER wird auf § 88 a AO i. V. m. § 5 Abs. 1 Nr. 13 FVG gestützt. Ich verzichte an dieser Stelle darauf, auf geäußerte rechtliche Bedenken wegen der Bestimmtheit der Vorschrift des § 88 a AO als Rechtsgrundlage für die Datenverarbeitung einzugehen (vgl. hierzu Tipke/Kruse, Kommentar zu Abgabenordnung, Finanzgerichtsordnung, § 88 a AO, Rdnr. 2). Abgesehen von den rechtlichen Voraussetzungen benötigen komplexe Datenbanksysteme und Verarbeitungsmethoden jedoch differenzierte Verfahrensregelungen und Anleitungen für die Nutzer. Die Anwender sind Sachbearbeiter und Sachgebietsleiter der Steuerfahndung, Betriebsprüfung, Strafsachen- und Bußgeldstellen, Umsatzsteuervoranmeldungsstellen sowie der Veranlagungsstellen. Der Zugriff auf die Datenbank erfolgt über den einzelnen zugelassenen Nutzer, der sich mit Namen und Kennwort an der Datenbank anmeldet. Dieser ist dann erst berechtigt Eingaben in hierfür vorgesehene Eingabemasken vorzunehmen. Das Verfahren entspricht modernen Datensicherheitsstandards. Im Hinblick auf die praktische Umsetzung bei der Datenverarbeitung habe ich jedoch festgestellt, dass

sich das Verfahren in Sachsen noch in einer Einführungsphase befindet und Verbesserungen erforderlich sind. Auf wenige Punkte gehe ich im Nachfolgenden ein.

Die entscheidenden Eingaben können, ohne dass sie vordefiniert sind, in ein hierfür vorgesehenes Freitextfeld eingegeben werden. Der Bearbeiter gibt also Informationen nach seinem Ermessen in das System ein. Die eingestellten Daten enthalten damit Informationen unterschiedlichster Art, so Eintragungen über Ermittlungen und Strafverfahren, Beobachtungen, Feststellungen aber auch bloße Vermutungen. Bei dem Verfahren werden also sowohl valide als auch nicht gesicherte Informationen verarbeitet. Die jeweiligen Eintragungen waren in den mir vorgestellten Fällen nicht datiert, so dass einige Informationen auch schon deswegen nach einiger Zeit an Aussagewert verlieren dürften. Das Fehlen einheitlicher inhaltlicher Vorgaben an die Texteingaben halte ich generell für eine Schwäche des Verfahrens. Für die Informationen ist eine 10-jährige Speicherungsdauer vorgesehen. Die Daten werden danach automatisch gelöscht. Ich habe ferner Bedenken bei der Behandlung abgeschlossener Fälle angemeldet. Vorstellbar sind u. a. die Einstellung von Straf-, Bußgeld- und Ermittlungsverfahren, Unternehmerwechsel oder das Versterben eines Steuerpflichtigen. Der Abschluss eines Falls wurde im Verfahren bisher nicht definiert und gekennzeichnet. Es erfolgt daher auch keine Löschung bei abgeschlossenen Fällen. Aus datenschutzrechtlicher Sicht halte ich in diesen Einzelfällen ergänzende Angaben bzw. Löschungen für erforderlich.

Das SMF ist auf meine Bedenken in wesentlichen Punkten eingegangen und hat zugesagt, das BMF auf vorzunehmende Verbesserungen in der Anwendung von ZAUBER aufmerksam zu machen. Das Verfahren ZAUBER und dessen Verbesserung sowie die Nutzung anderer Datenbanken im Bereich der Finanzverwaltung werde ich weiterverfolgen und in meinem nächsten Tätigkeitsbericht umfassend aufgreifen.

7 Kultus

7.1 Informations- und Auskunftsrecht von Eltern volljähriger Schüler

Nach dem Ereignis vom 26. April 2002, bei dem ein Schüler in Erfurt mehrere Lehrer, Mitschüler und sich anschließend selbst tötete, begann eine breite gesellschaftliche Diskussion, bei der im Mittelpunkt Fragen nach Verantwortung und den Möglichkeiten zur Verhinderung des Massakers standen. Der Vater eines der Opfer fragte am 29. April 2002 auf seiner Internetseite: „Warum weiß eine Mutter nicht, dass ihr Sohn vom Gymnasium verwiesen wurde, obwohl er in ihrem Haushalt lebt?“ Die bittere Antwort hierauf lautete, dass nach der Rechtsordnung und in einer Zeit, in der alles geregelt scheint, den Eltern Lasten abgenommen werden, Erziehung verstaatlicht und Kindertageseinrichtungen ein „eigenständiger Erziehungsauftrag“ angemaßt wird (vgl. § 2 SächsKitaG), die Mutter eines volljährigen Schülers noch nicht einmal über entscheidende schulbezogene Ereignisse ihres Sohnes informiert werden durfte. Nach dem Erfurter Ereignis war diese starre auf die Volljährigkeit von Schülern abhebende Sichtweise in Frage gestellt. Wegen der restriktiven Bestimmungen im Schulbereich, die auch in Sachsen die Möglichkeiten der Informationsweitergabe an die Eltern wegen der Volljährigkeit der Schüler hinderten, habe ich daher eine normenklare gesetzliche Neuregelung der Informations- und Auskunftspflicht von Eltern volljähriger Schüler unter Berücksichtigung der datenschutz- und verfassungsrechtlichen Gesichtspunkte angeregt.

Bei der Frage der Informationsweitergabe an die Eltern geht es dabei nicht nur um Einzelfälle wie in Erfurt, sondern auch um die zahlreichen Suizidfälle und –versuche junger Menschen mit Schulproblemen. Nach allgemeiner Erfahrung befinden sich auch volljährige Schüler, die zum Beispiel nicht versetzt werden, den Schulbesuch aufgeben oder schulische Ordnungsmaßnahmen verschuldet haben, in einer Lebenskrise, die nicht selten tragisch endet. Dem angemessen dadurch entgegenzuwirken, dass die Eltern (sie sind nicht irgendwelche Dritte – der Familienverband ist mit der Volljährigkeit nicht beendet) informiert werden, ist gesetzgeberisch nicht nur ein menschliches und an den Lebensrealitäten orientiertes, sondern auch ein verfassungsrechtlich erwünschtes Vorhaben. Der Familienverband ist nach Art. 6 GG besonders zu schützen; er wird häufig in der Lage sein, den jungen Menschen in Lebenskrisen aufzufangen. Deshalb ist eine schulbezogene Information der Eltern volljähriger Schüler in bestimmten Fällen erforderlich. Notwendig wird dies bei drastischen Ordnungsmaßnahmen der Schule, Nichtversetzung, Nichtzulassung bzw. Nichtbestehen in Bezug auf eine Abschlussprüfung sowie die Beendigung des Schulverhältnisses.

Eine Weitergabe von Informationen in diesen Fällen ist als „Eingriff“ in das Grundrecht auf informationelle Selbstbestimmung regelmäßig weder tiefgreifend noch per-

sönlichkeitsstörend. Zu orientieren hat sich der den Volljährigen freiwillig erziehende Staat allein an dessen objektivem Wohl, nicht an seinem bloßen Willen. Er hat dabei immer das mildeste zur Verfügung stehende Mittel einzusetzen. Eine tatbestandsbezogene Informationsweitergabe an die gegenüber ihren Kindern nicht in einem öffentlich-rechtlichen Subordinationsverhältnis agierenden Eltern ist dabei verhältnismäßig und, deren aktive Teilhabe vorausgesetzt, wegen des besonderen Eltern-Kind-Verhältnisses regelmäßig geeignet, in ihrem Fortkommen und ihrer Zukunft gefährdete Heranwachsende positiv zu beeinflussen.

Gestützt wird meine Auffassung durch die Verfassung selbst. Erwachsene sind zwar keine „Kinder" im Sinne des Art. 6 Abs. 2 GG, aber auch nach der Volljährigkeit sind sie noch auf Unterhalt und tatsächliche Hilfe angewiesen. Gründe sind der weitgehend späte Eintritt junger Menschen in das Berufsleben, das Streben und der Erfolgsdruck in Bezug auf höhere Schulbildungen sowie die Herabsetzung der Volljährigkeitsgrenze vom einundzwanzigsten auf die Vollendung des achtzehnten Lebensjahres. Viele Eltern haben daher für die Ausbildung und den Unterhalt ihrer Kinder aufzukommen, ihnen steht aber ein Sorgerecht nicht mehr zu, §§ 1610 Abs. 2, 1620 ff. BGB. Demgegenüber sieht die Rechtsordnung ein Bedürfnis des Jugendlichen an Pflege und Erziehung über die Volljährigkeit hinaus. Dies zeigt sich in den Gesetzen vieler Rechtsbereiche. Das öffentliche Angebot an Hilfe endet nicht mit dem 18. Lebensjahr. Das Jugendwohlfahrtsgesetz, das Jugendgerichtsgesetz, der Familienverband im Melderecht bis zur Vollendung des 28. Lebensjahres bestimmen, dass in der Rechtsordnung viele gegenseitige Pflichten, der Familienverband und die Sorge des Staates vom Erreichen der Volljährigkeit unbeeinflusst sind. So will es Art. 6 GG.

Art. 6 Abs. 2 Satz 2 GG, welches den Staat berechtigt und verpflichtet, über die Pflege und Erziehung der Kinder seitens der Eltern zu wachen, erfährt m. E. in diesem Zusammenhang eine besondere Bedeutung. Die Unterhaltsansprüche eines Kindes gegen seine Eltern, die sich aus den Vorschriften der §§ 1601 ff. BGB ergeben, müssen umgekehrt erlauben, dass unmittelbar in Bezug auf den Regel-(Schul)Abschluss entscheidende oder diesen gefährdende Tatbestände den ehemals Sorgeberechtigten und noch immer Unterhaltspflichtigen bekannt werden. Da dem (bestimmenden) Elternrecht aber wegen der Volljährigkeit (§ 2 i. V. m. § 1626 BGB) relativ starre Grenzen gesetzt sind, die Pflichten der Eltern jedoch weiter bestehen, liegt die Aufgabe des Staates nach Art. 6 Abs. 2 Satz 2 GG darin, die Einhaltung dieser Grenzen und die Erfüllung der Elternpflichten zu überprüfen, notfalls selbst zu übernehmen oder sonst sicherzustellen. Der Staat darf sich daher auch der Mitwirkung und Mithilfe seitens der ehemaligen Erziehungsberechtigten und Eltern bedienen und vergewissern dürfen. Dies stärkt die familiären und natürlichen Beziehungen und dient damit dem Schutz der Familie im Sinne der Verfassung.

Der Sächsische Staatsminister für Kultus ging auf mein Anliegen ein und ließ auf der Grundlage der von mir benannten Gesichtspunkte und Vorschläge den Entwurf

einer Vorschrift erarbeiten. Der vorgesehene neue § 50 a SächsSchulG beinhaltet zum Schutz der volljährigen Jugendlichen und der Gesellschaft die von mir vorgeschlagene Informationsbefugnis der Eltern volljähriger Schüler, die das 21. Lebensjahr noch nicht vollendet haben, durch die Schule. Sie ist Teil des Gesetzentwurfs der Staatsregierung „Zweites Gesetz zur Umsetzung des besseren Schulkonzepts“.

7.2 Datenverarbeitung zur Auslese verhaltensauffälliger Schüler

Der Lehrerpersonalrat einer Schulbehörde hatte sich mit der Bitte um datenschutzrechtliche Prüfung eines Screenings für Verhaltensauffälligkeiten im Schulbereich durch einen freien Bildungsträger an mich gewandt. Die Schulbehörde hatte die Maßnahme gebilligt und sogar veranlasst.

Demgemäß sollten die Lehrer von Grundschulen im Zuständigkeitsbereich der Schulbehörde für jeden einzelnen Schüler einen Bogen mit 49 Fragen in Bezug auf Verhaltensauffälligkeiten ausfüllen. Zwar sollte der Schüler nicht namentlich genannt werden, jedoch wäre aus dem Alter, der Klasse und den einzelnen Antworten mit geringem Zusatzwissen sehr schnell feststellbar gewesen, um welchen Schüler es sich konkret handelt.

Der Fragebogen enthält Fragen u. a. zu „sexuellen Auffälligkeiten“, „Überanpassung“, „Autoaggressionen“ und ähnlichen, tief in die Persönlichkeit hineinreichenden Beobachtungen und Bewertungen. Nach Art. 8 der EU-Richtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995) ist die Verarbeitung besonderer Kategorien personenbezogener Daten nur unter engen gesetzlichen Voraussetzungen zulässig.

In einem Schreiben an das SMK habe ich mit Bekanntwerden mein Unverständnis und meine Kritik an der vorgesehenen Aktion unverzüglich deutlich gemacht und um Bestätigung gebeten, dass derartige Befragungen in Sachsen in Zukunft unterbleiben. Das SMK hat sofort reagiert und die Schulbehörde auf die Unzulässigkeit einer solchen Datenerhebung hingewiesen, die Aktion gestoppt und angewiesen, das bis dahin gesammelte Material unverzüglich zu vernichten.

Es ist nicht Aufgabe des Lehrers, anlassfrei intensiv nach Verhaltensauffälligkeiten der Schüler zu suchen. Erst recht ist es nicht Aufgabe des Staates, das zu befördern. Erst wenn das Ausbildungsziel gefährdet und der Ablauf des Schulbetriebes insgesamt in Gefahr ist; ist es angemessen, Verhaltensauffälligkeiten nachzugehen, um Abhilfe zu schaffen. Die Befragungsaktion zielte offensichtlich darauf ab, Schüler für die Fördereinrichtung eines Freien Trägers (der vielleicht unter Schüler- und damit unter Geldmangel leidet) auszuwählen und von dort, wenn nicht übernehmen, so doch zumindest mitbetreuen zu lassen. Mit dieser Maßnahme wurde also ein Anliegen ver-

folgt, das unter keinem Gesichtspunkt dem erklärten schulpolitischen Ziel bestmöglicher Integration „auffälliger“ Schüler entspricht.

7.3 Unzulässige Datenverarbeitung durch Schulträger

Wiederholt gehen mir Petitionen zu, die die freie Schulwahl in Sachsen zum Gegenstand haben. Auslöser dieser Eingaben sind oftmals betroffene Eltern, die ihre Kinder nicht an der Mittelschule am Ort der Grundschule angemeldet haben, sondern die Schule in einem Nachbarort bevorzugen und nun von ihrer Gemeinde bzw. deren Bürgermeister gezielt angeschrieben werden, ihre Entscheidung nochmals zu überdenken und möglichst rückgängig zu machen. Die dafür notwendigen Adressdaten der Eltern werden bei der Gemeindeverwaltung - bzw. freiwillig oder unfreiwillig bei der Grundschule, die das Kind zu dieser Zeit noch besucht - erhoben. Diese Datenverarbeitungen sind unzulässig.

Aus dem Grundrecht auf informationelle Selbstbestimmung folgt, dass die Datenerhebung und Datenübermittlung grundsätzlich zweckgebunden zu erfolgen hat. Das Speichern, Ändern und Nutzen der Elterndaten (Adressdaten) ist gemäß § 12 Abs. 1 SächsDSG erlaubt, wenn es zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und die Daten nicht in unzulässiger Weise erhoben wurden. Die Daten dürfen nur für die Zwecke verarbeitet werden, für die sie ursprünglich auch erhoben worden sind (z. B. bei Einschulung in die Grundschule). Die Vorschrift, die das Zweckbindungsgebot beinhaltet, gilt auch für die Übermittlung von Daten. Nach § 13 Abs. 1 Nr. 1 SächsDSG ist das Übermitteln personenbezogener Daten dann zulässig, wenn es für die Aufgabenerfüllung der übermittelnden oder der empfangenden Stelle notwendig ist. Im vorliegenden Fall waren die gesetzlichen Voraussetzungen gerade nicht erfüllt. Die Zuständigkeit des Schulträgers für die Schulaufnahme an einer Wahlschule ist schon gar nicht gegeben, so dass sowohl das Übermitteln als auch das Empfangen und Nutzen der personenbezogenen Daten der Eltern, die das Angebot der freien Schulwahl nutzen, unzulässig ist.

In Sachsen gilt mit Abschluss der Grundschule die freie Schulwahl gemäß § 34 SächsSchulG. Die Eltern können also ihr schulpflichtiges Kind an der Mittelschule ihrer Wahl anmelden. Über die Aufnahme des Kindes an der gewählten Schule entscheidet nicht der Schulträger (die Gemeinde), sondern allein die staatliche Schulaufsicht (der Schulleiter). Nur an Schulen, deren Schließung gemäß § 24 SächsSchulG durch den Schulträger beschlossen und durch das SMK bestätigt ist, sind Anmeldungen und Aufnahmen von Schülern nicht mehr möglich.

Daran ändern auch nachvollziehbare Gründe, weshalb eine Gemeinde daran interessiert ist, Schulstandort für eine Mittelschule zu bleiben und dafür eine entsprechende Anzahl von Schülern zu werben, nichts. Verständlich ist es auch, dass ein Bürgermeis-

ter gern erfahren möchte, aus welchen Gründen heraus Eltern, die in seiner Gemeinde wohnhaft sind, ihre Kinder in die Schule im Nachbarort schicken. Es stehen einem Bürgermeister vielfältige Instrumente dafür zur Verfügung, u. a. im Rahmen von Schulelternabenden, Gemeindeforen und Fragestunden, die Entscheidungsfindung für eine Schule im Ort zu fördern bzw. mögliche Kritikpunkte datenschutzgerecht zu erfragen - aber eben alles auf dem Boden völliger Freiwilligkeit.

Merke: So schön und interessant manche politischen Absichten und Ideen sind, sie sind unerlaubt, wenn sie den Boden des Rechts verlassen.

7.4 Fragebogen zur Selbsteinschätzung

Durch einen Hinweis erfuhr ich, dass in einem Ausbildungszentrum eine Fragebogenaktion mit weit in den engsten Persönlichkeitsbereich hinein reichenden Fragen u. a. zur persönlichen Befindlichkeit und zum familiären Umfeld der Auszubildenden durchgeführt wurde. Die durch die Maßnahme gewonnenen Erkenntnisse wollten Lehrkräfte, die die Aktion in Eigeninitiative durchführten, dazu nutzen, aufgrund dieses Hintergrundwissens besser mit den Auszubildenden umzugehen und ihre Lebenslage besser verstehen zu können. Die Ausfüllung der Bogen wurde im Rahmen eines Projekttages als Hausaufgabe angeordnet. Die erhobenen Daten wurden nicht anonymisiert; es fehlte auch der Hinweis auf die Schutzwürdigkeit der Daten. Die volljährigen Auszubildenden wurden weder auf die datenschutzrechtliche Relevanz der Aktion hingewiesen noch wurde ihnen verdeutlicht, dass ihre ausdrückliche Einwilligung die Voraussetzung einer zulässigen Datenverarbeitung im Sinne des Sächsischen Datenschutzgesetzes ist. Die Einwilligung der Eltern der nichtvolljährigen Schüler wurde für diese Aktion ebenfalls nicht eingeholt. Damit verbunden hätte eine detaillierte Information über den Erhebungszweck und die weitere Datenverarbeitung (Speicherung, Nutzung, Löschung) erfolgen müssen. Abgesehen von den fehlenden formalen Voraussetzungen war die Erforderlichkeit der Datenerhebung erkennbar nicht gegeben; sie war unzulässig. Die Lehrkräfte hätten ihrer Aufsichts- und Sorgepflicht gegenüber den ihnen anvertrauten jungen Menschen - z. B. durch Einzel- oder Gruppengespräche in Verbindung mit sorgsamer Beobachtung der Auszubildenden im schulischen Umfeld - zweckmäßiger nachkommen können.

Ich habe mich umgehend an die Leitung des Ausbildungszentrums gewandt und gefordert, dass die Aktion sofort beendet wird und eventuell bereits ausgefüllte Bögen vernichtet werden. Das wurde sicher gestellt und die Lehrkräfte wurden entsprechend informiert.

8 Justiz

8.1 Datenverarbeitung bei den kommunalen Schiedsstellen

Kommunale Schiedsstellen dienen dem Ziel, bürgerliche Rechtsstreitigkeiten bereits vor einem gerichtlichen Verfahren beizulegen. Ihre Tätigkeit ist zwar gerichtsähnlich; zu den Gerichten gehören die Stellen jedoch nicht. Sie sind daher nicht nach § 24 Abs. 2 SächsDSG privilegiert, sondern unterliegen uneingeschränkt meiner datenschutzrechtlichen Kontrolle.

Aus Anlass eines Kontrollbesuches in einer sächsischen kommunalen Schiedsstelle musste ich feststellen, dass bereichsspezifische Regelungen für die Datenverarbeitung der Schiedsstellen fehlten. So gab es keine Aufbewahrungsvorschriften für das Schriftgut der Schiedsstellen, in denen beispielsweise die Speicherungsdauer für die von der Schiedsstelle erhobenen personenbezogenen Daten geregelt wäre. Ebenfalls ungeregelt war, unter welchen Voraussetzungen Dritten (Behörden, Gerichten, Privaten) personenbezogene Daten aus den Unterlagen der Schiedsstelle übermittelt werden dürfen. Alleiniger Maßstab für Eingriffe in das Recht auf informationelle Selbstbestimmung durch die Schiedsstellen waren daher die allgemeinen Bestimmungen des Sächsischen Datenschutzgesetzes.

Vor diesem Hintergrund habe ich gegenüber dem SMJus angeregt, Handlungsanleitungen zu schaffen, die den Umfang der zulässigen personenbezogenen Datenverarbeitung durch die Schiedsstellen präzisieren. Erfreulicherweise griff das SMJus meine Initiative auf und erstellte ein „Merkblatt zum Datenschutz bei den gemeindlichen Schiedsstellen“. Darin wird nun die Verschwiegenheit im Verkehr mit öffentlichen und nicht-öffentlichen Stellen, die Aufbewahrung des Schriftgutes und die Nutzung privater Computertechnik geregelt. Das Merkblatt soll den Schiedspersonen (d. h. dem Friedensrichter und dem Protokollführer) bei ihrer Verpflichtung auf das Datengeheimnis nach § 6 Abs. 2 SächsDSG übergeben werden. Mit dieser Praxis bin ich einverstanden.

8.2 Gestufte Notaraufsicht

Bei der Bearbeitung einer Eingabe eines Notars musste ich die Frage klären, ob es zulässig ist, dass mehrere Instanzen der Notaraufsicht gleichzeitig (parallel) Negativinformationen über den Notar sammeln.

Nach eingehender Prüfung der einschlägigen Rechts- und Verwaltungsvorschriften sowie der Literatur bin ich zu folgender Bewertung gelangt:

Die Bundesnotarordnung regelt, welchen Behörden das Recht der Aufsicht über die Notare zusteht und legt fest, dass diesen Aufsichtsbehörden (Präsident des Landgerichts; Präsident des Oberlandesgerichts; Landesjustizverwaltung = Staatsministerium der Justiz) die Prüfung und Überwachung der Amtsführung der Notare obliegt (§§ 92, 93 BNotO).

Nicht gesetzlich geregelt ist jedoch, welche dieser drei Justizbehörden jeweils zur Ausübung bestimmter Aufsichtsbefugnisse zuständig ist. Die Kommentarliteratur räumt sogar - bezeichnenderweise ohne nähere Begründung - insofern Gestaltungsfreiheit den Landesjustizverwaltungen ein. Falls die Landesjustizverwaltungen keine Regelungen getroffen haben, sei der Präsident des Landgerichts „als erste Aufsichtsinstanz zuständig".

Jedoch regelt im Freistaat Sachsen die Verwaltungsvorschrift des SMJus zur Ausführung der Bundesnotarordnung (VwVAusfBNotO) vom 13. Januar 1999 die Ausgestaltung der Notaraufsicht hierarchisch:

Nach Nr. 19 a VwVAusfBNotO veranlasst der Präsident des Landgerichts die Prüfung der Amtsgeschäfte des Notars gemäß § 93 BNotO, wobei in Aufsichts- und Disziplinarangelegenheiten den höheren Aufsichtsbehörden „über alle wesentlichen Vorgänge" zu berichten ist. Insofern legt die Verwaltungsvorschrift für Aufsichts- und Disziplinarangelegenheiten eine Primärzuständigkeit des Präsidenten des Landgerichts fest und definiert den Präsidenten des Oberlandesgerichts und die Landesjustizverwaltung als „übergeordnete Behörden".

Dem von Aufsichtsmaßnahmen betroffenen Notar steht somit ein Instanzenweg offen. Diese klare Gliederung der Notaraufsicht bedeutet zugleich, dass die Verarbeitung personenbezogener Daten in Aufsichtsangelegenheiten grundsätzlich der zuständigen Instanz, d. h. dem Präsidenten des Landgerichts zugewiesen ist; eventuelle Mitteilungen höherer Instanzen, die im Zusammenhang mit dem die aufsichtliche Maßnahme auslösenden Sachverhalt stehen, können mithin nichts an der Primärzuständigkeit des Präsidenten des Landgerichts ändern.

Dass diese Zuständigkeitsregelung eingehalten wird, ist für die Wahrung des Rechts auf informationelle Selbstbestimmung des betroffenen Notars unerlässlich, muss er doch Klarheit darüber haben, welche Stelle für die Verarbeitung seiner Daten verantwortlich ist. Gäbe es eine parallele und möglicherweise (durch Doppelspeicherungen) sich überlagernde Sachbearbeitung von Landgericht und Oberlandesgericht, würde das Prinzip der Verantwortlichkeit für die Datenverarbeitung, das im Übrigen auch die Europäische Datenschutzrichtlinie vorschreibt, ad absurdum geführt: Der Einzelne sähe sich mehreren öffentlichen Stellen ausgesetzt, die gleichzeitig in derselben Angelegenheit auf seine Grundrechte einwirken.

Eine solche Praxis, wie sie mir im Fall der vorerwähnten Eingabe durch die Sichtung der eingangs genannten Akten offenbar geworden ist, verstieße im Übrigen in gravierender Weise gegen das vom Bundesverfassungsgericht im Volkszählungsurteil festgelegte Transparenzgebot, das die Einhaltung prozeduraler Sicherungen fordert. Denn der betroffene Notar muss darauf vertrauen können, dass die notaraufsichtsregelnde Verwaltungsvorschrift strikt beachtet wird, legt sie doch im Rechtsschutzinteresse des Notars fest, dass dieser zum „Amtsprüfungsbericht" des Präsidenten des Landgerichts gehört wird (Nr. 20 b VwVAusfBNotO).

Diese dem verfassungsrechtlichen Grundsatz des fairen Verfahrens dienende Regelung verlöre ihren persönlichkeitsschützenden Sinn, wenn der Notar besorgen müsste, dass die höheren Aufsichtsbehörden ohnehin über Material „in seiner Sache" verfügen, weil Zuständigkeitsregeln der Verwaltungsvorschrift - gelinde gesagt - leger gehandhabt werden.

Ein „Selbsteintrittsrecht" der Aufsichtsbehörden wird nicht nur durch die Verwaltungsvorschrift - eine grundrechtswahrende und daher zugunsten des Betroffenen verbindliche Norm - ausgeschlossen, sie verbietet sich auch aus allgemeinen verwaltungsrechtlichen Grundsätzen. Im vorliegenden Fall war es demzufolge erst recht dem Oberlandesgericht verwehrt, selbst Material zu sammeln, also Daten unter Außerachtlassung des Landgerichts zu erheben.

Somit bleibt aus datenschutzrechtlicher Sicht festzuhalten:

1. Die Zuständigkeitsregelungen der Verwaltungsvorschrift haben persönlichkeitsschützende Funktion. Sie dienen der prozeduralen Grundrechtssicherung und sind insofern „andere Vorschriften über den Datenschutz" im Sinne des § 26 Abs. 1 SächsDSG. Würden sie nicht eingehalten, müsste dies förmlich beanstandet werden.
2. Die vorstehend dargelegten Grundsätze müssen bei der Bearbeitung von Angelegenheiten der Notaraufsicht durch die sächsischen Justizbehörden strikt eingehalten werden.
3. Die von der Verwaltungsvorschrift in Nr. 20 c vorgesehene Berichtspflicht darf nicht zur Missachtung der Zuständigkeitsregelungen führen.

Das SMJus hat in seiner schriftlichen Erwiderung auf meine vorstehende Argumentation zwar ebenfalls die persönlichkeitsschützende Funktion der Zuständigkeitsregelungen der Verwaltungsvorschrift eingeräumt, jedoch nicht in der gebotenen Deutlichkeit parallele Informationsbeschaffungen der Instanzen abgelehnt. Ich werde daher in den kommenden Monaten bei datenschutzrechtlichen Kontrollen prüfen, ob das SMJus die Gestaltung der Notaraufsicht im Freistaat Sachsen an meinen Empfehlungen ausgerichtet hat.

8.3 Videoüberwachung im Ministerialgebäude des SMJus

Am Ministerialgebäude des SMJus sind dort für Zugangskontrollen, aber auch zur Abwehr von Ordnungswidrigkeiten und Straftaten, sieben Videoüberwachungsanlagen an Haupt- und Nebeneingängen eingesetzt, zwei davon befinden sich unauffällig in Wechselsprechanlagen.

Der Videoüberwachungsbetrieb ist im Einzelnen geregelt. Während der normalen Dienstzeit werden die Videobilder durch die diensthabenden Pförtner des SMJus kontrolliert. Nachts werden die Videobilder an ein zentrales Wach- und Kontrollzentrum im SMI übertragen, von dort ferngesteuert und fernkontrolliert durch Wachleute eines privaten Wachdienstes. Tagsüber erfolgt keine Speicherung der Videoaufnahmen, die nächtlichen Aufnahmen werden jedoch für 60 Stunden aufgezeichnet.

Meine ersten Kontrollen ergaben - wie häufig bei anderen Videoüberwachungen z. B. zur Ausübung des Hausrechts - einige Mängel hinsichtlich der Zulässigkeit dieses Eingriffs in das Selbstbestimmungsrecht der beobachteten Personen.

So fehlten z. B.

- eine Dokumentation der eingesetzten Überwachungstechnik gemäß dem Datei- und Geräteverzeichnis nach § 10 SächsDSG,
- das Datenschutz- und Sicherheitskonzept für die Videoüberwachung gemäß § 9 SächsDSG,
- deutliche Hinweise für die Betroffenen auf die Videoüberwachung, z. B. durch Schilder mit Angaben des Überwachungszweckes und des Ansprechpartners der für die Datenverarbeitung verantwortlichen Stelle (Art. 10 der EG-Datenschutzrichtlinie vom 24. Oktober 1995).

Da von der Videoüberwachung auch Bedienstete des Staatsministeriums betroffen waren, lag auch eine Personaldatenverarbeitung vor. Eine Dienstvereinbarung zwischen der Leitung des Staatsministeriums mit dem Personalrat über die Videoüberwachung (§ 31 Abs. 1 SächsDSG) existierte nicht.

Nachdem zunächst grundsätzliche Zweifel geäußert wurden, ob bei dieser Videoüberwachung überhaupt personenbezogene Daten verarbeitet werden und die Zuständigkeit, insbesondere für die nächtliche Videoüberwachung, schwer zu klären war, hat das SMJus - nunmehr nach diversen Beratungen - einen entscheidenden Schritt in die richtige Richtung getan, mir eine sorgfältig ausgearbeitete „Dienstvereinbarung über Videoüberwachungsanlagen im Ministerialgebäude des SMJus“ vorgelegt, sich also gesetzesgemäß mit mir ins Benehmen gesetzt. Diese Dienstvereinbarung enthält sowohl eine Dokumentation der eingesetzten Überwachungstechnik als auch spezielle Maßnahmen zur Gewährleistung des Datenschutzes. Diese Dienstvereinbarung soll

vom Staatssekretär und dem Personalrat unterzeichnet werden. Für die betroffenen Bürger im öffentlichen Raum sollen Hinweisschilder entsprechend Art. 10 der EG-Datenschutzrichtlinie angebracht werden.

Ich begrüße diese Vorreiterrolle des SMJus und fordere alle anderen, an das zentrale Wach- und Kontrollzentrum angeschlossenen Ministerien auf, in ihrem Zuständigkeitsbereich dafür zu sorgen, dass die Voraussetzungen für eine rechtmäßige Videoüberwachung geschaffen werden, wie ich sie in meinem letzten Tätigkeitsbericht (10/5.14.2) unter dem Titel „Prüfkriterien für rechtmäßige Videoüberwachungen“ ausführlich dargelegt habe.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Nutzung von Fahrerlaubnisakten bei medizinisch-psychologischen Untersuchungen (MPU)

Neben der Bedeutung von Vorstrafen für die Fahreignungsprüfung (vgl. 7/9.1.4) tauchte die Frage nach der Verwertung rechtmäßig angelegter früherer Fahrerlaubnisakten bei der Erstellung eines Gutachtens bei medizinisch-psychologischen Untersuchungen (MPU) auf. Ein Petent, bei dem schon mehrere derartige Untersuchungen negativ ausgefallen waren, wandte sich an mich, weil er nicht hinnehmen wollte, dass vorangegangene MPU-Vorgangsakten zur Grundlage für eine erneute Begutachtung gemacht werden. Das wiederholt für den Antragsteller ungünstige Ergebnis der Untersuchung führte er auf den Inhalt seiner Führerscheinakte zurück.

Hierzu stelle ich Folgendes fest: Der zulässige Inhalt einer Führerscheinakte richtet sich nach der Aufgabe, welche die Fahrerlaubnisbehörde in Führerscheinangelegenheiten nach dem Straßenverkehrsgesetz und der Fahrerlaubnisverordnung zu erfüllen hat. Geeignet zum Führen eines Kraftfahrzeuges ist danach, wer die notwendigen körperlichen und geistigen Anforderungen erfüllt und nicht erheblich oder wiederholt gegen verkehrsrechtliche Vorschriften oder gegen Strafgesetze verstoßen hat (§ 2 Abs. 4 Satz 1 StVG).

Außer der physischen Eignung (Fähigkeit) des Fahrerlaubnisbewerbers ist stets auch seine charakterliche Eignung (Zuverlässigkeit) als Voraussetzung für das Führen eines Kraftfahrzeuges nötig, wobei gegen seine Zuverlässigkeit auch Straftaten nicht verkehrsrechtlicher Art sprechen können. Aus Art und Anzahl der Vorstrafen kann sich eine charakterliche Nichteignung ergeben. Als für die Frage der Eignung wesentlich werden dabei Erkenntnisse angesehen, die im Straßenverkehr zu einer Gefährdung Dritter führen können (vgl. Jagusch/Hentschel, Kommentar zum Straßenverkehrsrecht, 33. Aufl., § 2 Rdnrn. 12 ff.). Stützt die Fahrerlaubnisbehörde ihre Entscheidung auf solche Tatsachen, so müssen diese aktenkundig sein, damit die Verwaltungsentscheidung nachvollziehbar und gerichtlich überprüfbar ist. Insofern bestehen im Grundsatz keine datenschutzrechtlichen Bedenken gegen die Aufnahme entsprechender Unterlagen in die Fahrerlaubnisakte.

Im konkreten Fall waren die Ermittlungsergebnisse verschiedener Behörden bezüglich Fahrens ohne Führerschein, Vortäuschens einer Straftat sowie der wegen Verbreitung gefälschter Führerscheine, Betrug etc. in die Fahrerlaubnisakte eingegangen. Diese Datenverarbeitungen waren rechtmäßig. Die übermittelten Unterlagen belegen

Tatsachen, die auf eine Nichteignung hinweisen und im Zuge eines Verfahrens zur Wiedererteilung der Fahrerlaubnis berücksichtigt werden durften.

In vorangegangenen Tätigkeitsberichten habe ich die Auffassung vertreten, dass der Antragsteller selbst die Verfahrenshoheit über Auswahl des Gutachters und die Freigabe der ihn betreffenden Fahrerlaubnisdaten haben muss (1/5.12.2; 2/9.1.4 und 2/9.1.5). Diese Einschätzung behält auch im dargestellten Fall ihre Gültigkeit. Einer MPU unterzieht sich der Antragsteller *freiwillig*. Weigert er sich allerdings, rechtmäßig verwertbare Teile seiner aktenkundigen Karriere als Verkehrsteilnehmer dem Gutachter zur Verfügung zu stellen, obwohl diese von der Behörde als relevant und unverzichtbar angesehen werden, so hat die Behörde diesen Umstand bei ihrer Entscheidung über eine Zuteilung der Fahrerlaubnis zu berücksichtigen.

9.1.2 Öffentlicher Aushang des Bescheides einer Fahrerlaubnisbehörde

Im Aushangkasten einer Stadtverwaltung hing der Bescheid der Fahrerlaubnisbehörde an einen Bürger aus, der mit Name und Anschrift angegeben war. Darin wird dieser nach § 2 a StVG aufgefordert, sich an einem Aufbauseminar für Fahranfänger „zu unterziehen“; ferner wird veröffentlicht, dass er die Kosten für das Verfahren zu tragen habe. In den anschließenden Entscheidungsgründen wird auf eine Eintragung in das Verkehrszentralregister Bezug genommen (übrigens fehlte im Aushang die Fortsetzung des Bescheides und die Unterschrift).

Die öffentliche Bekanntmachung sei, so die Stadtverwaltung, gewählt worden unter Bezug auf § 15 SächsVwZG, da der Empfänger des Schreibens von der Post nicht aufgefunden werden konnte und der Aufenthaltsort des Empfängers unbekannt war. Ein Wohnungsschild oder ein Briefkasten an der angegebenen Adresse habe gefehlt.

Eine derartige öffentliche Bekanntgabe von sensiblen persönlichen Angelegenheiten des Bürgers verletzt jedoch sein Persönlichkeitsrecht und stellt den Betroffenen an eine Art „öffentlichen Pranger“. Das ist aus Datenschutzgründen unzulässig.

Bei dem Bescheid der Fahrerlaubnisbehörde handelt es sich um eine Anordnung nach § 2 a Abs. 2 Satz 1 Nr. 1 StVG. Weil gegen diese Maßnahme ein befristeter Rechtsbehelf zulässig ist, ist sie durch Zustellung dem Empfänger bekannt zu machen (§ 50 Abs. 1 Satz 1 OWiG), er wird an den Betroffenen zugestellt (§ 51 Abs. 2 OWiG). Für das Zustellungsverfahren gelten gemäß § 51 Abs. 1 Satz 1 OWiG die landesrechtlichen Vorschriften. Nach § 15 Abs. 1 Nr. 1 SächsVwZG kann durch öffentliche Bekanntmachung zugestellt werden, wenn der Aufenthaltsort des Empfängers unbekannt ist.

Bei der öffentlichen Zustellung ist entweder das zuzustellende Schriftstück oder eine

Benachrichtigung an der dafür bestimmten Stelle auszuhängen, in der anzugeben ist, dass und wo das Schriftstück abgeholt werden kann. Eine solche Benachrichtigung ist auszuhängen, wenn die berechtigten Interessen eines Beteiligten es gebieten (§ 15 Abs. 2 Satz 3 SächsVwZG). Diese Regelung ist im Interesse des Grundrechtes der Betroffenen auf informationelle Selbstbestimmung verfassungskonform auszulegen. Danach darf im Regelfall lediglich nur eine Benachrichtigung ausgehängt werden. Das Aushängen des kompletten Schriftstückes ist nur auf Ausnahmefälle zu beschränken. Ein solcher Extremfall wäre z. B. dann gegeben, wenn das Interesse des Betroffenen eine sofortige Kenntnisnahme des vollständigen Inhalts des zuzustellenden Schriftstückes sein vermutetes Interesse an der Wahrung seiner Privatsphäre überwiegt. Ein solcher Fall liegt hier offensichtlich nicht vor.

Im Allgemeinen genügt bei derartigen öffentlichen Bekanntmachungen eine schlichte Mitteilung, dass – unter Bezug auf die Rechtsgrundlage – der betreffende Bürger, dessen letzte Wohnanschrift angegeben wird, in einem angegebenen Amt zu den üblichen Sprechzeiten ein Schriftstück in Empfang nehmen kann. Gegebenenfalls kann damit ein Hinweis auf die Rechtsfolgen dieser Zustellung angeführt sein. Ein Hinweis auf den Inhalt des Schreibens ist im Hinblick auf den größtmöglichen Schutz der Privatsphäre nicht angebracht und hat zu unterbleiben.

Nach einigen Diskussionen versprach die Stadtverwaltung, in Zukunft dafür zu sorgen, dass in solchen Fällen allein die Benachrichtigungskarte über das Abholen eines Schriftstückes im Schaukasten ausgehängt werden soll.

9.1.3 Unzulässige Datenerhebungen bei der Ahndung von Verkehrsordnungswidrigkeiten

Bei Verfahren zur Ahndung von Verkehrsordnungswidrigkeiten stehen die Bußgeldbehörden oft vor dem Problem, dass sich der Tatvorwurf gegen den Fahrzeugführer richtet, aber nur der Halter des Fahrzeuges - über das Kfz-Kennzeichen - ermittelt werden kann. Um den Fahrzeugführer herauszufinden, hatte deshalb eine sächsische Bußgeldstelle Formulare verwendet, mit denen der Fahrzeughalter nach dem verantwortlichen Fahrzeugführer befragt wurde. Das Formular enthielt auch den Hinweis, dass dem Halter im Weigerungsfall eine Fahrtenbuchauflage erteilt oder die Kosten des Verfahrens auferlegt würden.

Diese Praxis habe ich kritisiert. Denn die Befragung ist eine Datenerhebung bei Dritten, die in diesem Stadium des Ordnungswidrigkeitenverfahrens zur Aufgabenerfüllung der Bußgeldstelle nicht erforderlich ist: Denn bei der ersten Stufe dieses Verfahrens, dem Verwarnungsgeldverfahren, wird nämlich noch keine Entscheidung darüber getroffen, ob der Betroffene eine rechtswidrige oder vorwerfbare Handlung begangen hat. Diese Entscheidung hat die Bußgeldstelle erst nach einer umfassenden

Ermittlung des Sachverhaltes im Bußgeldverfahren zu treffen. Die Durchführung eines Verwarnungsgeldverfahrens zielt gerade darauf ab, Ermittlungen zu vermeiden, die im Rahmen eines späteren Bußgeldverfahrens eventuell angestellt werden müssen. Auch ist zu berücksichtigen, dass die Verfahrenserledigung per Verwarnung von der freiwilligen Mitwirkung des Betroffenen abhängt. Diese freiwillige Mitwirkung kann aber nicht die Übermittlung von Daten Dritter, nämlich des Kfz-Führers, umfassen, weil der Betroffene nicht über die Persönlichkeitsrechte dieser Person verfügen kann. Dies bedeutet, dass im Verwarnungsgeldverfahren der Betroffene nicht dazu aufgefordert werden darf, Daten Dritter zu übermitteln. Der Dritte darf nämlich nur durch eine Ermittlungshandlung der Behörde im Rahmen des Bußgeldverfahrens nach § 35 OWiG ermittelt werden.

Erst recht ist es unzulässig, bereits im Verwarnungsgeldverfahren beim Betroffenen den Eindruck zu erwecken, im Weigerungsfall könne er mit einer Fahrtenbuchauflage oder den Kosten des Verfahrens belastet werden. Ein Hinweis dieser Art darf erst ergehen, wenn sich das Verfahren in der nächsten Stufe, d. h. im Bußgeldverfahren, befindet.

Aufgrund meiner Kritik hat die Behörde inzwischen die Formulare datenschutzgerecht gestaltet.

9.2 Gewerberecht

In diesem Jahr nicht belegt.

9.3 Industrie- und Handelskammern; Handwerkskammern

In diesem Jahr nicht belegt.

9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

9.5 Sonstiges

In diesem Jahr nicht belegt.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

Patientendatenschutz in Kliniken

Durch die Eingabe einer Petentin wurde ich über folgenden Sachverhalt informiert: Kurz nachdem diese im Krankenhaus eines öffentlich-rechtlichen Trägers entbunden hatte, hatte sie gegen ihren Willen umfangreiche Werbesendungen eines Anbieters von Babyartikeln erhalten. Die Petentin mutmaßte, dass der Umstand ihrer Entbindung und ihre Anschrift durch eine „undichte“ (öffentliche) Stelle an den Anbieter gelangt sein könnte.

Meine Recherchen ergaben keinen Hinweis auf einen Datenschutzverstoß bei einer der mit dem Geburtsvorgang befassten öffentlichen Stellen (Krankenhaus bzw. Standesamt des Geburtsorts). Gleichwohl nehme ich diesen Vorgang zum Anlass, auf Folgendes hinzuweisen:

Im Krankenhaus erhalten die verarbeiteten Informationen die Qualität von Patientendaten und unterliegen damit einem besonderen Schutz, § 33 SächsKHG (vgl. u. a. 9/10.1.3). Eine Weitergabe zu kommerziellen Zwecke ist nicht voraussetzungslos zulässig. Die Krankenhausleitung ist daher gehalten, ihre Mitarbeiter über diese Rechtslage regelmäßig zu belehren.

Die zuständigen Standesämter sind über die Geburt zu unterrichten (§§ 16 ff. PStG). Regelmäßig erfolgt die Benachrichtigung durch die Entbindungsstationen der Krankenhäuser. Soweit nachher Anfragen von privater Seite erfolgen, die Daten über Neugeburten in der Gemeinde betreffen, ist die Weitergabe der Daten an diese nur statthaft, wenn die Betroffenen wirksam in eine Datenübermittlung eingewilligt haben (Schriftform).

Die in den Krankenhäusern verwendeten Geburtsanzeigeformulare enthalten meist Abschnitte, die eine Einwilligung in die Datenweitergabe vorsehen. Häufig sind die verwendeten Vordrucke nicht datenschutzgerecht. Wegen der erforderlichen Wirksamkeit der Einwilligungen sollten die Krankenhäuser als Verwender der Formulare sicherstellen, dass der Einwilligende den Kreis der Datenempfänger hinreichend konkretisieren kann. Keinesfalls darf die Einwilligung stillschweigend vorausgesetzt werden (§ 4 Abs. 1 Nr. 2 SächsDSG). Das Muster einer datenschutzgerechten Einwilligung ist unter 11/16.2.3 abgedruckt.

10.2 Sozialwesen

10.2.1 Kein Recht der Krankenkassen auf eigene Einsichtnahme in die Behandlungsunterlagen der Krankenhäuser

Über die Zulässigkeit der Anforderung von Arzt-, Operations- und Entlassungsberichten durch die gesetzlichen Krankenversicherungen an sich selbst - statt an den MDK - hat es in den letzten Jahren heftige Auseinandersetzungen zwischen den Krankenkassen und den Datenschutzbeauftragten des Bundes und der Länder gegeben. Die „Kassen“ wollten, auch in Sachsen, mit Hilfe dieser Unterlagen vor allem das Bestehen ihrer Leistungspflicht unter dem Gesichtspunkt der sachlich-rechnerischen Richtigkeit der Krankenhausabrechnung überprüfen. In meinem 9. Tätigkeitsbericht habe ich unter 10.2.3 im Hinblick auf einen etwas anders gelagerten Informations-Gewinnungs-Zweck, nämlich die von Krankenkassen an Krankenhäuser gerichteten Auskunftsersuchen bei Vorliegen von Anhaltspunkten für eine Verantwortung dritter Schadensverursacher, ausführlich begründet, warum sowohl die Datenübermittlung durch das Krankenhaus als auch die Datenerhebung durch die Krankenkasse mangels Rechtsgrundlage unzulässig wären. Zwar habe ich mich insoweit damals gegenüber - oder sagen wir freundlicher: bei - einer gesetzlichen Krankenversicherung in Sachsen durchgesetzt (den seinerzeit von dieser für kurz bevorstehend gehaltenen § 294 a SGB V gibt es, das sei nur am Rande erwähnt, immer noch nicht). Aber im Übrigen, also was die Anforderungen der pauschal als *Krankenhausentlassungsberichte* bezeichneten Unterlagen zu Zwecken der Abrechnungskontrolle betrifft, konnten sich die Krankenkassen seinerzeit zunächst auf eine nicht Krankenhäuser, sondern Vertragsärzte betreffende Entscheidung des LSG Baden-Württemberg vom 11. Dezember 1996 - L 5 KA 1130/95 - sowie eine Entscheidung des Bayerischen LSG von 1998 und dann auf eine sich daran anschließende gerade Krankenhäuser betreffende Rechtsprechung, namentlich eine Entscheidung des LSG Rheinland-Pfalz vom 1. März 2001 - L 5 KR 55/00 -, berufen, die ihnen ein Recht auf Herausgabe der Behandlungsunterlagen ihrer Versicherten zum Zwecke der Rechnungsprüfung und Wirtschaftlichkeitskontrolle zusprach. Da meine Kollegen und mich diese Rechtsprechung rechtlich nicht überzeugt hat und die Datenschutzbeauftragten - aber auch etwa das Bundesversicherungsamt - allenthalben diese Rechtsprechung nicht akzeptiert haben, ist die Rechtslage umstritten gewesen, bis das Bundessozialgericht die Auffassung der Datenschützer bestätigt und das Urteil des LSG Rheinland-Pfalz (welches die Revision nicht zugelassen hatte!) mit Urteil vom 23. Juli 2002 - B 3 KR 64/01 R, NJW 2003, 845, aufgehoben hat.

Nach dieser Entscheidung haben die Krankenkassen zwar das Recht, eine Krankenhausabrechnung auch rechnerisch und sachlich zu überprüfen. „Die für die sachlich-rechnerische Überprüfung einer Krankenhausabrechnung gegebenenfalls erforderliche Einsichtnahme in die Behandlungsunterlagen der Versicherten können die Krankenkassen indessen [...] nicht verlangen. Sie sind insoweit vielmehr auf ein

Tätigwerden des MDK angewiesen“ (BSG, a. a. O. S. 847 lSp.). Zwar sind die Krankenkassen, so das Gericht, nach § 284 Abs. 1 Nrn. 7 und 8 SGB V befugt, Sozialdaten für Zwecke der Krankenversicherung zu erheben, soweit dies für die Beteiligung des MDK (§ 275 SGB V) bzw. zur Abrechnung mit den Leistungserbringern erforderlich ist. *Bei wem* die Sozialdaten erhoben werden dürfen, bestimmt die Vorschrift jedoch nicht. Dies richtet sich, so das BSG, vielmehr nach § 67 a SGB X (da nach § 37 Satz 2 SGB I i. V. m. § 35 Abs. 2 SGB I die Erhebung von Sozialdaten durch die Krankenkassen nur unter den Voraussetzungen des 2. Kapitels des SGB X zulässig ist). Nach § 67 a Abs. 2 Satz 2 Nr. 2 Buchstabe a SGB X dürfen Sozialdaten ohne Mitwirkung des Betroffenen bei anderen als in § 35 SGB I bzw. § 69 Abs. 2 Sozialgesetzbuch Zehntes Buch genannten Stellen oder Personen, mithin auch bei Krankenhäusern, nur erhoben werden, wenn eine Rechtsvorschrift die Erhebung bei Ihnen zulässt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt.

Eine solche Erlaubnisnorm gibt es dem Urteil zufolge nicht: § 100 Abs. 1 Satz 1 Nr. 1 SGB X kommt nach Auffassung des Gerichtes schon von der Rechtsfolge her nicht in Betracht, weil die Vorschrift, wie sich bereits aus dem Wortlaut ergebe, eine Auskunftspflicht normiere, eine Auskunft jedoch etwas anderes sei als die Herausgabe von Unterlagen.

§ 301 SGB V kommt deswegen nicht als Rechtsgrundlage für die Herausgabe ärztlicher Berichte in Betracht, weil die Vorschrift aus datenschutzrechtlichen Gründen *abschließend* aufzähle, welche Angaben den Krankenkassen bei einer Krankenhausbehandlung ihrer Versicherten durch die Krankenhäuser (unmittelbar) zu übermitteln sind, Behandlungsunterlagen der Versicherten jedoch gerade keine Erwähnung gefunden hätten.

Inwieweit § 67 a Abs. 2 Satz 2 Nr. 2 Buchstabe b SGB X eine Erhebungsbefugnis der Krankenkassen begründen könnte, weil die Aufgaben der Krankenkassen nach dem Sozialgesetzbuch ihrer Art nach eine Erhebung bei dem Krankenhaus erforderlich machen (§ 67 a Abs. 2 Satz 2 Nr. 2 Buchstabe b aa SGB X) oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde (Buchstabe b bb) hat das Gericht (anders als bei rein datenschutzrechtlicher Betrachtungsweise, vgl. 9/10.2.3 S. 134 oben) offenlassen können, weil es für seine Entscheidung nur darauf ankam, ob die Krankenkassen einen *Anspruch* auf Überlassung der für erforderlich gehaltenen Unterlagen haben, was sich aus diesen beiden Vorschriften jedoch nicht ableiten lässt, die ja nur *Erhebungs-Befugnisse* aussprechen.

Entsprechende Übermittlungsbefugnisse oder gar Übermittlungspflichten der Krankenhäuser enthält das Sozialgesetzbuch, namentlich in §§ 86 bis 119 SGB X, nicht.

Abschließend hat das Gericht auch noch § 67 a Abs. 1 Satz 1 SGB X als mögliche Erhebungsbefugnis zugunsten der Krankenkassen geprüft, ist aber zu dem Ergebnis

gekommen, dass weder für die Abrechnung mit den Leistungserbringern (§ 284 Abs. 1 Satz 1 Nr. 8 SGB V) noch für die Beteiligung des MDK (Nr. 7 der genannten Vorschrift) die Krankenkassen selbst in die Behandlungsunterlagen Einsicht nehmen können müssen, so dass es an der in § 67 a Abs. 1 Satz 1 SGB X verlangten *Erforderlichkeit* fehlt. Denn es reicht aus, nach § 275 Abs. 1 Satz 1 Nr. 1 SGB V bei Zweifeln an der sachlich-rechnerischen Richtigkeit einer Krankenhausabrechnung eine gutachtliche Stellungnahme des MDK einzuholen. Und dieser ist im Falle einer Abrechnungsprüfung nach § 276 Abs. 2 Satz 1, 2. Halbsatz SGB V ausdrücklich ermächtigt, die erforderlichen Sozialdaten bei den Krankenkassen anzufordern, und nach § 277 Abs. 1 Satz 1 SGB V verpflichtet, den Krankenkassen die notwendigen Informationen, d. h. das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund, mitzuteilen.

Ich gehe davon aus, dass die Krankenversicherungen das Urteil des Bundessozialgerichtes beherzigen und sich nicht mehr mit derartigen Verlangen an die Krankenhäuser wenden.

Es könnte sein, dass sich ein praktisches Bedürfnis dafür herausstellt, dass die Krankenkassen über die ihnen nach § 301 Abs. 1 Satz 1 Nr. 3 SGB V standardisiert nach dem sog. ICD-Code (§ 301 Abs. 2 SGB V) mitzuteilenden Diagnosen hinaus in denjenigen Fällen besondere Ausprägungen einer Erkrankung mitgeteilt bekommen, in denen nur diese besondere Ausprägung - eben ausnahmsweise - eine stationäre Behandlung erforderlich macht und daher rechtfertigt. Das ermöglichte der Krankenkasse, in solchen Fällen von einer Überprüfung durch den MDK - und damit auch von einer Verarbeitung personenbezogener Daten - abzusehen. Man würde dann genau prüfen müssen, ob diese zusätzlichen Angaben noch von § 301 Abs. 1 Satz 1, insbesondere Nr. 3, SGB V umfasst sind oder eine dahingehende Ergänzung des dort beschriebenen Datensatzes erforderlich wäre. Gegenüber dem, was die Krankenkassen bisher alles als sog. Krankenhausentlassungsberichte angefordert haben, bestünde jedoch auf jeden Fall ein himmelweiter Unterschied.

10.2.2 Verarbeitung personenbezogener Daten durch Krankenkassen zu Zwecken der Mitgliederwerbung

Eine bundesweit tätige Krankenkasse bat mich, dagegen einzuschreiten, dass die AOK und die IKK Sachsen vormals bei ihnen Versicherte anschrieben, um sie für eine Rückkehr in die frühere Krankenkasse zu gewinnen. AOK und IKK hatten, wie sich herausstellte, nur getan, was fast alle anderen gesetzlichen Krankenkassen in dieser oder jener Form auch taten. Wie im Falle der Marktforschung (9/10.2.2) ist Hintergrund für ein solches für öffentliche Stellen - „Körperschaften des öffentlichen Rechtes“! - ungewohntes Verhalten der so genannte Wettbewerb zwischen den gesetzlichen Krankenkassen aufgrund des durch das „Gesundheitsstrukturgesetz“ vom

Dezember 1992 in § 173 SGB V eingeräumten Rechtes, unter verschiedenen gesetzlichen Krankenversicherungen zu wählen.

Hier handelte es sich schlicht um Versuche der *Mitglieder-Rückwerbung* mittels der noch von der früheren Mitgliedschaft her vorhandenen Daten.

Ich habe AOK und IKK erklärt, dass solche Aktionen nur auf der Grundlage wirksamer Einwilligungserklärungen zulässig sind, in denen die früheren Mitglieder der Nutzung ihrer Daten zu Zwecken der Rück-Werbung von vornherein, also zumindest noch im Zusammenhang mit der Beendigung der Mitgliedschaft, zugestimmt haben. Die Nutzung der Daten ist dann nach § 284 Abs. 3 SGB V i. V. m. § 67 b Abs. 1 Satz 1 SGB X zulässig.

Eine Einwilligungserklärung, die diese Voraussetzungen erfüllt, hat aber, soweit ersichtlich, im Regelfall gefehlt.

Gegenüber meiner Rechtsauffassung konnte sich die AOK mit Recht auf den einen oder anderen meiner Kollegen berufen, der die Verarbeitung personenbezogener Daten zu Zwecken der Mitglieder-Rückwerbung als durch § 284 Abs. 1 Satz 1 Nr. 1 SGB V erlaubt angesehen hat, weil seiner Meinung nach nicht nur auch schon die bloße Anbahnung von Versicherungsverhältnissen zur „Feststellung des Versicherungsverhältnisses“ im Sinne dieser Vorschrift gehöre, sondern sogar darüber hinaus auch die Mitgliederrückwerbung unter eine solche Anbahnung falle.

Dem habe ich mich nicht anschließen können, weil die Krankenkasse bei der Mitgliederrückwerbung Daten nutzt, die der Versicherte der Krankenkasse in Erfüllung seiner Versicherungspflicht seinerzeit anvertraut hat.

Nunmehr kann man die Rechtslage als bis auf weiteres geklärt betrachten, nachdem das Bundessozialgericht mit Urteil vom 28. November 2002 - B 7/1 A 2/00 R -, RDV 2003, 142 in Bestätigung einer vom BVA gegenüber den Ersatzkassen eingenommenen strengen Auffassung wohl jeglicher Werbung der gesetzlichen Krankenkassen einen Riegel vorgeschoben hat, sofern bei dieser seitens der Krankenkasse personenbezogene Daten *erhoben* werden.

Dazu hat das Gericht (1) zunächst klargestellt (S. 144 rSp. unten/145 lSp. oben), dass (entgegen einer auch von einzelnen Datenschutzbeauftragten vertretenen weniger strengen Auffassung) auch die zum Zwecke einer Mitglieder-*Neu*werbung von den Krankenkassen zu erhebenden Daten *Sozialdaten im Sinne von § 67 Abs. 1 Satz 1 SGB X* sind, dass ihre Verarbeitung durch die Kassen also den Regeln insbesondere auch der §§ 67 ff. SGB X unterliegt, und zwar das, *obwohl* nach einer weiteren, noch wichtigeren Feststellung des Gerichtes (2 a) die Mitgliederwerbung, solange entsprechende Gesetzesänderungsvorhaben (vgl. BT-DS 14/1245) noch nicht verwirklicht

sind, nicht zu den Aufgaben gehört, für welche die Krankenkassen personenbezogene Daten *erheben* dürfen (S. 143 lSp. oben), abgesehen davon, dass überdies (2 b) eine Beschaffung personenbezogener Daten auch gar nicht für die Erfüllung einer Aufgabe „Mitglieder-Werbung“ erforderlich im Sinne von § 67 a Abs. 1 Satz 1 SGB X wäre - weil sich Werbung eben auch anders betreiben lässt, nämlich so, dass der Werbende sich an das Publikum richtet und es dem einzelnen Interessenten überlässt, den persönlichen Kontakt aufzunehmen (S. 143 rSp. unten/144 lSp. oben).

Dass (1) trotz (2 a) gilt, begründet das Gericht mit der für das allgemeine Datenschutzrecht bedeutsamen Überlegung (3), dass die Anwendung der Vorschriften über den Sozialdatenschutz dann, wenn der Adressat der Schutzgebote [also der Verbote mitsamt der zugehörigen Erlaubnis-Ausnahmen] sich auf eine gesetzliche Aufgabe nach dem Sozialgesetzbuch beruft, nicht davon abhängig gemacht werden könne, ob diese Ansicht richtig ist (S. 145 lSp. oben).

Allgemeiner formuliert bedeutet das: Beruft sich eine öffentliche Stelle darauf, zur Erfüllung einer ihr gesetzlich übertragenen Aufgabe personenbezogene Daten zu verarbeiten, so ist diese Datenverarbeitung schon dann rechtswidrig, wenn die Verarbeitung bei Richtigkeit dieses von der öffentlichen Stelle eingenommenen Standpunktes rechtswidrig wäre. (Man wird vielleicht einschränken können, dass dies zumindest im Bereich der so genannten besonderen Geheimnisse, also der spezialgesetzlichen allgemeinen datenschutzrechtlichen Verarbeitungsverbote, gilt, d. h. in Bereichen wie dem des Sozial-, des Steuer- und des Statistikgeheimnisses.)

Außerdem hat das Gericht (4), damit über das BVA hinausgehend, für die Datenerhebung, also die Neu-Werbung, hervorgehoben, dass insoweit auch die Einwilligung der Betroffenen die Erhebung wohl nicht rechtfertigen kann, weil das Gesetz dies anders als für alle (anderen) Verarbeitungsarten (§ 67 b Abs. 1 Satz 1 SGB X) nicht vorsieht (S. 144 rSp., 145 lSp. oben).

Schließlich hat die Entscheidung (5) die mit dem von mir gegenüber den genannten gesetzlichen Krankenversicherungen eingenommenen Standpunkt übereinstimmende Folgerung gezogen (S. 145 lSp.), dass die Krankenkassen bei fehlender Einwilligung des Betroffenen vorhandene personenbezogene Daten zu Werbezwecken nicht *nutzen* oder sonst *verwenden* dürfen: § 67 Abs. 1 i. V. m. § 67 c SGB X.

Insgesamt bin ich also durch das Urteil in meiner vergleichsweise strengen Auffassung bestätigt, ja was Fragen angeht, die in Sachsen noch nicht zu entscheiden gewesen waren, noch überboten worden.

10.2.3 Übermittlung von Sozialdaten durch eine Krankenkasse an eine GmbH zum Zwecke der Überprüfung von Kostenvoranschlägen für Sehhilfen

Eine Krankenkasse hat mich davon unterrichtet, dass sie mit einer GmbH eine „Vereinbarung zur Überprüfung von Kostenvoranschlägen für Sehhilfen“ abgeschlossen habe. Damit die GmbH die Kostenvoranschläge von Optikern und Augenärzten auf ihre „Wirtschaftlichkeit und Zweckmäßigkeit“ prüfen könne, übermittelte die Krankenkasse ihr die Verordnung oder den Berechtigungsschein, den Kostenvoranschlag und eine Darstellung vorheriger Versorgungen. Diese Unterlagen enthielten den Namen und das Geburtsdatum des Versicherten, die Indikation sowie die Art und den Preis der Versorgungsleistung.

Die Krankenkasse sah in der Begutachtung eine sog. Datenverarbeitung im Auftrag (§ 80 SGB X). Eine solche Datenverarbeitung im Auftrag im Sinne des § 80 SGB X ist zu unterscheiden von einer sog. Funktionsübertragung. Abzugrenzen sind beide Formen danach, ob lediglich die Datenverarbeitung in ihrer „Hilfsfunktion“ dem Auftragnehmer übertragen wird oder ob dieser über die technische Durchführung der Verarbeitung hinaus mit Hilfe der überlassenen Daten materielle vertragliche Leistungen erbringt, und damit eine Aufgabe des auftraggebenden Leistungsträgers erfüllt (vgl. von Wulffen/Roos, SGB X, 4. Auflage 2001, § 80 Rdnr. 3; Kasseler Kommentar-Scholz, Sozialversicherungsrecht, Band 2, Stand: August 2002, SGB X § 80, Rdnr. 4; Hauck/Haines, Sozialgesetzbuch, Kommentierung zu § 80 SGB X, Rdnr. 20).

Bedeutsam ist diese Abgrenzung von Datenverarbeitung im Auftrag und Funktionsübertragung deshalb, weil bei jener die Datenverarbeitung privilegiert ist, bei dieser jedoch nicht. Konkret: Anders als bei der Datenverarbeitung im Auftrag stellt die Datenweitergabe an den von der Behörde eingeschalteten Dritten bei der Funktionsübertragung eine Übermittlung personenbezogener Daten dar, die nur dann zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat (§ 67 b Abs. 1 Satz 1 SGB X).

Auf meine Stellungnahme hin, dass hier wohl eine Funktionsübertragung vorliege, mit der Folge, dass der GmbH personenbezogene Daten übermittelt würden, eine Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X jedoch nicht in Betracht komme, zog die Krankenkasse in Betracht, die Einwilligung der Versicherten einzuholen. Eine Einwilligungserklärung kann aber aus folgendem Grund nicht Rechtsgrundlage einer Datenübermittlung, wie sie hier beabsichtigt war, sein: Die öffentliche Stelle darf nicht eine Datenverarbeitung durch Dritte auf Einwilligungsgrundlage stattfinden lassen, wenn dadurch von gesetzlichen Aufgabenzuweisungen abgewichen wird. Im Sozialgesetzbuch Fünftes Buch ist vorgesehen, dass die Krankenkassen die zur Einschaltung medizinischen Sachverstandes in bestimmten Fällen erforderlichen gutachterlichen Stellungnahmen beim MDK einzuholen haben (§ 275 SGB V). Einem (privaten) Dritten darf also keine Aufgabe übertragen werden, für deren Erfüllung

nach dem Gesetz der MDK zuständig ist, die damit verbundene Datenübermittlung kann nicht wirksam auf die Einwilligung des Versicherten gestützt werden. Zumindest die Verfassungsgrundsätze des *Vorbehaltes des Gesetzes* und der *Gesetzmäßigkeit der Verwaltung* (Vorrang des Gesetzes) wären verletzt.

Die Krankenkasse konnte nicht überzeugend darlegen, dass die GmbH andere Aufgaben wahrnehmen sollte als der MDK wahrzunehmen hätte; im Gegenteil: Die Tätigkeit der GmbH sollte sich nicht darauf beschränken zu untersuchen, ob das jeweilige Hilfsmittel preisgünstiger zu erhalten wäre, sondern sie sollte gerade prüfen, ob statt des verordneten Hilfsmittels zunächst ein anderes, weniger teures Hilfsmittel hätte verordnet werden können. Für eine solche Erforderlichkeits-Prüfung ist jedoch gemäß § 275 Abs. 3 Nr. 2 SGB V der MDK zuständig. Folge also: Eine Datenübermittlung an Dritte zum Zweck der Erfüllung dieser Aufgabe darf auch nicht auf Einwilligungsgrundlage erfolgen.

Nachdem ich der Krankenkasse dies mitgeteilt hatte, schwenkte sie auf einen Vorschlag ein, den ich bereits zuvor unterbreitet hatte: die Pseudonymisierung der zu übermittelnden Daten. Die den Versicherten unmittelbar identifizierenden Daten auf den der GmbH zu übersendenden Unterlagen werden geschwärzt, an ihre Stelle tritt eine Nummer, über die der Versicherte nach der Überprüfung des Kostenvoranschlages von der Krankenversicherung wieder identifiziert werden kann.

Die Krankenkasse hat sich mit diesem Vorschlag zunächst nicht anfreunden können; sie meinte, die GmbH müsse Namen und Anschrift des Versicherten kennen, um ihn erforderlichenfalls befragen zu können. Schließlich hat sich die Krankenkasse dann doch mit meinem Vorschlag einverstanden erklärt und eingesehen, dass der Gutachter, wenn er Fragen hat, diese dem zuständigen Bearbeiter der Krankenkasse mitteilen kann, der dann seinerseits den Versicherten ansprechen kann. Die Krankenkasse wollte auf dieser Grundlage die zur Begutachtung erforderlichen medizinischen Daten dann aber unter einer Auftragsnummer übermitteln, die aus der laufenden Fallnummer und der betreffenden Jahreszahl, dem Geburtsdatum und der Krankenversicherungsnummer des Versicherten bestehen sollte. Auf meinen Einwand, dass die Versicherungsnummer nicht übermittelt werden dürfe, da anhand ihrer der Versicherte relativ leicht identifiziert werden könne, hat die Krankenkasse sich dann bereitgefunden, auf die Krankenversicherungsnummer als Bestandteil der Kennziffer zu verzichten.

Durch diese Verfahrensweise ist das Recht des Versicherten auf informationelle Selbstbestimmung gewährleistet.

10.2.4 Datenerhebung zur Feststellung des Bedarfes im Hinblick auf den Besuch von Kindertageseinrichtungen

Wie bekannt, sind in Sachsen einige örtliche Träger der öffentlichen Jugendhilfe - das sind gemäß § 69 Abs. 1 Satz 2 SGB VIII die Landkreise und kreisfreien Städte - zeitweise oder auf Dauer dazu übergegangen, die Zulassung zum Besuch von Kindergärten, sog. „Kinderkrippen“ (für die Unter-Dreijährigen) und (Schul-)Horten (für schulpflichtige Kinder - vgl. § 1 Abs. 1 bis 4 SächsKitaG, §§ 22 Abs. 1, 24 Satz 1 und 2 SGB VIII) oder die gesetzlich vorgesehene Übernahme von Zahlungspflichten zum Ausgleich für verminderte oder entfallende Elternbeiträge (§ 15 Abs. 4 Satz 1 und 2 SächsKitaG) ganz oder teilweise davon abhängig zu machen, dass Umstände vorliegen, welche die Eltern darauf angewiesen sein lassen, dass ihre Kinder durch diese ganz überwiegend von der öffentlichen Hand (Land, Gemeinde, Kreis und kreisfreie Stadt, vgl. §§ 13 ff. SächsKitaG) finanzierten Einrichtungen „einen Teil des Tages oder ganztags“ (§ 22 Abs. 1 SGB VIII) betreut werden.

Konkret wollen die betreffenden Landkreise bzw. Städte wissen, inwieweit die mit dem Kind in häuslicher Gemeinschaft lebenden Eltern („Personenberechtigten“) wegen Erwerbstätigkeit oder Ausbildung daran gehindert sind, sich selbst ganztägig um ihr Kind zu kümmern.

Diejenigen Beschlüsse - Stadtratsbeschlüsse oder Beschlüsse des Kreisjugendhilfeausschusses -, die mir vorgelegen haben, haben den Spielraum nicht überschritten, den der Bundesgesetzgeber dem örtlichen Träger der öffentlichen Jugendhilfe im Hinblick auf die Feststellung des *Bedarfes* wie auch im Hinblick auf die *Dauer* des Kindergartenbesuches einräumt, auf den gemäß § 3 Abs. 1 SächsKitaG, § 24 Satz 1 SGB VIII ein *Anspruch* besteht. Insbesondere weichen diese Beschlüsse nicht von den Entscheidungen des Bundesverfassungsgerichtes vom 28. Mai 1993, E 88, 203, 258 ff., 260 und des Bundesverwaltungsgerichtes vom 27. Januar 2000, E 110, 320, 325 ab.

Allerdings hat das VG Dresden in einem Beschluss vom 28. Januar 2003 - 6 K 344/03 (SächsVBl. 2003, 93) die Auffassung vertreten, das Sächsisches Kindertagesstättengesetz verbiete es dem örtlichen Träger der öffentlichen Jugendhilfe, bei der ihm gemäß § 80 Abs. 1 Nr. 2 SGB VIII, § 8 Abs. 1 Satz 1 bis 3 SächsKitaG obliegenden Aufgabe der Konkretisierung des *Bedarfes*, entsprechend dem gemäß § 24 Satz 2 SGB VIII, § 3 Abs. 2 SächsKitaG Kindertageseinrichtungsplätze anzubieten sind, darauf abzustellen, ob die Eltern (Personensorgeberechtigten) darauf angewiesen sind, wegen Berufstätigkeit oder Ausbildung das Kind fremdversorgen zu lassen (a. a. O. S. 94 rSp.). Das Gericht folgert dies daraus, dass das Sächsisches Kindertagesstättengesetz, anders als § 22 Abs. 1 und 2 SGB VIII, in § 2 Abs. 1 den Kindertageseinrichtungen einen gesteigerten, *eigenständigen* Betreuungs-, Bildungs- und Erziehungsauftrag, und zwar im Rahmen einer auf die Förderung der Persönlichkeit des

Kindes ausgerichteten *Gesamtkonzeption* (!), übertrage. Daraus wiederum leitet das Gericht ab, dass es nach sächsischem Recht *weder allein darum gehe, den Eltern die Betreuung des Kindes abzunehmen, wenn wegen einer Berufstätigkeit* [oder wegen Ausbildung] *das Kind fremdversorgt werden muss, noch darum gehe, bei besonderem Hilfebedarf die Eltern zu unterstützen. Der Auftrag beziehe sich gerade auf alle Kinder, unabhängig von ihren häuslichen Verhältnissen und eventuell vorliegenden erzieherischen Defiziten.*

Das Gericht sieht sich allerdings veranlasst, den örtlichen Trägern der öffentlichen Jugendhilfe zuzubilligen, dass sie die Zugangskriterien zur Feststellung des *Bedarfes* im Sinne des Sächsisches Kindertagesstättengesetzes so wählen, dass Kinder, welche die im Gesetz den Kindertagesstätten auferlegte *Persönlichkeitsförderung auch in der Familie durch die Personensorgeberechtigten erfahren können*, von der Aufnahme in eine Kinderkrippe oder einen Hort ausgeschlossen werden können (VG Dresden a. a. O.).

Man muss sich klarmachen, was der in dieser Gerichtsentscheidung eingenommene Rechtsstandpunkt für Folgen hätte: Da, wie das Gericht dem BVerwG (a. a. O.) folgend einräumt, der Bedarf nicht allein anhand der Nachfrage zu ermitteln ist, besagte das Sächsisches Kindertagesstättengesetz in dieser Auslegung, dass zur Feststellung des Vorliegens eines *Bedarfes* im Sinne des § 3 Abs. 2 SächsKitaG eine behördliche Feststellung darüber stattzufinden hätte, inwieweit Eltern, die nicht berufs- oder ausbildungsbedingt einen Teil des Tages ihr Kind nicht betreuen können, in der Lage sind, diejenige *Persönlichkeitsförderung* ihrem Kind angedeihen zu lassen, wie sie das Gesetz den Kindertagesstätten zur Aufgabe macht. Dies könnte sicherlich zuverlässig nur geschehen durch eine gründliche kinderpsychologische Untersuchung des Kindes wie der Eltern, die angesichts der hohen Entwicklungsgeschwindigkeit der kleinen Kinder auch in verhältnismäßig kurzen Abständen wiederholt werden müsste, da sich die Verhältnisse - in der einen oder anderen Richtung - verhältnismäßig schnell ändern können.

Man muss kein Datenschutzbeauftragter sein, um dies als Horror-Vorstellung zu erkennen: Nicht nur das Grundrecht auf informationelle Selbstbestimmung, auch, und in erster Linie, das den Eltern in Art. 6 Abs. 2 GG als Pflicht eingeräumte „natürliche Recht“, ihre Kinder zu pflegen und zu erziehen, wird verletzt. Die Vorstellung, dass „der Staat“ sich sogar verpflichtet sehen müsste, all die vielen Kinder, deren *Persönlichkeitsförderung* nach seiner Auffassung durch die Personensorgeberechtigten nicht optimal stattfinden kann, zwangsweise in Kindertageseinrichtungen zu „stecken“, ist dann unabweisbar.

In diesem Zusammenhang, nämlich unter dem Gesichtspunkt der Geeignetheit der Datenerhebung: Gibt es gesicherte Erkenntnisse über die persönlichkeitsfördernde Wirkung der realen Kindertageseinrichtungen und damit einen Vergleichsmaßstab?

Selbst wenn es solche verlässlichen Untersuchungen gäbe und sie feststellen würden, welch segensreiche Wirkung die Krippen, Gärten und Horte hätten: Der Staat darf nicht die Eltern ersetzen, er darf dies auch nicht „als freiwillige Einrichtung“ anbieten! Er hat vielmehr nur Rahmenbedingungen dafür zu setzen, dass die Eltern ihrer Pflege- und Erziehungspflicht nachkommen können und wollen. So will es Art. 6 Abs. 2 GG. Auch das SGB VIII verfolgt ja - in § 8 Abs. 1 Satz 1 und § 22 Abs. 1 - das Ziel, dass das Kind bzw. der Jugendliche in der Entwicklung zur Eigenverantwortlichkeit gefördert wird. Verantwortung lernt man - auch als Eltern - nur durch Verantwortung, nicht durch von ihr entlastende und damit bevormundende Betreuung und Versorgung, mag diese auch noch so gut gemeint und bequem sein. Ein Staat, der Betreuer und Vormund ist, entzieht der Demokratie die Grundlage.

Weniger problematisch liegt der Fall der Verkürzung der Zeit, für die der gemäß § 24 Satz 1 SGB VIII, § 3 Abs. 1 SächsKitaG bestehende *Anspruch* auf „Besuch eines Kindergartens“ besteht, den das VG Dresden nicht zu entscheiden gehabt hat: Die Dauer dieses „Besuches“ am Tag ist im Gesetz nicht definiert; aus § 24 Satz 3 SGB VIII ist vielmehr zu schließen, dass die Dauer dieses „Besuches“ nicht zwangsläufig durch eine *Ganztagsbetreuung* definiert ist, so dass einer Bemessung des zeitlichen Umfanges, auf den Anspruch besteht, im Sinne eines Angewiesenheits-Bedarfes kein grundsätzliches Hindernis entgegensteht.

Der von mir damit grundsätzlich eingenommene Rechtsstandpunkt bedeutet im Hinblick auf die Datenverarbeitung im einzelnen Folgendes:

Im Falle des unmittelbar von den Eltern beim örtlichen Träger der öffentlichen Jugendhilfe geltend zu machenden Antrages auf Übernahme des Elternbeitrages gemäß § 15 Abs. 4 Satz 2 SächsKitaG i. V. m. § 90 Abs. 3 und 4 SGB VIII i. V. m. §§ 76 bis 79 BSHG, also in Abhängigkeit vom Einkommen der Eltern, darf das Jugendamt unmittelbar - aber nicht durch die Träger der freien Jugendhilfe - die Daten erheben, aus denen hervorgeht, dass der in der genannten Weise konkretisierte *Bedarf* besteht. Und im Falle des Anspruches des Trägers der Kindertageseinrichtung, sei es nun ein freier Träger oder die Kommune - gegen den örtlichen Träger der öffentlichen Jugendhilfe gemäß § 15 Abs. 4 Satz 1 SächsKitaG auf Erstattung der gemäß § 15 Abs. 1 Satz 3 SächsKitaG vorgesehenen Absenkung des Elternbeitrages für Alleinerziehende und Geschwisterkinder kann der Träger der Kindertageseinrichtung - freier Träger wie kommunaler - seine Erstattungsansprüche nunmehr nur noch dann erfolgreich geltend machen, wenn er insoweit nachweist, dass die jetzt enger definierten Bedarfs-Voraussetzungen erfüllt sind, wozu er die in den mir bisher vorgelegten Fragebögen erhobenen Daten jeweils benötigt. Damit ist die nötige gesetzliche Grundlage für diesen Vorgang der Erhebung und Weiterverarbeitung personenbezogener Daten gegeben: § 67 a Abs. 1 Satz 1 SGB X erlaubt das Erheben von Sozialdaten durch Sozialleistungsträger (hier: Jugendamt des Landkreises oder der kreisfreien Stadt), wenn die Kenntnis dieser Daten zur Erfüllung einer Aufgabe der erhebenden Stelle - also

wiederum des Landratsamtes oder des Jugendamtes der kreisfreien Stadt - nach dem Sozialgesetzbuch erforderlich ist. Entsprechend erlaubt § 67 c Abs. 1 Satz 1 SGB X die Speicherung und Nutzung der betreffenden Daten für diesen Zweck. § 61 Abs. 1 Satz 1und 2 SGB VIII erklären diese Vorschriften des Zehnten Buches des Sozialgesetzbuch für auch im Bereich der Kinder- und Jugendhilfe anwendbar, aus §§ 62 bis 64 SGB VIII ergibt sich nichts Abweichendes.

Das Jugendamt benötigt, wie dargelegt, die Daten, um das Bestehen seiner Leistungspflicht prüfen zu können.

Insoweit Daten in dieser Weise von kreisangehörigen Gemeinden als Betreibern von Kindertagesstätten verarbeitet werden, gelten die genannten Vorschriften gemäß § 61 Abs. 1 Satz 3 SGB VIII *entsprechend*.

Freie Träger von Kindertageseinrichtungen dürfen die betreffenden Daten ebenfalls erheben und weiterverarbeiten (vgl. § 61 Abs. 4 SGB VIII).

Es ist ein ganz normaler Vorgang, dass Sozialleistungen nur gewährt werden, wenn dem Sozialleistungsträger die Daten vorliegen, aus denen hervorgeht, dass der Leistungsempfänger die im Gesetz vorgesehenen Leistungsvoraussetzungen erfüllt. Das Besondere ist hier nur, dass der Leistungsträger die Voraussetzungen enger als früher gefasst hat - eben meiner Auffassung nach im Rahmen des ihm im Gesetz eingeräumten Spielraumes. Das führt zu einem Datenbedarf, der so zuvor nicht bestanden hat, als man jede Nachfrage als *Bedarf* anerkannt hat.

Wovor wir auf jeden Fall bewahrt bleiben müssen, das ist die Datenerhebung, die „fällig“ - ich möchte nicht sagen: „statthaft“! - wäre, wenn das VG Dresden mit seinen zitierten Ausführungen Recht hätte. (Grundlegende Kritik hat die Entscheidung jetzt durch Scheffer, LKV 2003, 316, gefunden.)

10.2.5 Aufzeichnungen über Leistungen, die im Rahmen der sog. „Hilfe zur Erziehung“ nach SGB VIII erbracht werden

Soweit erforderlich, ist nach den §§ 27 ff. SGB VIII als Teil der Sozialleistung nach § 8 SGB I (Kinder- und Jugendhilfe) sog. *Hilfe zur Erziehung* zu leisten. Ambulant - man spricht hier von „aufsuchender Sozialarbeit“ - wird diese Hilfe insbesondere als sog. *sozialpädagogische Familienhilfe* (§ 31 SGB VIII) sowie in der Funktion als sog. *Erziehungsbeistand* (§ 30 SGB VIII) geleistet. Diese Tätigkeit wird weitgehend von freien Trägern durchgeführt (vgl. § 3 SGB VIII), finanziert von den Trägern der öffentlichen Jugendhilfe auf der Grundlage einer mit dem freien Träger abzuschließenden Vereinbarung (§ 77 SGB VIII). Solchen Vereinbarungen sind gemäß § 17 Abs. 5 SächsLaJuHiG leistungsgerechte Entgelte zugrunde zu legen, die den Trägern der freien Jugendhilfe - bei sparsamer und wirtschaftlicher Betriebsführung - die

erforderliche Hilfegewährung ermöglichen. Die Vereinbarungen haben den Grundsätzen der Wirtschaftlichkeit, Sparsamkeit und Leistungsfähigkeit zu entsprechen und sollen Art, Inhalt, Umfang und Qualität der zu erbringenden Leistungen beschreiben. Grundlage für die Ausgestaltung der Hilfe ist - jedenfalls bei einer voraussichtlich länger dauernden Hilfe - gemäß § 36 Abs. 2 SGB VIII ein sog. Hilfeplan.

Eine sächsische Großstadt war nun dazu übergegangen, sich von den freien Trägern Aufstellungen über die erbrachten Leistungen vorlegen zu lassen, in denen der Sozialarbeiter, der dabei tätig gewesen ist, bezogen auf 30-minütige Zeiteinheiten unter Nennung des Tages und der Uhrzeit eine Kurzbeschreibung seiner Aktivitäten gibt (Beispiel: „Begleitung zu einem Gespräch mit der Krankenkasse“) und diese Angaben durch den Hilfeempfänger durch Unterschrift bestätigt werden.
Diese sog. „Leistungsdokumentation für ambulante Hilfen“ ist dann dem sog. „Allgemeinen Sozialdienst“ (ASD) vorzulegen, der sie nach Prüfung der Daten an die sog. „Wirtschaftliche Jugendhilfe“ (WiJu) weitergibt. Die Erlaubtheit dieser Verfahrensweise ist Gegenstand mehrerer an mich gerichteter Anfragen gewesen. Die darin vorgebrachten Einwände und Zweifel haben sich als unbegründet erwiesen:

(1) Wenn man zunächst davon absieht, welche Stelle der betreffenden kreisfreien Stadt als örtlichen Träger der öffentlichen Jugendhilfe (vgl. § 85 Abs. 1 SGB VIII, § 1 Abs. 1 SächsLaJuHiG) im Einzelnen tätig wird, ergibt sich das aus Folgendem: Die Befugnis der zuständigen Stelle des betreffenden Trägers der öffentlichen Jugendhilfe, also des bei ihm eingerichteten Jugendamtes (vgl. § 69 Abs. 3 SGB VIII), die betreffenden Daten über den Hilfeempfänger (und auch über die tätig gewordenen Beschäftigten des freien Trägers und damit auch über diesen selbst) zu erheben, folgt aus § 62 SGB VIII, § 67 a SGB X (siehe auch § 61 Abs. 1 Satz 1 SGB VIII. Auf die Unterschiede im Wortlaut bzw. das genaue Verhältnis zwischen beiden Vorschriften kommt es hier nicht an). Danach ist das Erheben von (Sozial-) Daten zulässig, soweit ihre Kenntnis zur Erfüllung einer der Behörde durch Gesetz - hier SGB VIII - zugewiesenen Aufgabe erforderlich ist.

Die Aufgabe, um deren Erfüllung es hier geht, ist die Prüfung der Wirtschaftlichkeit und Qualität der durch den Träger der freien Jugendhilfe in dem betreffenden Fall erbrachten Leistungen. Zwar werden Leistungen der Jugendhilfe von Trägern der freien Jugendhilfe genauso wie von Trägern der öffentlichen Jugendhilfe wahrgenommen, § 3 Abs. 2 Satz 1 SGB VIII, § 17 Abs. 1 Satz 1 SächsLaJuHiG. Das bedeutet aber nicht, dass der Träger der öffentlichen Jugendhilfe damit von seiner Aufgabe befreit wäre. Er bleibt vielmehr dem Hilfeempfänger gegenüber für die ordnungsgemäße Gewährung von Sozialleistungen verantwortlich (Schellhorn, Rdnr. 13 zu § 3 SGB VIII). Nur ihn trifft ja die gesetzliche Leistungspflicht (§ 3 Abs. 2 Satz 2 SGB VIII, § 17 Abs. 1 Satz 2 SächsLaJuHiG). Im Bereich der Hilfen zur Erziehung hat daher das Jugendamt unter anderem die Gesamtsteuerung und -planung, den Abschluss der Leistungs-, Entgelt- und Qualitätsentwicklungsvereinbarungen sowie die Finan-

zierung der Leistungsangebote zu gewährleisten. Um dieser Verantwortung gerecht werden zu können, muss der Träger der öffentlichen Jugendhilfe die durch den Träger der freien Jugendhilfe erbrachten Leistungen - gerade auch zum Schutz des jeweiligen Hilfeempfängers - überprüfen können. (vgl. zu einer ähnlichen Fragestellung schon 9/10.2.8)

Selbstverständlich muss die Datenerhebung auf den erforderlichen Umfang beschränkt bleiben. Die in der mir vorgelegten „Leistungsdokumentation“ abgefragten Daten überschreiten nach meiner Einschätzung das erforderliche Maß nicht: Ohne diese Angaben könnte der verantwortliche Sozialleistungsträger nicht wirklich überprüfen, ob im Einzelfall eine Beratung durchgeführt worden ist, die dem ausgearbeiteten Hilfeplan entspricht und für welche eine entsprechende Bezahlung an den Träger der freien Jugendhilfe zu erfolgen hat. Wenn der Träger der öffentlichen Jugendhilfe selbst die Erziehungshilfe durchführte, müssten, um eine interne Aufsicht zu ermöglichen, mindestens dieselben Angaben dokumentiert werden. Die insoweit erhobenen Daten umfassen lediglich chronologische Daten wie den jeweiligen Arbeitsstand, jedoch keine näheren Angaben über den Inhalt der Beratung zwischen Leistungsempfänger und Leistungserbringer. Der Fragebogen ist auch nicht so gestaltet, dass er es nahelegte, unnötig konkrete Angaben zu machen.

(2) Was die Aufteilung der Bearbeitung der vorgelegten Unterlagen auf den ASD, und nach Weiterleitung auf die WiJu betrifft, handelt es sich um Folgendes: Zunächst überprüft der ASD mittels der Leistungsdokumentation, ob die im Hilfeplan festgelegten Ziele noch richtig sind, und er überprüft ferner die sachliche Richtigkeit der Abrechnung des freien Trägers unter dem Gesichtspunkt, ob die erbrachten Leistungen den Aufgaben entsprechen, die in dem dem freien Träger erteilten Auftrag mit diesem vereinbart worden sind. Danach wird der Vorgang an die WiJu weitergegeben und von dieser daraufhin überprüft, inwieweit die dokumentierten Leistungen den geltenden Leistungs- und Entgeltvereinbarungen entsprechen - was noch zur sachlichen Richtigkeit gehört -, sowie auf die rechnerische Richtigkeit. Die WiJu hat auch die Zahlungen zu veranlassen.

Es besteht insoweit eine Art Arbeitsteilung zwischen der ausschließlich zum Jugendamt gehörenden „wirtschaftlichen Jugendhilfe“ und dem ASD bei der Erledigung der Aufgaben nach dem SGB VIII.

Diese Arbeitsteilung ist datenschutzrechtlich unbedenklich: Als Träger der öffentlichen Jugendhilfe hat die betreffende Stadt die in § 2 SGB VIII genannten Aufgaben wahrzunehmen. Hierfür hat sie aufgrund der ihr kraft des kommunalen Selbstverwaltungsrechtes zustehenden Organisationshoheit einen „Allgemeinen Sozialdienst“ für die Erfüllung bestimmter Aufgaben nach dem SGB VIII eingerichtet. Das ist zulässig: § 69 Abs. 3 SGB VIII ist dahingehend auszulegen, dass durch die bundesgesetzliche Vorgabe, für die Erfüllung der Aufgaben nach dem SGB VIII

ein Jugendamt einzurichten, nicht ausgeschlossen werden soll, dass einzelne „Sonderdienste“ für die Erfüllung bestimmter Aufgaben aus dem Bereich des SGB VIII eingesetzt werden (Schellhorn, Rdnrn. 15 ff. zu § 69, Rdnr. 3 zu § 70 SGB VIII). Die Organisationseinheit ASD bildet somit für den Bereich der Erledigung der Aufgaben nach dem SGB VIII eine funktionale Einheit mit der als „Jugendamt“ bezeichneten Organisationseinheit, wobei deren Verwaltungsspitze die uneingeschränkte Aufsicht („mit allen Entscheidungs- und Durchgriffsrechten im Handlungsalltag“) hinsichtlich aller nach dem SGB VIII wahrzunehmenden Aufgaben gegenüber dem ASD obliegt - und auch zustehen muss (Münder u. a., Frankfurter Kommentar zum SGB VIII, § 69 Rdnr. 11, übereinstimmend Wiesner/Mörsberger Rdnr. 38 zu § 66 SGB VIII, jeweils m.w.N.). Damit ist „das Jugendamt“ und „der ASD“ insoweit als *eine* Behörde (Leistungsträger) im Sinne von § 35 Abs. 1, § 12 SGB I anzusehen, also als *eine* Stelle (im funktionellen Sinne) der Datenschutzvorschriften der §§ 67 f. SGB X (vgl. § 61 Abs. 1 Satz 1 SGB VIII). Die Weitergabe vom ASD an die WiJu ist somit im Rechtssinne keine Übermittlung, sie braucht also die für deren Zulässigkeit geltenden Voraussetzungen nicht zu erfüllen. Abgesehen davon wäre die Weitergabe auch als Übermittlung nach § 64 Abs. 1 SGB VIII, § 69 Abs. 1 Nr. 1, 1. Fall SGB X offensichtlich zulässig, weil Erhebungs- und Weiterverwendungszweck identisch sind.

Beide beteiligten Stellen, ASD und WiJu, *nutzen* die in den ihnen vorliegenden Unterlagen enthaltenen Daten in rechtmäßiger, den Anforderungen der § 64 Abs. 1 SGB VIII, § 67 c Abs. 1 Satz 1 SGB X entsprechenden Weise, insbesondere auch zur Überprüfung der an das Jugendamt gerichteten Zahlungsverlangen. Allerdings ist gemäß § 35 Abs. 1 Satz 2 SGB I (Sozialgeheimnis) sicherzustellen, dass auch innerhalb der Behörde bzw. der beiden Organisationseinheiten die Daten nur Befugten zugänglich gemacht werden bzw. nur an Befugte weitergeleitet werden (vgl. schon 6/10.2.1, S. 135). Befugt in diesem Sinne sind nur diejenigen Beschäftigten, die die Daten benötigen, um die ihnen übertragenen Aufgaben wahrzunehmen. Es ist jedoch insoweit kein Fehler in der Organisation des Ablaufes zu erkennen: Die Leistungsdokumentation geht nach Prüfung durch die WiJu zurück an den ASD, die vom freien Träger gestellte Rechnung verbleibt bei der WiJu.

10.2.6 Verdeckter zusätzlicher Personenbezug in Jugendhilfe-Akten

Wenn Geschiedene um das Sorgerecht oder das Recht auf Umgang mit den Kindern untereinander streiten, hat vielfach die eine oder die andere Seite den Eindruck, das Jugendamt, das berät (§§ 17 f SGB VIII), in gerichtlichen Verfahren mitwirkt (§ 50 SGB VIII) oder in Unterhaltsangelegenheiten tätig wird (§§ 52 a f. SGB VIII), sei parteiisch und handle rechtswidrig. Manchmal soll ich dann die Verarbeitung personenbezogener Daten durch das Jugendamt prüfen, vor allem aber bei Auseinandersetzungen über Akteneinsichtsansprüche „entscheiden“.

Auskunftsansprüche lassen sich dabei auf § 83 SGB X, den dem § 17 SächsDSG entsprechenden datenschutzrechtlichen Auskunftsanspruch im SGB-Bereich, wohl weniger jedoch auf den im Verwaltungsverfahren bestehenden besonderen Anspruch des § 25 Abs. 3 SGB X, § 29 VwVfG, stützen. Dabei ist der *verdeckte zusätzliche Personenbezug* zu beachten, der das Datum zum *latent-eigenen Datum* eines im gespeicherten Kontext nicht ausdrücklich genannten Dritten machen kann, wie ich (10/5.8.3) bereits an Hand eines Beispiels aus dem Archiv- bzw. Baurecht dargelegt habe.

Aufgrund der engen rechtlichen und tatsächlichen, jedenfalls rechtlich relevanten Beziehungen zwischen den Beteiligten reicht der verdeckte (zusätzliche) Personenbezug sehr weit. Beispiel: Das Jugendamt stellt selbst fest oder lässt sich vom Elternteil 1 oder von Dritten etwas sagen über das Verhältnis zwischen dem Elternteil 1 und dem Kind. Hat der Elternteil 2 im Hinblick auf diese Information einen Auskunftsanspruch, weil es sich um ein auch auf seine Person bezogenes Datum handelt?

Nach meiner Auffassung ist die Frage positiv zu beantworten: Angaben über das Verhältnis zwischen einem Kind und einem Elternteil haben jeweils einen für den datenschutzrechtlichen Auskunftsanspruch des Betroffenen relevanten impliziten (verdeckten, latenten) Zusatz-Bezug auf den anderen Elternteil. Denn die Beziehung zwischen dem einzelnen Elternteil und dem Kind betreffen mittelbar auch den anderen Elternteil (wohingegen man wohl nicht sagen kann, das die Beziehung zwischen den Eltern in jeder Hinsicht auch das Kind betreffen). Ganz offenkundig ist dies zum Beispiel etwa bei dem Datum, das Kind habe erklärt, das es bei der Mutter bleiben möchte: Diese Angabe bezieht sich auch auf den Vater.

Dieser Zusatz-Bezug erstreckt sich auch auf die Person eines Dritten (Außenstehenden) Hinweisgebers, der etwas über das Verhältnis zwischen dem Kind und dem anderen Elternteil angegeben hat. Den verdeckten Zusatz-Bezug haben ferner auch diejenigen Angaben, die ein Elternteil oder aber ein Kind jeweils ausschließlich über sich selbst macht, soweit diese Aussagen im Hinblick darauf wiedergegeben oder aufgezeichnet werden, dass sich daraus Erkenntnisse für das Dreierverhältnis Mutter-Vater-Kind bzw. darüber gewinnen lassen, welche Beziehungen zu welchem Elternteil für das Kindeswohl günstig oder ungünstig sind. Sinnfällig wird das an den psychologischen Gutachten, die in diesen Fällen üblicherweise oft auch Bestandteil der Gerichtsakte und damit ohnehin - aus gutem Grund - den Parteien zugänglich sind.

Für den Auskunftsanspruch-Ausschlussgrund gemäß § 17 Abs. 5 Satz 1 SächsDSG, § 83 Abs. 4 SGB X folgt aus der Unteilbarkeit des Dreierverhältnisses, dass dann, wenn ein Elternteil gegenüber der Behörde Angaben über das Verhältnis zwischen dem anderen Elternteil und dem Kind macht, der Elternteil, welcher diesen Hinweis gegeben hat, in keinem Falle als Hinweisgeber geschützt wird. Der Grund ist, dass die Tatsache, dass der andere Elternteil sich über das Verhältnis des Kindes zu dem betroffenen Elternteil geäußert hat, ein Faktum ist, mit dem jener andere Elternteil sich

im Hinblick auf das Dreierverhältnis selbst dargestellt und zugleich auch auf dieses Dreierverhältnis eingewirkt hat. Die Tatsache der Hinweisgebung ist in diesem Fall Gestaltung des Dreierverhältnisses, auf das sich zugleich die im Hinweis enthaltene Angabe bezieht. Solches gilt jedoch nicht mehr in dem Fall, dass die Großeltern der Kinder oder dass Nachbarn Hinweisgeber sind. (Noch größer ist der Unterschied zu Fällen, in denen der Hinweisgeber etwa durch ein Arbeitsverhältnis mit dem Betroffenen verbunden ist und zum Beispiel der Arbeitnehmer durch einen Hinweis eine Kontrolle der Behörde in dem Betrieb ausgelöst hat, vgl. oben Abschnitt 10.1. n.)

Die Grenze, die Simitis/Dammann in Rdnr. 42 zu § 3 BDSG unter Berufung auf andere Stimmen in der Literatur zu ziehen versucht, überzeugt demgegenüber nicht: Aus der mangelnden gesetzlichen Regelung der Daten-Verfügungsgewalt (Löschung, Berichtigung) über Daten mit Doppelbezug meint Dammann den Grundsatz folgern zu können, dass Betroffener nur derjenige sei, auf dessen Verhältnisse sich die Daten *unmittelbar* beziehen - Personen, über die sich nur mittelbar, durch Rückschluss, etwas ergebe, weil sie mit der ersten Person in einer bestimmten Beziehung stehen, seien hingegen nicht Betroffene. Das habe zur Folge, dass Verhältnisse eines Angehörigen (!), wie etwa die Religionszugehörigkeit oder eigene Einkünfte, die steuerlich oder sozialrechtlich für Rechte und Pflichten der ersten Person maßgeblich sind, dadurch noch nicht zu (auch-)eigenen Verhältnissen würden. Das leuchtet vom praktischen Ergebnis her schon deswegen nicht ein, weil in solchen Fällen der mittelbar Betroffene notwendig davon erfährt, ja sogar sich darüber unterrichten und dann gegenüber der Behörde Angaben machen muss, wie die Verhältnisse, die unmittelbar - primär - nur solche des Angehörigen sind, tatsächlich sind: Im Zusammenhang der Bearbeitung seiner steuerlichen oder sozialrechtlichen Angelegenheiten sind diese primär fremden Verhältnisse sekundär - abgeleitet - auch seine eigenen.

Aber auch rechtsdogmatisch läßt sich die Überlegung widerlegen: Aus der Tatsache der mangelnden Allein-Verfügungsbefugnis des ‚Dritten' zur Datenveränderung - gegen Dammann - darf nicht gefolgert werden, dass er auch keine nicht-datenverändernde Mit-Verfügungsbefugnis habe. Löschungs- und Berichtigungsansprüche können in der Tat notwendig nur exklusiv zugebilligt werden, müssen also wohl gemeinschaftlich (gesamthänderisch) ausgeübt werden. Auskunftsansprüche hingegen sind mit konkurrierenden Auskunfts-Ansprüchen (anders als mit Geheimhaltungs-Ansprüchen) ohne weiteres kompatibel, die Rechtsordnung kann sie zur kumulativen Ausübung zubilligen.

10.2.7 Wohngeld: Verdächtiger Verzicht auf Fortsetzung der Sozialleistungen?

Wie ich durch einen Zeitungsartikel erfahren habe, hatte ein Wohngeldempfänger der Wohngeldstelle des Sozialamtes einer Sächsischen Großstadt - wie dies seine Pflicht war

(§ 29 Abs. 4 Satz 1 WoGG, vgl. auch § 60 Abs. 1 Satz 1 Nr. 2 SGB I) - seine bevorstehende Arbeitsaufnahme, also den Beginn eines versicherungspflichtigen Beschäftigungsverhältnisses, mitgeteilt und gebeten, die Zahlung des Wohngeldes einzustellen, da er mit seinem Einkommen dann „über der Bezugsgrenze liege“, also nicht mehr berechtigt sei, Wohngeld in Anspruch zu nehmen. Die Wohngeldstelle hatte daraufhin aber nicht einfach die Zahlungen eingestellt und die Akte geschlossen, sondern sie hatte vielmehr nun den Wohngeldempfänger aufgefordert, Verdienstbescheinigungen und ähnliche Einkommensnachweise für die Vergangenheit vorzulegen. Begründung des Amtes der Presse gegenüber: Jede Änderung, die Einfluss auf das Wohngeld habe, müsse angezeigt werden, „das betrifft natürlich auch den Fall, wenn am Ende der Wohngeldanspruch bei Null liegt. Es gilt einfach, den Verwaltungsakt abzuschließen“. Und: Es müsse doch geprüft werden, ob der Wohngeldempfänger nicht schon früher als angegeben ein gegenüber den bei Antragstellung gemachten Angaben erhöhtes Einkommen erzielt und damit zu Unrecht Wohngeld erhalten habe.

Ein Fall für die Presse geworden war die Angelegenheit dadurch, dass die Behörde dem ehemaligen Wohngeldbezieher ein Bußgeld auferlegt hatte, als der sich geweigert hatte Unterlagen für die Zeit vor dem von ihm angegebenen Beginn seines neuen Arbeitsverhältnisses beizubringen (vgl. § 43 Abs.1 Nr. 2 WoGG), und die Weigerung im anschließenden Ordnungswidrigkeiten-Verfahren erst beim Oberlandesgericht Dresden erfolgreich gewesen war, allerdings ohne dass das die Wohngeldstelle von weiteren Erhebungsbestrebungen abgehalten hätte.

Die Stellungnahme, die die Behörde dann mir gegenüber abgegeben hat, war erst recht verwirrend. Der eigentliche Kern des Problems konnte erst herausgearbeitet werden, nachdem schon das SMI sehr schnell auf den Vorfall reagiert, meinen rechtlichen Bedenken im Ergebnis zugestimmt, sowie das Sozialamt daraufhin mir gegenüber eingelenkt und erklärt hatte, von einer weiteren Datenerhebung in diesem Fall abzusehen.

Das Sozialamt hat sich nämlich dann darauf berufen, dass nach seinen Erfahrungen in neun von zehn Fällen der teilweise oder vollständige Wegfall der Voraussetzungen für den Bezug von Wohngeld schon rund drei bis vier Monate zurückliege, wenn die Leistungsbezieher das melden oder nach Auslaufen des Bewilligungszeitraumes keinen (neuen) Antrag auf Fortsetzung der Wohngeldleistung stellten. Das gehe aus den Unterlagen hervor, die zur Begründung von Folge-Anträgen auf Wohngeld eingereicht würden, die dann später in einigem Abstand vom Ende des vorhergehenden Leistungsbezugs- und Leistungsbewilligungs-Zeitraum gestellt würden. Dann zeigten diese Unterlagen, namentlich die Nachweise des Jahreseinkommens, aber auch die Mietverträge oder die Angaben über die Haushaltsgröße (Personenanzahl), dass die Verhältnisse sich seiner Zeit schon vor der Änderungsmitteilung bzw. vor dem Auslaufen der Wohngeldleistung geändert haben müssen.

Daraus nun hatte die Behörde in dem vorliegendem Fall gefolgert, Ermittlungen für die dem Verzicht vorausgegangene Zeit seien geboten. (Und in dieser Auffassung, dass heißt in ihrem Verdacht, hatte sie sich vermutlich durch die Weigerung des Betroffenen bestätigt gesehen, während dieser sich möglicherweise in seinem Stolz verletzt gefühlt hatte.)

Die Auffassung der Behörde war falsch, und sie hatte es auch eingesehen und ihre Praxis generell insoweit geändert.

Folgende Erwägung hat dabei meines Erachtens maßgeblich zu sein: Sozialleistungen sind nur im Falle tatsächlicher Bedürftigkeit zu erbringen. Wer jedoch auf die (fortgesetzte) Zahlung von Sozialleistungen verzichtet, muss hierfür nicht noch Unterlagen vorlegen. Es bedarf keines Nachweises dafür, dass man nichts mehr „vom Staat“ möchte. Insofern hatte die Behörde jedoch schon Zweifel, und zwar deswegen, weil ein Verzicht im WoGG gar nicht erwähnt wird und sie sich durch die Verzichts-Vorschrift des SGB I gehalten sah, gerade möglichem früherem unberechtigtem Leistungsbezug, der im Zusammenhang mit einem Verzicht steht, nachzugehen. § 46 Abs. 2 SGB I bestimmt nämlich, dass ein Verzicht unwirksam ist, soweit durch ihn Rechtsvorschriften umgangen werden. Diese Vorschrift soll jedoch ausschließlich dafür sorgen, dass durch einen Verzicht nicht die Rangfolge im System der sozialen Sicherung, unter Einbeziehung der familiären Unterhaltspflichten, verletzt wird - mehr nicht. Außerdem gibt es, entgegen der Auffassung der Behörde, keinen Grund, denjenigen, der auf Sozialleistungen verzichtet, zwangsweise dadurch zu beglücken, das man sich seine Unterlagen geben lässt, um zu prüfen, ob er nicht doch noch leistungsberechtigt ist.

Zum Anderen darf das Sozialamt seine Ermittlungen wegen des Verdachtes auf unberechtigten Leistungsbezug nicht unterschiedslos auf alle Fälle des Endes des Leistungsbezuges ausdehnen, insbesondere auch nicht auf die der Beendigung durch Mitteilung des Wegfalles der Voraussetzungen. Denn der von der Behörde angeführte Erfahrungs-Satz trifft nur auf diejenigen zu, die in einem so dichten Abstand zum vorhergehenden Leistungszeitraum einen neuen Antrag stellen, dass die für den Folgeantrag vorgelegten Unterlagen Aussagen über den vorhergehenden Leistungszeitraum erlauben. Das aber war in diesem Fall ja noch gar nicht geschehen. Dass demgegenüber allein aus der Tatsache, dass auf die Fortzahlung des Wohngeldes bis zum Ende des Leistungsbewilligungszeitraumes verzichtet wird, schon ein Verdacht abzuleiten ist, dass also deswegen die Angaben des ehemaligen Leistungsbeziehers in Zweifel zu ziehen sind, ist durch nichts zu begründen.

Aber auch sonst bestand, soweit ersichtlich, für die Wohngeldbehörde kein konkreter Anlass zu der Vermutung, der Wohngeldempfänger sei seiner Zeit bei der Beantragung und Bewilligung von Wohngeld seiner Verpflichtung, wahrheitsgemäße Angaben zu machen, nicht nachgekommen. Die dennoch hierzu durchgeführte Ermittlungstätig-

keit - und damit Datenerhebung - der Behörde war somit nicht erforderlich im Sinne von § 67 a Abs. 1 Satz 1 SGB X, § 60 Abs. 1 Satz 1 SGB I und damit rechtswidrig. Denn: Die Befugnis des Sozialleistungsträgers, im Rahmen des ihm nach § 20 Abs. 1 und 2 SGB X („Untersuchungsgrundsatz“) eingeräumten Ermessens über das Ausmaß der Ermittlungen zu entscheiden, bedeutet nicht, dass die Behörde auf der Grundlage eines nicht näher begründeten pauschalen allgemeinen Verdachtes grundsätzlich davon ausgehen darf, die vom Leistungsempfänger abgegebenen Erklärungen über seine Einkommens- und Vermögensverhältnisse seien mit einiger Wahrscheinlichkeit unwahr. Der Umfang der Ermittlungspflicht ist nicht in das Belieben der Behörde gestellt. Die Aufklärungspflicht beschränkt sich insoweit auf die Behebung eigener, auf Grund konkreter Anhaltspunkte sich nahelegender Zweifel. Der Untersuchungsgrundsatz bedeutet nicht, dass jede Behauptung bezweifelt werden muss und erst dann der Entscheidung zu Grunde liegen darf, wenn sie bewiesen ist. (Vgl. dazu Hess. VGH Entsch. vom 7. Februar 1995 - 9 TG 3113/94, RDV 1995, 175, unter Verweis auf Formulierungen der amtlichen Gesetzesbegründung; zu einer ganz ähnlichen Fragestellung habe ich mich schon in 10/10.2.4 geäußert.)

10.2.8 Ein Tiger ohne Zähne - oder: Das Dilemma fehlender Befugnisse

Auf Anregung des Bundesbeauftragten für den Datenschutz beschäftigte sich der Arbeitskreis „Gesundheit und Soziales“ der Datenschutzbeauftragten des Bundes und der Länder in seiner 37. Sitzung im Februar 2002 mit der Thematik: „Abrechnung/ Kostenerstattung der Länder an die gesetzlichen Krankenkassen bei der Durchführung des Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen“. In § 4 des Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen vom 21. August 1995 (BGBl. I S. 1050, zuletzt geändert durch Artikel 8 des Gesetzes vom 15. Dezember 2001 (BGBl. I S. 3762) ist geregelt, dass die Länder den gesetzlichen Krankenkassen die ihnen durch dieses Gesetz entstehenden Kosten erstatten. Das Nähere einschließlich des haushaltstechnischen Verfahrens und der Behördenzuständigkeit regeln die Länder. Die Erörterung im Arbeitskreis sollte dazu beitragen, ein möglichst einheitliches, datenschutzgerechtes Kostenerstattungsverfahren auf Länderebene herbeizuführen. Insbesondere sollten *keine Vornamen, Familiennamen und Anschriften* betroffener Frauen übermittelt werden.

Im Anschluss an die Sitzung des Arbeitskreises wandte ich mich an das SMS mit der Frage, wie das Kostenerstattungsverfahren nach § 4 des Gesetzes zur Hilfe für Frauen bei Schwangerschaftsabbrüchen in besonderen Fällen in Sachsen geregelt sei, insbesondere im Hinblick auf die damit verbundenen Datenverarbeitungsvorgänge. Es bedurfte der nochmaligen Erinnerung, ehe mir das SMS vier Monate später einen Abdruck seines Schreibens „in gleicher Angelegenheit“ an das BMFSFJ übersandte. In diesem Schreiben führte das SMS aus, dass „seitens der Krankenkassen, der Krankenhäuser bzw. durch die Kassenärztliche Vereinigung Sachsen übermittelt werden:

Familienname, Vorname, Geburtsdatum und Anschrift“ - offen blieb, an wen diese Daten seitens der genannten Stellen übermittelt werden. Die weiteren Ausführungen in dem an das Bundesministerium gerichteten Schreiben ließen vermuten, dass der genannte Datensatz der „Erstattungsbehörde“ übermittelt wird. Nur: Welche Stelle des Freistaates Sachsen ist diese „Erstattungsbehörde“? Und: Benötigt sie den übermittelten Datensatz nur, wie das Staatsministerium schrieb, „für die Erfüllung der Aufsichts- und Kontrollaufgaben“ oder auch für die Kostenerstattung selbst? Weiter teilte das Staatsministerium dem Bundesministerium mit, dass es sich mit den Krankenkassen auf eine Abkürzung des Erstattungsweges geeinigt hätte: „Die Unterlagen“ würden nunmehr dem Sächsischen Landesamt für Familie und Soziales vorgelegt. Auch diese Ausführungen erhellen jedoch nicht, *wer wem welche personenbezogenen Daten übermittelt*.

Ich habe das SMS gebeten, zu diesen Fragen Stellung zu nehmen. Inzwischen habe ich es zweimal an die Beantwortung meines Schreibens erinnert und mit Nachdruck um die Beantwortung der in meinem Schreiben aufgeworfenen Fragen gebeten. Die Stellungnahme steht immer noch aus, obwohl dem Staatsministerium bekannt sein dürfte, dass es gemäß § 25 SächsDSG dazu verpflichtet ist, mich bei der Erfüllung meiner Aufgaben zu unterstützen, mir insbesondere Auskunft zu meinen Fragen zu erteilen.

An diesem Fall wird ein Mangel des Sächsischen Datenschutzgesetzes sichtbar: Es normiert zwar eine Unterstützungspflicht öffentlicher Stellen, jedoch keine Befugnis, die Erfüllung dieser Pflicht auch durchzusetzen.

Demgegenüber hat der Europäische Gesetzgeber erkannt, dass eine „Kontrollstelle für den Schutz von Personen bei der Verarbeitung personenbezogener Daten“ nur dann erfolgreich arbeiten kann, wenn nicht nur negativ einer anderen Stelle Pflichten auferlegt werden, sondern positiv der Kontrollstelle Rechte und Befugnisse zu deren Durchsetzung übertragen werden. Entsprechend regelt Art. 28 Abs. 3 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 (ABl. Nr. L281 Seite 31), dass jede Kontrollstelle nicht nur über „Untersuchungsbefugnisse“ (erster Spiegelstrich), sondern auch über „wirksame Einwirkungsbefugnisse“, wie beispielsweise die Möglichkeit, das Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Datenverarbeitung Verantwortlichen zu richten (zweiter Spiegelstrich), und ein „Klagerecht“ (dritter Spiegelstrich) verfügt.

Eine diesen Regelungen vergleichbare Vorschrift findet sich im Entwurf des neuen Sächsischen Datenschutzgesetzes, das ja auch die Richtlinie umsetzen will, nicht wieder, womit Sachsen aber in Deutschland alles andere als allein steht.

Mir bleibt daher nichts weiter, als das SMS nochmals zur Beantwortung meiner Fragen aufzufordern und zu hoffen, dass ich eine Antwort erhalte, die den Sachverhalt so

darlegt, dass ich ihn rechtlich bewerten und die Rechtmäßigkeit der Datenverarbeitung prüfen kann. Davon abgesehen: Die Zusammenarbeit mit dem SMS ist grundsätzlich gut. Möglicherweise ist der Fall in den Mühlwerken der Verwaltung untergegangen. Ich denke, das lässt sich reparieren.

10.2.9 Datenabgleich der BAföG-Ämter mit dem Bundesamt für Finanzen

Nur arme Studenten, solche, die auch keinen ausreichenden Unterhaltsanspruch haben, erhalten finanzielle Unterstützung nach dem BAföG. Die Angaben der Studenten zu ihrer Finanzsituation sind aber leider oft falsch. Wie kann man die Angaben kontrollieren? Die BAföG-Ämter sind, wie nachträglich bekanntgeworden ist, bundesweit dazu übergegangen, zur Überprüfung der von Antragstellern und Leistungsbeziehern gemachten Angaben über Einkünfte und anrechenbares Vermögen einen einhundertprozentigen Datenabgleich mit dem BfF durchzuführen: Die BAföG-Ämter übermitteln, und zwar in Sachsen mithilfe des Statistischen Landesamtes als Auftrags-Datenverarbeiters, die Namen und andere unmittelbar identifizierende Daten derjenigen Personen, die Leistungen nach dem BAföG beantragen bzw. erhalten, an das BfF, dieses gleicht die Angaben mit den bei ihm vorhandenen Daten über die Höhe der gemäß Freistellungsauftrag tatsächlich in Anspruch genommenen Freistellung von der Zinsabschlagsteuer ab und unterrichtet in den Treffer-Fällen über den Betrag. In Sachsen wertet das Statistische Landesamt die Rückmeldungen aus und fertigt Aktenvermerke, anhand deren die BAföG-Ämter abklären, ob die vom BfF mitgeteilten Zinseinkünfte dem vom Antragsteller angegebenen Vermögen entsprechen oder eine Abweichung zu vermuten ist. Sollte letzteres der Fall sein, so wird zum Zweck der Sachaufklärung Kontakt mit dem Betreffenden aufgenommen.

Daran sind zwei relevante Datenverarbeitungsvorgänge zu unterscheiden: Zum einen die Datenübermittlung durch das BAföG-Amt an das BfF und zum anderen die Datenübermittlung durch das BfF an das BAföG-Amt. (Die Einschaltung des Statistischen Landesamtes als Auftragsdatenverarbeiters kann dabei vernachlässigt werden.) Rechtsgrundlage der Letzteren ist die Vorschrift des § 45 d EStG. Seinem Wortlaut nach erlaubt § 45 d Abs. 3 EStG dem BfF, die ihm von dem Sozialleistungsträger übermittelten Daten mit den vorhanden Daten nach Abs. 1 im Wege des automatisierten Datenabgleichs zu überprüfen und das Ergebnis dem Sozialleistungsträger mitzuteilen. Zu ersterem, nämlich für die Datenübermittlung des BAföG-Amtes an das BfF fehlt es jedoch an einer solchen gesetzlichen Erlaubnisnorm: Weder umfaßt § 45 d Abs. 3 EStG auch diese Übermittlung, noch findet sich in der übrigen Rechtsordnung eine entsprechende Erlaubnisnorm.

Die von den BAföG-Ämtern zu übermittelnden Daten unterliegen als Sozialdaten (§§ 11, 18 Abs. 1 SGB I) den Regelungen des Sozialgesetzbuchs und unterfallen dem in § 35 Abs. 1 SGB I normierten Sozialgeheimnis. Gemäß § 35 Abs. 2 SGB I ist eine

Erhebung, Verarbeitung und Nutzung von Sozialdaten nur unter den Voraussetzungen des zweiten Kapitels des SGB X zulässig. Dort wiederum bestimmt § 67 d Abs. 1 SGB X, dass eine Übermittlung von Sozialdaten nur zulässig ist, soweit eine gesetzliche Übermittlungsbefugnis nach den § 68 bis 77 oder „nach einer anderen Rechtsvorschrift in diesem Gesetzbuch“ vorliegt.

Eine Übermittlungsbefugnis der BAföG-Ämter ergibt sich insbesondere nicht aus der (allein in Frage kommenden) Vorschrift des § 69 Abs. 1 Nr. 1 SGB X. Zwar dient die Übermittlung der Daten der Erfüllung der Zwecke, für die sie erhoben worden sind, denn zu den Aufgaben des Leistungsträgers gehört nicht nur die Ermittlung von Daten zur Feststellung der Leistungsvoraussetzungen, sondern auch die Überwachung der Berechtigung zum Bezug der Leistungen (vgl. Hauck/Haines, SGB X, § 69 Rdnr. 19). Allerdings ist eine Übermittlung von Sozialdaten *nur* zulässig, wenn sie zur Aufgabenerfüllung *erforderlich* ist - und zwar *in jedem einzelnen Fall*. Es müssten also in jedem einzelnen Fall Anhaltspunkte dafür vorliegen, dass der Auszubildende unwahre Angaben über sein Vermögen gemacht hat. Bezogen auf die Datenerhebung bei einem Antrag auf Gewährung von Sozialhilfe habe ich bereits in meinem 10. Tätigkeitsbericht unter 10.2.4 unter Berufung auf eine Entscheidung des Hessischen Verwaltungsgerichtshofes ausgeführt, dass „ein pauschaler Allgemeinverdacht gegenüber den von einem Hilfesuchenden abgegeben Erklärungen und Angaben nicht ausreichend [ist], um dem Hilfesuchenden eine besondere Beweisführung aufzugeben. Ohne Vorliegen konkreter Anhaltspunkte ist das Verlangen, der Einholung von Bankauskünften zuzustimmen, eine überflüssige Ermittlungstätigkeit des Sozialhilfeträgers und somit nicht *erforderlich* im Sinne von § 60 Abs. 1 Nr. 1 SGB I.“ Nicht erforderlich ist demzufolge auch die mit der Einholung von Bankauskünften verbundene Datenerhebung (§ 67 a Abs. 1 Satz 2 SGB X). Es ist kein Grund ersichtlich, warum dies bei der Überwachung der Berechtigung zum Bezug der Leistungen anders beurteilt werden sollte.

Im Gegenteil: Einen Hinweis dahingehend, dass eine Datenübermittlung nur zulässig ist, wenn konkrete Verdachtsgründe für einen Leistungsmissbrauch gegeben sind, enthalten auch die folgenden Ausführungen bei von Wulffen/Roos, SGB X § 69, Rdnr. 13, die sich direkt an die Feststellung, dass zu den Aufgaben der Sozialleistungsträger auch die Überprüfung des Vorliegens der Voraussetzungen für die Leistungsgewährung gehört, anschließen; dort heißt es: „Bei einem eingeleiteten Ermittlungsverfahren wegen Verdachts, Sozialleistungen zu Unrecht bezogen zu haben, bedarf es für die Erteilung von Auskünften der Sozialleistungsbehörde keiner richterlichen Anordnung nach § 73 [SGB X].“ Der im Zusammenhang mit der Übermittlung von Sozialdaten stehenden Hinweis auf ein eingeleitetes Ermittlungsverfahren indiziert das Vorliegen eines konkreten Verdachts des Leistungsmissbrauches, denn ohne konkreten Anfangsverdacht wäre ein Ermittlungsverfahren nicht eingeleitet worden. Ein verdachtsunabhängiger Abgleich aller BAföG-Fälle ist demnach meines Erachtens unzulässig.

Auch § 45 d Abs. 3 EStG kann nicht als Rechtsgrundlage herangezogen werden; er umfasst diese Datenübermittlung nicht. Dass der Gesetzgeber für die mit dem Datenabgleich gemäß § 45 d Abs. 3 EStG verbundene Datenübermittlung durch die Sozialleistungsträger eine eigenständige Befugnisnorm für erforderlich hält, wird durch die Existenz des § 117 BSHG deutlich. Nach § 117 Abs. 1 Satz 1 Nr. 3 BSHG sind die Träger der Sozialhilfe befugt, Personen, die Leistungen nach dem Bundessozialhilfegesetz beziehen, daraufhin zu überprüfen, ob und welche Daten nach § 45 d EStG dem BfF (Auskunftsstelle) übermittelt worden sind. Gemäß § 117 Abs. 1 Satz 2 BSHG dürfen sie zum Zwecke der Überprüfung nach Satz 1 den Auskunftsstellen die zum Abgleich erforderlichen Daten übermitteln.

Die mangels einer entsprechenden gesetzlichen Regelung im Bereich der Ausbildungsförderung bestehende Lücke darf gerade angesichts dieser Regelung nicht dadurch geschlossen werden, dass die Übermittlungsbefugnis des § 69 SGB X extensiv ausgelegt wird bzw. man eine entsprechende Übermittlungsbefugnis in § 45 d Abs. 3 EStG hineinließt. Auch die festgestellte erhebliche Missbrauchs-Quote rechtfertigt eine solche Gesetzesanwendung nicht. Dagegen, eine neue gesetzliche Abgleichs-Erlaubnis zu schaffen - spezifisch im BAföG geregelt, nicht unspezifisch im SGB X - wäre angesichts der Höhe dieser Missbrauchsquote verfassungsrechtlich wohl nichts einzuwenden.

Diese meine Rechtsauffassung teilen die Datenschutzbeauftragten der Länder einstimmig; der Datenschutzbeauftragte des Bundes ist anderer Ansicht. Dementsprechend wurde auf der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden festgestellt: „Alle Länder sind sich einig, dass der vollständige Abgleich, was die Übermittlung durch die BAföG-Ämter an das Bundesamt für Finanzen angeht, nicht die nötige Rechtsgrundlage hat. Der Bund wiederholt seine Ansicht, wonach der Abgleich rechtlich noch vertretbar sei, wird aber die Einfügung einer gesetzlichen Erlaubnis zu Klarstellungszwecken fordern.“ Inzwischen hat der BfD mitgeteilt, dass es innerhalb der Bundesregierung Bestrebungen gebe, den Entwurf einer entsprechenden gesetzlichen Regelung - bedauerlicherweise im SGB X - vorzulegen. Offenbar wird der Gesetzgeber wach: Seine, nur seine Aufgabe ist es, angesichts großer Neigung der Studenten, falsche Angaben zu Vermögen (und Einkommen) zu machen, für eine ordentliche und rechtsstaatlich saubere Kontrollbefugnis zu sorgen. Diese zu schaffende normenklare Rechtsgrundlage sollte neben § 117 BSHG ein Schulbeispiel dafür werden, dass der unzweifelhaft vorhandene Sozialleistungsmissbrauch dringend flächendeckend unterbunden werden müsste. Dem Subsidiaritätsprinzip muss auch dadurch Geltung verschafft werden, dass die persönliche Leistungsfähigkeit tatsächlich ausgeschöpft wird, ehe die Allgemeinheit in Anspruch genommen wird. Die Parlamentarier sind aufgefordert, dies offensiv zu vertreten und die Erlaubnisnormen zu beschließen.

Bereits im Februar 2003 habe ich dem Sächsischen Landesamt für Ausbildungsförderung meine Rechtsauffassung dargelegt und es nachdrücklich gebeten, angesichts

der Unzulässigkeit der Datenübermittlung durch die BAföG-Ämter an das BfF den automatisierten Abgleich der BAföG-Ämter beim BfF unverzüglich einzustellen und, soweit das BfF bereits Ergebnisse mitgeteilt hat, diese nicht zu nutzen und sie umgehend zu löschen. Das - insoweit zuständige (§ 3 Abs. 1 SächsAG-BAföG) - SMWK habe ich um Stellungnahme gebeten.

Auf meine Erinnerung hin teilte das Sächsische Landesamt für Ausbildungsförderung Ende Mai 2003 mit, dass mir die in meinem Schreiben vom 13. Februar 2003 erbetene Stellungnahme vom SMWK zugehe. Nach nochmaliger Erinnerung und Hinweis auf Erstellung dieses Tätigkeitsberichtes hat das Ministerium schließlich erklärt, dass es den vollständigen Datenabgleich für „vertretbar“ erachte, und sich dabei - ohne sich die Mühe einer eigenen Begründung zu machen auf den BfD berufen. Auch wenn das SMWK nicht einmal dazu Stellung genommen hat, kann angenommen werden, dass es meine Bitte, den Datenabgleich einzustellen, nicht erfüllen wird.

Dennoch sehe ich gemäß § 26 Abs. 2 SächsDSG von einer förmlichen Beanstandung ab, da - so jedenfalls das SMWK - das Bundesministerium für Bildung und Forschung die Länder zur Durchführung des Datenabgleichs zwischen den BAföG-Ämtern und dem BfF auf eventuelle Regressansprüche des Bundes gegen die Länder hingewiesen und angewiesen hat, den Datenabgleich zwischen den BAföG-Ämtern und dem BSF durchzuführen und für den Fall der Nichtbefolgung die Geltendmachung von Schadensersatzansprüchen angedroht hat. Ich bringe also durchaus Verständnis auf für die Lage des Ministeriums, das keine andere Möglichkeit sieht, als der Anweisung des BMBF zu folgen, das - und zwar auch seitdem die Landesdatenschutzbeauftragten den Abbruch des Datenabgleichs fordern - unverändert und ausdrücklich an seiner Anordnung festhält. Der Mut, eine eigene Rechtsauffassung zu entwickeln fehlte aber; der bloße Hinweis auf die angeblich große Anzahl falscher Angaben ersetzt die juristische Argumentation nicht.

Es kann gut sein, dass der eine oder andere Betroffene wegen dieses Abgleiches auch vor Gericht ziehen wird.

10.3 Lebensmittelüberwachung und Veterinärwesen

Lebensmittelüberwachung: Auskunft über den angeblichen Gewährsmann des Hinweisgebers

Das LÜVA eines Landkreises hatte von einem Anrufer, der seinen Namen nicht nennen wollte, den Hinweis erhalten, in der Küche eines Kinder- und Jugenderholungszentrums gelangten Mehlmotten und Mäusekot in die ausgereichten Speisen. Auf die Erwiderung, anonymen Hinweisen werde nicht nachgegangen, hatte der Anrufer dadurch reagiert, dass er zehn Minuten später erneut anrief und erklärte, er meine sei-

nen Hinweis ernst, die betreffende Information habe er von einer in der betreffenden Küche beschäftigten (weiblichen) Person, wobei er einen Namen nannte. Dem LÜVA, das schon seit vielen Jahren in der üblichen Weise diese Küche kontrollierte, war dieser Name - rechtmäßig - als derjenige einer in der Küche Beschäftigten bekannt gewesen. Am nächsten Tag hatte das LÜVA dann unangekündigt eine Kontrolle in der Küche durchgeführt, deren Ergebnis es als nicht völlig ausgeschlossen, aber doch als sehr unwahrscheinlich hatte erscheinen lassen, dass in den Wochen oder Tagen davor die vom Anrufer angegebenen Zustände bzw. Praktiken geherrscht hatten: Es waren keine Mäuse und keine Mehlmotten zu sehen gewesen, wenn auch vorsorglich Fallen aufgestellt waren, was auch den Vorschriften entsprach; Verunreinigungen von Nahrungsmitteln durch Vorratsschädlinge waren nicht festgestellt worden.

Das Heim wurde von einem Verein mit einigen Dutzend festangestellter Kräfte betrieben, davon fünf Frauen im Küchenbereich, die alle am Ort wohnten.

Weil die Behörde bei ihrer Kontrolle angegeben hatte, dass sie einen Hinweis erhalten habe, bei dem der Name einer der fünf in der Küche beschäftigten weiblichen Arbeitskräfte gefallen sei, wollte der Geschäftsführer des Freizeit- und Erholungszentrums nunmehr vom LÜVA den im Hinweis genannten Namen wissen. Er selber habe noch keine Fragen an die in der Küche Tätigen gerichtet, aber es herrsche große Unruhe und Verunsicherung, die sich abträglich auf den Umgang der Beschäftigten mit den Gästen (Kunden) auswirkten, der Vereinsvorstand sei beunruhigt und wolle Klarheit, weniger gegebenenfalls die „Bestrafung“ der Schuldigen. Die Behörde wollte von mir wissen, was sie zu tun habe.

Auf den Akteneinsichtsanspruch nach § 29 VwVfG konnte das Auskunftsbegehren nicht gestützt werden. Denn der in dieser Vorschrift gewährte Einsichts- bzw. Auskunftsanspruch entfällt mit Abschluss des Verwaltungsverfahrens (insbesondere der Unanfechtbarkeit des Verwaltungsaktes; vgl. Knack/Clausen Rdnr. 4.2 zu § 29, Kopp Rdnr. 7, jeweils zu § 29 VwVfG und jeweils mit weiteren Nachweisen).

Es blieb also nur die Möglichkeit des datenschutzrechtlichen Auskunftsanspruches gemäß § 17 SächsDSG. Dieser Anspruch steht bei strikter Gesetzesauslegung gemäß § 17 Abs. 1 i. V. m. § 3 Abs. 1 SächsDSG nur natürlichen Personen zu, nicht juristischen. Betroffen waren bei dem das Kinder- und Jugenderholungszentrum betreibenden Verein auch die Verantwortlichen, wie namentlich der Geschäftsführer; mittelbar betroffen waren auch die fünf in der Küche arbeitenden Personen sowie diejenigen, welche die Aufsicht über sie führten. Daher hatte ich keine Bedenken, dass sich das Auskunftsverlangen grundsätzlich auf § 17 Abs. 1 SächsDSG stützen konnte.

Zu beachten war dabei jedoch die Ausnahmeregelung des Abs. 5 des § 17 Sächs DSG, wonach *die Auskunftserteilung unterbleibt, soweit die personenbezogenen Daten bzw. die Tatsache ihrer Speicherung unter anderem wegen überwiegender Ge-*

heimhaltungsinteressen der speichernden Stelle oder eines Dritten geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Für die Anwendung dieser Vorschrift hat die Rechtsprechung die Regel entwickelt, dass genau derjenige Hinweisgeber geschützt wird, der redlich war, nämlich nicht bewusst oder leichtfertig falsche Angaben gemacht hat. Ich habe das ausführlicher in Abschnitt 9/10.2.10 erläutert.

Die Anwendung dieser Regel auf den vorliegenden Fall war jedoch nicht ganz einfach.

Zunächst einmal: Das gespeicherte Datum, dessen Mitteilung verlangt wurde, war, dass *der anonyme Hinweisgeber sich für die Richtigkeit seiner Angabe darauf berufen hatte, dass er sein Wissen von der namentlich genannten, in der Küche arbeitenden Person erhalten habe.* Das war, was die Zustände betrifft, die angeblich in der Küche geherrscht hatten, eine Angabe zur Person der in der Küche Arbeitenden bzw. für sie verantwortlichen Personen und zugleich eine Angabe über die angebliche Herkunft von Daten über die Betreffenden, vgl. § 17 Abs. 1 Nr.1 und 3 SächsDSG.

Es gab drei Möglichkeiten:

A 1 Die genannte Person war mittelbarer Hinweisgeber, also beteiligt, aber *redlich,* weil die Angabe zutreffend war,

A 2 die Namensträgerin war als mittelbare Hinweisgeberin beteiligt und *unredlich* oder

B die Namensträgerin war an dem Informationsvorgang gänzlich unbeteiligt, sie hatte ihn nicht veranlasst, er konnte ihr nicht zugerechnet werden (was meiner Auffassung nach auch dann der Fall war, wenn sie Wahres gesagt hatte, was dann ein Zuhörer, ohne dass sie damit hatte rechnen müssen, unter Aufbauschung der Information missbraucht hatte) - vielmehr hat der Anrufer eine falsche Fährte legen wollen.

Im Falle A 1 war die Namensträgerin nach der oben genannten *Abwägungsregel* zu schützen, im Falle A 2 gerade nicht, musste ihr Name also bekanntgegeben werden.

Für den Fall B habe ich den Auskunftsanspruch für ausgeschlossen gehalten, die Auskunftserteilung also für rechtswidrig, und zwar deswegen, weil die Namensträgerin das Opfer eines Dritten gewesen wäre, ihr Name dem Betroffenen nicht bei der Verfolgung rechtlicher Interessen würde weiterhelfen können, andererseits aber die Namensträgerin in einen Verdacht hätte geraten müssen, den sie nicht würde entkräften können, weil man negative Tatsachen - also dass man etwas *nicht getan* hat - kaum je beweisen kann.

Eine begründete Entscheidung des LÜVA über den geltend gemachten Auskunftserteilungsanspruch hätte also der Sachverhaltsaufklärung bedurft. Diese wäre grund-

sätzlich möglich, die dazu erforderliche Verarbeitung personenbezogener Daten zur Aufgabenerfüllung auch erforderlich gewesen. Notfalls hätte eine Melderegisterauskunft zu dem betreffenden Namen bei dem zuständigen Einwohnermeldeamt eingeholt und dann die Trägerin des Namens angehört werden müssen. Dabei wäre es aus Datenschutzgründen selbstverständlich unzulässig gewesen, die Person dabei unter ihrer Arbeitsplatz-Anschrift anzuschreiben. Angesichts dessen, dass sich der Vorgang in eingeweihten Kreisen herumgesprochen haben musste, wäre es auch unzulässig gewesen, die Namensträgerin unter Verwendung eines den Absender (Landratsamt, insbesondere LÜVA) erkennbar werden lassenden Briefumschlages anzuschreiben. Der Geschäftsführer des Vereins hätte in einem solchen Fall seine Einwilligung darin erklärt, dass das LÜVA gegenüber der Trägerin des Namens in diesem Zusammenhang bekanntgegeben hätte, dass es die anonyme Anzeige gegeben habe, dass dabei der Name der Betreffenden genannt worden sei und dass die Geschäftsführung des Betriebes Auskunft darüber verlangt habe, um welchen Namen es sich handele.

Aus folgenden Gründen bin ich endlich doch zu der Auffassung gelangt, dass das LÜVA diese (zusätzlichen) Sachverhaltsaufklärungsversuche *nicht unternehmen*, sondern *den Auskunftsanspruch zurückweisen sollte*: Sollte die Namensträgerin vorsätzlich oder auch nur leicht fahrlässig gehandelt, also eine unzutreffende Beschreibung der Zustände in der Küche abgegeben haben, würde sie aller Wahrscheinlichkeit nach schlicht alles abstreiten. Dazu würde es für sie nicht des geringsten Aufwandes bedürfen - sie würde nur sagen müssen, sie habe damit nichts zu tun und könne sich nicht erklären, wieso man ihr diese Aussage zuschreibe. Dann würde der Sachverhalt unaufgeklärt und auch unaufklärbar bleiben.

Bei Unaufklärbarkeit aber überwiegt meiner Auffassung nach das Schutzinteresse eines aus unaufklärbaren Gründen von einem Dritten benannten Namensträgers. Er geriete notwendig ins Gerede; es bliebe etwas an ihm hängen. Die Abwägung fällt daher wie im Falle B aus. Die Speicherung des Namens des angeblichen Gewährsmannes ist dann im Vergleich zur Existenz des Hinweises und noch mehr zum Ergebnis der Kontrolle im Betrieb nur von sehr untergeordneter Bedeutung, die Nachteile einer Offenlegung des Namens der genannten Person könnten für diese jedoch sehr groß sein, gerade weil man sich gegen das „Hängenbleiben“ eines nicht bewiesenen Vorwurfs nicht wehren kann.

Überdies habe ich die Wahrscheinlichkeit für recht groß gehalten, dass der Anrufer nicht redlich gewesen ist, und zwar gerade auch im Hinblick auf die Namensträgerin (seine Tatsachenbehauptung war ja auch falsch).

Im Ergebnis habe ich daher der Behörde geraten, den Auskunftsanspruch zurückzuweisen.

Selbstverständlich habe ich der Behörde nahegelegt, sich dafür auf meine Stellungnahme zu berufen, die ich auch im vollen Wortlaut dem Geschäftsführer des Betriebes habe zukommen lassen - weil für ihn und vielleicht auch für die Belegschaft seines

Betriebes nachvollziehbar werden sollte, warum in der Angelegenheit eine Auskunft bisher nicht erteilt worden war und nach Auffassung des Sächsischen Datenschutzbeauftragten auch nicht erteilt werden sollte. Zusätzlich habe ich mit dem Geschäftsführer des Betriebes abgesprochen, dass dann, wenn ein zweiter Fall unberechtigter Anschwärzung des Beherbergungsbetriebes bei einer Behörde eintreten sollte, er die Einwilligung erteilen werde, dass sämtliche in Frage kommenden Behörden gewarnt würden, dass das Kinder- und Jugenderholungszentrum zur Zeit Opfer unberechtigter Anschuldigungen werden könne. Dies entsprach im übrigen der klugen Vorgehensweise des LÜVA, das nicht nur gleich zu Anfang seiner Kontrolle mitgeteilt hatte, dass diese aufgrund eines Hinweises erfolge, sondern auch die Frage gestellt hatte, ob der Betrieb zur Zeit sich in Auseinandersetzungen mit Beschäftigten, ehemaligen Beschäftigten oder dergleichen befinde. Dem konnte man entnehmen, dass der Betrieb zu diesem Zeitpunkt noch nicht bei den zuständigen Behörden in Verruf geraten, objektiv also keine Rufschädigung eingetreten war.

Da ich von der Angelegenheit dann nichts mehr gehört habe, gehe ich davon aus, dass der Beherbergungsbetrieb mit der von mir empfohlenen Entscheidung hat leben können, insbesondere in dieser zum juristischen Neuland gehörenden Frage nicht die Gerichte angerufen hat.

10.4 Rehabilitierungsgesetze

In diesem Jahr nicht belegt.

11 Landwirtschaft, Ernährung und Forsten

In diesem Jahr nicht belegt.

12 Umwelt

12.1 Unterrichtung der Staatlichen Umweltfachämter über verwaltungs- und ordnungsrechtliche Maßnahmen der Vollzugsbehörden

Der Datenschutzbeauftragte eines Landratsamtes hatte Zweifel, ob seine Behörde die Staatlichen Umweltfachämter (kurz: StUFÄ) über den Stand verwaltungs- und ordnungsrechtlicher Verfahren unterrichten darf, die aufgrund von Feststellungen dieser Ämter eingeleitet worden sind. So hatte es das SMUL über die Regierungspräsidien für den Bereich des *anlagenbezogenen Immissionsschutzes* in einem Erlass den Landkreisen und kreisfreien Städten „als unteren Verwaltungsbehörden“ aufgegeben

Der Erlass des SMUL bezieht sich auf Fälle, in welchen die StUFÄ für die Erfüllung der Überwachungsaufgaben nach § 52 Abs. 1, 2, 3 und 6 BImSchG gemäß Nr. III. 1.6.2 des Anhangs zur Zuständigkeitsverordnung Immissionsschutz (ImSchZuV, vom 20. Juni 2000, SächsGVBl. S. 302, 307, zuletzt geändert durch Verordnung vom 12. Juli 2002, SächsGVBl. S. 243), zuständig sind, und festgestellt haben, dass eine Anlage in einer nicht den immissionsschutzrechtlichen Anforderungen entsprechenden Weise betrieben wird, und das auch denjenigen Behörden mitgeteilt haben, deren Aufgabe es ist, daraufhin nachträgliche Anordnungen (§§ 17, 24 BImSchG) zu treffen oder die Anlage zu schließen (§§ 20, 25 BImSchG).

Für diese Maßnahmen - wie auch für die Erteilung von Genehmigungen - als sog. *Vollzugsaufgaben* sind andere Behörden zuständig, nämlich, sofern nicht ausnahmsweise das RP oder SMUL selbst zuständig sind, die Landkreise oder kreisfreien Städte (Nr. III. 1.1.12, 1.1.13, 1.2.1 oder 1.2.2 des Anhangs zur ImSchZuV, wenn man die Fälle der Zuständigkeit der Bergbehörden zwecks Vereinfachung einmal vernachlässigt). Dieselben Behörden leiten gegebenenfalls ein Bußgeldverfahren ein oder unterrichten wegen des Verdachtes auf eine (Umwelt-)Straftat die Staatsanwaltschaft.

Bei der im Erlass verlangten Unterrichtung der StUFÄ durch die Vollzugsbehörden handelt es sich um eine Übermittlung personenbezogener Daten. Deren Zulässigkeit richtet sich mangels spezialgesetzlicher Regelung nach § 13 Abs. 1 SächsDSG.

Die Datenübermittlung ist im Sinne von § 13 Abs. 1 Nr. 1 SächsDSG zur Aufgabenerfüllung der StUFÄ, also der Empfänger-Stelle, *erforderlich*. Damit sie ihre Überwachungsaufgabe überhaupt sinnvoll wahrnehmen können, müssen die StUFÄ wissen, wie gegebenenfalls die Pflichten des jeweiligen Anlagenbetreibers durch Anordnungen der Vollzugsbehörden bestimmt worden sind. Daher sind die StUFÄ insbesondere über den Erlass verwaltungsrechtlicher Anordnungen, die im Einzelfall die immissionsschutzrechtlichen Pflichten der Betreiber der Anlagen konkretisieren, und über das

Ergebnis hiergegen eingelegter Rechtsbehelfe zu unterrichten. Gleiches gilt für die Unterrichtung über die Einleitung und insbesondere den Abschluss von Ordnungswidrigkeitenverfahren bzw. strafgerichtlicher Verfahren. Denn auch hier wird - wenn auch nicht verwaltungsrechtlich unmittelbar bindender Weise - eine Entscheidung über das Vorliegen eines Verstoßes gegen immissionsschutzrechtliche Pflichten als Vorfrage getroffen, was dann ebenfalls Auswirkungen auf die weitere Überwachungstätigkeit der StUFÄ und somit auf deren ordnungsgemäße Aufgabenerfüllung hat.

Auch die in § 13 Abs. 1 Nr. 2 SächsDSG genannte zusätzliche Voraussetzung, nämlich die Wahrung der Zweckbindung (oder doch das Vorliegen einer privilegierten Zweckänderung), ist erfüllt. Denn es besteht hier insoweit Zweckidentität zwischen den Aufgaben der Vollzugsbehörden und der StUFÄ als Überwachungsbehörden. Geht es doch jeweils um die Sicherstellung der Einhaltung der immissionsschutzrechtlichen Vorschriften beim Betreiben bestimmter Anlagen, sei es nun durch Überwachung oder bei Feststellung von Verstößen durch Herbeiführen verwaltungs- oder ordnungsrechtlicher Konsequenzen.

Allerdings ist die Übermittlung jeweils auf die im konkreten Fall tatsächlich für die StUFÄ erforderlichen Daten zu beschränken, mit gewissen Erleichterungen gemäß §§ 13 Abs. 4, 12 Abs. 5 SächsDSG.

Oft verstellt die organisatorische Zusammenfassung funktionell verschiedener Behörden den Blick auf die Zweckbindung, die für die Verarbeitung personenbezogener Daten gilt; im vorliegenden Fall kann man jedoch sehen, dass es auch umgekehrt sein, dass also die Aufteilung des Vollzuges eines Gesetzes auf organisatorisch getrennte Behörden den Blick für die Zweckidentität verstellen kann (vgl. auch den Fall von 10.2.5).

12.2 Erhebung von „Angaben zur Entsorgung des Abwassers aus Kleinkläranlagen und abflusslosen Gruben“ durch einen Abwasserzweckverband zum Zwecke der Aufstellung eines Abwasserbeseitigungskonzeptes

Ein Petent übersandte mir das Schreiben eines Abwasserzweckverbandes, in dem dieser ihn gebeten hatte, den beigefügten Fragebogen „Angaben zur Entsorgung des Abwassers aus Kleinkläranlagen und abflusslosen Gruben“ auszufüllen und zurückzusenden. In dem Fragebogen sollten neben den Angaben zur Person des Grundstückseigentümers und zum Grundstück insbesondere Angaben über die betriebene Kleinkläranlage oder abflusslose Grube, Sickergrube oder Absetzgrube gemacht werden. Gefragt wurde zum Beispiel nach Baujahr, Größe und Art der Anlage sowie deren behördlicher Genehmigung und Bauabnahme. Weiter enthielt der Fragebogen Fragen

nach dem baulichen Zustand der Anlage und der Art und Weise der Entsorgung des Abwassers und des Klärschlamms.

Nachdem der Petent den Fragebogen nicht innerhalb der ihm vom Zweckverband hierfür gesetzten Frist zurückgesandt hatte, „bat“ dieser ihn noch einmal, seiner Aufforderung binnen drei Wochen nachzukommen, und wies ihn darauf hin, dass er „gemäß § 49 Abwassersatzung die Angaben zu den vorhandenen abflusslosen Gruben und Kleinkläranlagen ... zur Verfügung zu stellen“ habe „und dass bei Nichtinformation eine Ordnungswidrigkeit im Sinne von § 124 Abs. 6 SächsGemO“ vorliege.

1. Ich habe den Zweckverband darauf hingewiesen, dass *§ 49 seiner Abwassersatzung* nicht als Rechtsgrundlage für die gesamte Datenverarbeitung herangezogen werden konnte. Gemäß § 49 Abs. 1 Nr. 2 dieser Abwassersatzung waren nämlich nur die bei Inkrafttreten der Satzung vorhandenen abflusslosen Gruben und Kleinkläranlagen anzuzeigen; gemäß § 49 Abs. 3 Nr. 2 der Abwassersatzung war außerdem der Entleerungsbedarf der abflusslosen Gruben und Kleinkläranlagen mitzuteilen. Die mittels Fragebogen abgefragten Angaben gingen jedoch weit über diese Informationen hinaus, waren also nicht von § 49 der Abwassersatzung gedeckt.

2. Der Zweckverband nannte daraufhin als in Betracht kommende Rechtsgrundlage die Vorschrift des *§ 63 Abs. 2 SächsWG i. V. m. dem „Erlass des SMUL zum weiteren Ausbau der Abwasserbeseitigung in Sachsen“*. § 63 Abs. 2 Satz 1 SächsWG bestimmt, dass die Abwasserbeseitigungspflicht den Gemeinden obliegt, in deren Gebiet das Abwasser anfällt. Gemäß § 63 Abs. 2 Satz 2 SächsWG haben die Abwasserbeseitigungspflichtigen ein Abwasserbeseitigungskonzept aufzustellen, das u.a. die „Teile des Entsorgungsgebietes bezeichnet, die über nicht öffentliche Anlagen, insbesondere Kleinkläranlagen und abflusslose Gruben entsorgt werden sollen“ (Nr. 3).
   Ich habe dem Zweckverband erläutert, dass § 63 Abs. 2 SächsWG und/oder der Erlass des SMUL ebenfalls nicht als Rechtsgrundlage für die Datenverarbeitung herangezogen werden konnten. Der Erlass des SMUL stellt als solcher schon keine Erlaubnisnorm im Sinne des § 4 Abs. 1 Nr. 1 SächsDSG dar, denn als abstrakt generelle Anordnung einer Behörde an die ihr nachfolgenden Behörden entfaltet er keine unmittelbare Außenwirkung, begründet also für die Bürger keine Rechte und Pflichten (Maurer, Allgemeines Verwaltungsrecht, § 24, Rdnr. 1 und 17). Verwaltungsvorschriften sind halt keine „Gesetze“, keine „Rechtsvorschriften“, sie können Grundrechtseingriffe nicht legitimieren. Die Vorschrift des § 63 Abs. 2 SächsWG ist meines Erachtens hinsichtlich der zu verarbeitenden Daten nicht hinreichend konkret in dem Sinne, als sie die für die Erstellung des Abwasserbeseitigungskonzeptes erforderlichen Daten genau bezeichnet; auch der Erlass des SMUL macht diesbezüglich keine Angaben, kann also die gesetzliche Vorschrift nicht konkretisieren. Im Gegenteil: Wie schon der Wortlaut des § 63 Abs. 2 Satz 2 Nr. 3 SächsWG nahelegt, soll das Abwasserbeseitigungskonzept *keine Angaben zu jeder einzelnen Kleinkläranlage und abflusslosen Grube* enthalten, geschweige denn nähere An-

gaben zu deren Errichtung, baulichem Zustand oder Entsorgung. Es soll *nur die Teile des Entsorgungsgebietes*, die über Kleinkläranlagen und abflusslose Gruben entsorgt werden sollen, bezeichnen.

Da die Datenverarbeitung nicht durch eine Rechtsvorschrift erlaubt und damit nach § 4 Abs. 1 SächsDSG unzulässig war, habe ich den Zweckverband gebeten, die unzulässigerweise erhobenen und gespeicherten Daten zu löschen. Über meine Rechtsauffassung habe ich auch das SMUL durch Übersenden eines Abdrucks meines Schreibens an den Abwasserzweckverband informiert.

3. Auf mein Schreiben hin teilte mir der Zweckverband schließlich mit, dass „die Befragung im Auftrage des Landratsamtes" erfolgt war. Ich habe mich also an den Landkreis gewandt und ihn um Stellungnahme zu dieser Behauptung gebeten. Noch bevor ich eine Antwort des Landkreises erhielt, teilte mir der Zweckverband allerdings mit, dass er die mittels Fragebogen erhobenen und anschließend gespeicherten Daten gelöscht habe.

   Der Landkreis erklärte schließlich, dass sich „die Rechtsgrundlagen für die Kontrollen von wasserrechtlich erlaubnis- oder bewilligungsbedürftigen oder anzeigepflichtigen Anlagen u. a. aus *§ 21 des Wasserhaushaltsgesetzes ... sowie § 95 des Sächsischen Wassergesetzes* ergeben". Ich habe ihm geantwortet, dass sich auch diese Vorschriften nicht als Rechtsgrundlage für die vom Abwasserzweckverband vorgenommene Datenverarbeitung heranziehen ließen. (Es ist erfahrungsgemäß verräterisch, wenn Behörden für ihr Handeln die Begründungen wechseln; sie sind rechtsstaatlich nicht sattelfest):

   Die Überwachungs-Befugnisse des § 21 WHG setzen zwar nicht voraus, dass eine Gewässerbenutzung erlaubnis- oder bewilligungspflichtig ist. Wie sich bereits aus dem Wortlaut des § 21 Abs. 1 Satz 1 WHG ergibt, ist jeder, der ein Gewässer benutzt, verpflichtet, eine behördliche Überwachung der Anlagen, Einrichtungen und Vorgänge zu dulden, die für die Gewässerbenutzung von Bedeutung sind (vgl. Dame, in: Sieder-Zeitler-Dame, WHG-Kommentar, § 21 Rdnr. 9). Wer eine Kleinkläranlage oder abflusslose Grube betreibt, bedarf hierfür zwar keiner wasserrechtlichen Genehmigung (§ 67 Abs. 2 Satz 1 Nr. 4, Nr. 5 SächsWG i. V. m. § 2 Abs. 1 WHG), dennoch stellt das Betreiben einer solchen Anlage eine Gewässerbenutzung im Sinne des § 21 WHG dar: § 3 Abs. 1 Nr. 4 und Nr. 5 WHG definieren als Gewässerbenutzung das Einbringen und Einleiten von Stoffen in oberirdische Gewässer bzw. in das Grundwasser.

   Nach § 21 Abs. 1 Satz 1 WHG hat der Benutzer aber nur eine *behördliche* Überwachung zu dulden. Eine behördliche Überwachung in diesem Sinne ist die Überwachung der Benutzung durch diejenigen Organe, die nach den Landesgesetzen zur Gewässerüberwachung berufen sind. Nicht schon jede Behörde, die wasser-

rechtliche Aufgaben wahrzunehmen hat, ist Überwachungsbehörde im Sinne des § 21 Abs. 1 Satz 1 WHG. So werden z. B. einer Gemeinde mit der Übertragung der Abwasserbeseitigungspflicht keine wasserrechtlichen Befugnisse als Ordnungsbehörde übertragen (so Dame, a. a. O., Rdnr. 13).

Gemäß § 119 Abs. 1 i. V. m. § 118 Abs. 1 Nr. 3 SächsWG sind die Landkreise als untere Wasserbehörden zum Vollzug des Wasserhaushaltsgesetzes und des Sächsischen Wassergesetzes berufen, *nicht jedoch die Gemeinden oder Zweckverbände*. Daraus folgt, dass es nicht zu den Aufgaben des Abwasserzweckverbandes gehört, die Gewässerbenutzung zu überwachen. Daraus folgt weiter, dass der Zweckverband nicht befugt ist, die Betreiber von Kleinkläranlagen oder abflusslosen Gruben aufgrund einer Rechtsvorschrift zu befragen, die (nur) die Wasserbehörden oder technischen Fachbehörden zu Datenerhebungen ermächtigt.

Es lag auch keine wirksame Beauftragung des Abwasserzweckverbandes mit der Datenerhebung vor, wie sie § 95 SächsWG vorsieht: Der Landkreis teilte etwa ein halbes Jahr später mit, den Zweckverband zu keinem Zeitpunkt beauftragt zu haben, Daten zu erfassen, die über die für die Aufgabenerfüllung in eigener Zuständigkeit erforderlichen Angaben nach der Abwassersatzung in Verbindung mit den gesetzlichen Grundlagen des Wasserrechts hinausgehen. Mangels wirksamer Beauftragung haben dem Abwasserzweckverband also auch die in § 95 SächsWG normierten Befugnisse nicht zugestanden.

4. Nach nochmaliger Aufforderung nahm nunmehr auch das SMUL zu dieser Problematik Stellung und erklärte, es teile meine Auffassung insoweit, als die Vorschriften der § 21 WHG und § 95 SächsWG nicht als Rechtsgrundlage für die Datenverarbeitung durch den Abwasserzweckverband herangezogen werden könnten. Es meinte jedoch, dass § 63 Abs. 2 SächsWG die erforderliche Rechtsgrundlage hierfür bilde; für die Erstellung eines Abwasserbeseitigungskonzeptes sei beispielsweise die Kenntnis des Zustands, des Baujahrs und des ordnungsgemäßen Betriebs der dezentralen Anlagen erforderlich. Ich habe dem Staatsministerium mitgeteilt, dass mich seine Ausführungen nicht überzeugen und ich bei meiner Auffassung bleiben würde.

Daraufhin erklärte das SMUL, die Argumente zur datenschutzrechtlichen Einschätzung der angesprochenen Sachverhaltskonstellation seien nunmehr im wesentlichen ausgetauscht. Es schlug vor, den Sachverhalt anlässlich der anstehenden umfassenden Novellierung des Sächsischen Wassergesetzes im Zuge der Umsetzung der Wasserrahmenrichtlinie der EU nochmals einer Prüfung zu unterziehen. Es sei daran interessiert, dass ich ihm einen Formulierungsvorschlag für eine als Rechtsgrundlage für die Datenverarbeitung zum Zweck der Erstellung eines Abwasserbeseitigungskonzeptes in Betracht kommende Vorschrift unterbreite.

Ich darf also wohl davon ausgehen, dass sich das SMUL letztlich meiner Argumentation nicht verschlossen und eingesehen hat, dass § 63 Abs. 2 Satz 2 SächsWG lediglich eine Aufgabe ausspricht, für deren Erfüllung es zwar zweckdienlich erforderlich wäre, die im Streit stehenden Daten der einzelnen Betreiber der Kleinkläranlagen und abflusslosen Gruben zu erheben, dass der Vorschrift aber die hierfür notwendige klare Bezugnahme auf eine vollständige Kenntnis jeder einzelnen der betreffenden Anlagen fehlt.

Selbstverständlich werde ich das SMUL bei der Novellierung des Sächsischen Wassergesetzes unterstützen.

13 Wissenschaft und Kunst

13.1 Stichprobenziehung für die Bevölkerungsbefragung im Rahmen des Forschungsvorhabens „Winkover“

Im Rahmen des Forschungsvorhabens „Winkover“ beabsichtigt das Institut für Verkehrsplanung und Straßenverkehr an der Fakultät Verkehrswissenschaften „Friedrich List“ an der TU Dresden, eine Bevölkerungsbefragung durchzuführen. Hierzu soll zunächst eine Stichprobe von 1.500 bis 2.000 Personen aus den Fahrerlaubnisregistern der Landkreise Vogtlandkreis (Sachsen), Hof (Bayern), Teltow-Fleming (Brandenburg), Wittenberg (Sachsen-Anhalt) sowie Herzogtum Lauenburg (Schleswig-Holstein) gezogen werden. Die Behörden sollen dem Institut Namen, Vornamen, Geburtsdatum, Anschrift und Führerscheinklasse übermitteln. Das Institut will dann die Telefonnummern dieser Personen ermitteln, die Testpersonen im einzelnen über die Art und Bedeutung der Befragung informieren, und ihre Teilnahmebereitschaft erbitten. Es soll danach ein repräsentative Gruppe von etwa 300 Personen, geschichtet nach Geschlecht und Alter übrig bleiben, denen ein Fragebogen zugeschickt werden soll. Die Befragung soll dann wie folgt ablaufen: Das Institut übergibt dem Statistischen Landesamt in Kamenz eine Adressliste. Das Landesamt druckt die Fragebögen und die Umschläge, wobei erstere mit einer laufenden Nummer versehen werden. Gemäß den Zusicherungen der Forscher dient die Nummer allein dazu, die einzelnen Blätter eines Fragebogens zusammenzuführen, sollten diese beim späteren Einlesen durcheinander geraten. Die Nummer werde jedoch nicht zum Namen einer bestimmten Person gespeichert werden, so dass über die Nummer keine Verknüpfung von Person und Fragebogen möglich sei. Das Landesamt übernimmt auch die Versendung der Fragebögen zusammen mit einem an das Institut adressierten Rückumschlag. Das Institut wird dann die ausgefüllten Fragebögen wieder dem Landesamt übergeben, das die Bögen einliest und dem Institut die aggregierten Daten zur Verfügung stellt.

Zur Zulässigkeit dieser Datenverarbeitung habe ich - nachdem ich mich mit den Datenschutzbeauftragten Bayerns, Brandenburgs, Sachsen-Anhalts und Schleswig-Holsteins abgestimmt hatte - dem Institut Folgendes mitgeteilt:

1. Stichprobenziehung: Grundsätzlich dürften die Fahrerlaubnisbehörden die im Fahrerlaubnisregister gespeicherten Daten (§ 50 Abs. 1 und 2 StVG) gemäß § 38 Abs. 1 i. V. m. § 57 StVG an Hochschulen übermitteln, soweit dies zur Durchführung bestimmter wissenschaftlicher Forschungsarbeiten *erforderlich* ist (§ 38 Abs. 1 Nr. 1 StVG). Die Voraussetzungen dieser Vorschrift seien meines Erachtens vorliegend nicht erfüllt: Die Übermittlung der Daten sei für die Durchführung des Forschungsvorhabens *nicht erforderlich*, denn das Forschungsziel ließe sich auf andere Weise erreichen, die weniger in das Recht des Einzelnen auf informationelle Selbstbestimmung eingreife. Es bestünde nämlich die Möglichkeit, die Fahrerlaubnisbehörde als so genannten Adressmittler tätig werden zu lassen. Das heißt, die Fahrerlaubnisbehörden stellen den Kontakt zwischen den zu Befragenden und dem Institut in der Weise her, dass sie den Testpersonen mit einem Begleitschreiben den Fragebogen samt Anschreiben des Instituts zusenden. Hierbei dürften sich die Fahrerlaubnisbehörden des Statistischen Landesamtes als Auftragsdatenverarbeiters (§ 7 SächsDSG) bedienen. Das Statistische Landesamt könne also - wie vorgesehen - die Fragebögen und Umschläge drucken.

   Das Adressmittlungsverfahren ist deshalb weniger einschneidend, weil hier jemand, von dem der Betroffene weiß, dass er diese Daten gespeichert hat, personenbezogene Daten nutzt, aber sie eben nicht weitergibt. Der Betroffene hat es nun selbst in der Hand, Angaben zu seiner Person einem Dritten zur Kenntnis zu bringen, indem er den Fragebogen ausfüllt und an das Institut zurücksendet ober indem er das eben nicht tut.

   Die Befugnis der Fahrerlaubnisbehörden, die Daten zum Zwecke der Adressmittlung zu nutzen, dürfte bereits in § 38 Abs. 1 StVG impliziert sein, im Ergebnis kann dies jedoch offenbleiben, da sie sich jedenfalls aus § 12 Abs. 2 Nr. 4 SächsDSG ergäbe.

2. Befragung: Gegen die Datenerhebung mittels Fragebogen hätte ich - unter datenschutzrechtlichen Gesichtspunkten - keine Einwände. Zum einen, weil der Schutzbereich der informationellen Selbstbestimmung gar nicht eröffnet sei, da schon keine personenbezogenen Daten im Sinne des § 3 Abs. 1 SächsDSG verarbeitet werden würden. Denn die mittels Fragebogen erhobenen Angaben könnten nicht einer bestimmten Person zugeordnet werden, da weder auf dem Fragebogen, noch auf dem Rückumschlag der Name und die Anschrift des Absenders verzeichnet seien.

   Eine Anonymisierung wäre auch dann gewährleistet, wenn Angaben wie Name, Vorname, Geburtsdatum und Anschrift dem Institut vorlägen. Denn auch hier

könnten die vorhandenen und die mittels Fragebogen erhobenen Daten nicht miteinander verknüpft werden. Insbesondere soll nämlich keine (Teilnehmer-)Nummer vergeben werden, die die Verknüpfung ermöglichte. Die auf den Fragebögen angegebenen Nummern dienen nur der Kennzeichnung zusammengehörender Bestandteile eines Fragebogen-Satzes.

Gegen die Durchführung des von mir vorgeschlagenen Adressmittlungsverfahrens wandte das Institut ein, dass ein solches Vorgehen den Erkenntniswert der Forschungsergebnisse stark beeinträchtigen würde: Erkenntniswert hätten die Ergebnisse nur, wenn die befragte Personengruppe repräsentativ sei. Denn nur dann könnten die Forschungsergebnisse auf die übrige, nicht befragte Bevölkerung übertragen werden; wären sie also verallgemeinerungsfähig. Die Repräsentativität der zu befragenden Personengruppe sei um so größer, je größer die Antwortbereitschaft der zu Befragenden sei. Die Antwortbereitschaft hänge von verschiedenen Merkmalen ab, und zwar nicht nur von solchen, die Bestandteil des Datenschutzes sind, welchen die Fahrerlaubnisbehörde zur Ziehung der Stichprobe nutzt. Aus diesem Grunde bestünde keine Möglichkeit, die Roh-Stichprobe so zu gewichten, dass sie in der Weise zusammengesetzt ist, dass diejenigen Personenkreise, welche eine unterdurchschnittliche Reaktionsbereitschaft haben, entsprechend überproportional in ihr vorkommen, so dass der Unterschied in der Reaktionsbereitschaft in der Vorgewichtung so berücksichtigt werden kann, dass die End-Stichprobe repräsentativ ist. Die Forscher haben erläutert, dass zwar die geringere Antwortbereitschaft Jüngerer bei der Ziehung der Roh-Stichprobe berücksichtigt werden könne, nicht jedoch die geringere Teilnehmerbereitschaft anderer Personen, etwa derjenigen, die als Fahrzeugführer bei der Polizei bzw. der Straßenverkehrsbehörde überdurchschnittlich oft in Erscheinung getreten sind, oder der Personen, die allgemein eine Abneigung gegen „Schriftkram“ haben. Dagegen sei die vorherige telefonische Kontaktaufnahme geeignet, die Antwortbereitschaft zu erhöhen; ein Methodenvergleich habe ergeben, dass bei vorheriger telefonischer Ansprache insgesamt bis zu 84 % der zu Befragenden antworteten, gegenüber nur 12,6 % bei allein schriftlicher Ansprache. Für eine wissenschaftlich korrekte Durchführung des Forschungsvorhabens sei also die Herstellung eines telefonischen Kontaktes zu den in die Roh-Stichprobe aufgenommenen Personen erforderlich.

Diesen Argumenten des Instituts konnte ich mich nicht verschließen und habe gegenüber dem Institut erklärt, dass ich an meinem zuvor dargelegten Rechtsstandpunkt, wonach die Übermittlung des Datensatzes: *Familienname, Vorname, Geburtsdatum, Anschrift und Führerscheinklasse* durch die Fahrerlaubnisbehörde nicht erforderlich im Sinne des § 38 Abs. 1 Nr. 1 StVG sei, nicht festhalte. Die Gruppen der Testpersonen dürfen also doch vom Institut namensbezogen geordnet werden. Anhand der Adressdaten dürfen die Telefonnummern ermittelt und die Testpersonen dann namensbezogen angerufen, aufgeklärt und um Mitarbeit gebeten werden. Wird das abgelehnt, werden die Daten sofort gelöscht. Die TU Dresden ist mir da ein Garant.

Meine Kollegen in den ebenfalls von der Untersuchung betroffenen Bundesländern Bayern, Brandenburg, Sachsen-Anhalt sowie Schleswig-Holstein habe ich von der Änderung meiner Auffassung unterrichtet; sie haben mir nicht widersprochen.

13.2 Einsichtnahme einer Studentin in die Unterlagen einer GmbH, über deren Vermögen das Insolvenzverfahren eröffnet ist

Eine Rechtsanwältin teilte mir mit, dass sie zur Insolvenzverwalterin über das Vermögen einer privatrechtlichen GmbH, die als anerkannte private Krankenanstalt ein ambulantes Rehabilitationszentrum betrieben hat, bestellt worden war. In die in ihrem Besitz befindlichen Unterlagen der GmbH wollte nun eine Studentin der TU Dresden im Rahmen der Anfertigung ihrer Diplomarbeit zum Thema „Ökonomische Aufarbeitung der Situation in und um die A-GmbH“ Einsicht nehmen. Dieses Ansinnen habe sie aus datenschutzrechtlichen Gründen zurückgewiesen, da die Unterlagen auch personenbezogene Daten von Arbeitnehmern und Patienten der GmbH enthielten. Daraufhin habe die Betreuerin der Studentin sie mit Nachdruck, nämlich unter Androhung, sich ansonsten an „die entsprechende übergeordnete Aufsichtsbehörde“ zu wenden, aufgefordert, der Studentin die Einsicht in die Unterlagen zu gewähren. Dabei habe die Betreuerin darauf hingewiesen, dass „zur Bearbeitung keine patientenbezogenen Daten verwendet werden“. Die Insolvenzverwalterin wollte von mir wissen, ob sie die Akteneinsichtnahme durch die Studentin zu recht verweigert hatte.

Meine Antwort lautete: Ja. Denn die Einsicht in hinsichtlich des Arbeitnehmer- bzw. Patientenbezuges unanonymisierte Unterlagen der Gemeinschuldnerin ist rechtswidrig. Dabei kann es dahinstehen, inwieweit der Sächsische Datenschutzbeauftragte für die Verarbeitung personenbezogener Daten durch Insolvenzverwalter zuständig ist. Denn jedenfalls ist er für die Verarbeitung personenbezogener Daten durch die TU Dresden als öffentliche Stelle des Freistaates Sachsen zuständig; die Studentin wollte als Mitglied der TU handeln. Mit anderen Worten: Unabhängig davon, ob die *Gewährung* von Einsicht in die Unterlagen durch die Insolvenzverwalterin zulässig ist, ist es jedenfalls unzulässig, wenn sich die Universität von der Insolvenzverwalterin Informationen *zukommen lässt*.

(1) Die Zuständigkeit - und zugleich die Anwendbarkeit des Sächsischen Datenschutzgesetzes - für die Verarbeitung personenbezogener Daten durch Insolvenzverwalter wäre durch § 2 Abs. 2 Satz 1 SächsDSG begründet, wenn dieser *Aufgaben der öffentlichen Verwaltung* wahrnähme. Manches spricht in der Tat dafür, die Tätigkeit des Insolvenzverwalters als die Erfüllung einer von Hause aus eigentlich der staatlichen Rechtspflege zugehörigen Aufgabe anzusehen, die im Übrigen auch nicht „Rechtsprechung“ wäre, so dass die Zuständigkeit des Sächsischen Datenschutzbeauftragten nicht nach § 24 Abs. 2 SächsDSG ausgeschlossen wäre. Die Tätigkeit

des Insolvenzverwalters wird jedoch üblicherweise als die Ausübung eines *privaten Amtes* bezeichnet (Münchner Kommentar/Papier, 3. Auflage 1997, Rdnr. 132 zu § 839 BGB; Soergel/Siebert/Vinke, 12. Auflage 1999, Rdnr. 105 zu § 839 BGB; Häsemeyer Insolvenzrecht, 1992, 15. Kapitel, I 2 d) und damit rechtlich so eingeordnet wie der Rechtsanwalt und der vom Gericht beauftragte Sachverständige (vgl. auch Palandt/Thomas, Rdnr. 217 zu § 823, Rdnr. 30 zu § 839 BGB).

Bei Anwendbarkeit des Sächsischen Datenschutzgesetzes auf die Tätigkeit des Insolvenzverwalters wäre die mit der Gewährung der Einsicht verbundene Datenübermittlung mangels Erlaubnis schon deswegen unzulässig, weil nach den Angaben der Betreuerin der Zweck der Forschung durch die Verwendung anonymisierter Daten erreicht werden könnte (§ 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG). Unabhängig davon käme zudem ein aus dem Arztgeheimnis folgendes Übermittlungsverbot in Frage.

Selbst wenn man annimmt, dass aufgrund der in § 4 InsO ausgesprochenen Verweisung auf die ZPO der § 299 Abs. 2 ZPO nicht nur für das Konkursgericht, sondern auch für den Insolvenzverwalter gilt (vgl. Smid, Insolvenzordnung, 1999, Rdnr. 9 zu § 4), wäre das Ergebnis kein anderes. Denn die Vorschrift erlaubt eine Akteneinsicht nur auf der Grundlage eines *rechtlichen* Interesses; ein bloßes *berechtigtes* Interesse, wie es Forscher haben, ist nicht ausreichend. Das habe ich bereits in 8/5.8.2 anhand der Rechtsprechung ausführlich dargelegt.

(2) Geht man davon aus, dass der Insolvenzverwalter keine hoheitlichen Aufgaben übertragen bekommen hat, für ihn als nicht-öffentliche Stelle bei der Verarbeitung personenbezogener Daten also die Regeln des dritten Abschnittes des Bundesdatenschutzgesetzes gelten und damit keine Zuständigkeit des Sächsischen Datenschutzbeauftragten besteht, ist letztere im vorliegenden Fall doch unzweifelhaft insoweit begründet, als die Universität als öffentliche Stelle tätig ist. Dabei mag es dahinstehen, ob die forschenden Organisationseinheiten an den staatlichen Hochschulen vollständig an die Regeln gebunden sind, die für die Verarbeitung personenbezogener Daten durch öffentliche Stellen gelten. Jedenfalls aber sind die staatlichen Hochschulen insofern an das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 33 SächsVerf) gebunden, dass sie bzw. ihre Mitglieder nicht eine Verarbeitung personenbezogener Daten organisieren oder auf andere Weise veranlassen dürfen, die im Verhältnis zu den Betroffenen (Probanden, Versuchspersonen usw.) nach allgemeinen zivilrechtlichen Regeln rechtswidrig wäre. Unabhängig davon, ob die Daten durch die Hochschule selbst oder durch einen nicht bei ihr angestellten Doktoranden oder Diplomanden verarbeitet werden, besteht daher meiner Auffassung nach eine öffentlich-rechtliche, aus der Grundrechtsbindung der Hochschule als Organisation folgende Verantwortung der Hochschule betreffend die Tätigkeit derjenigen Hochschulbediensteten, die Forschung organisieren. Diese Verantwortung ist von dem zuständigen Hochschulorgan mittels Dienstrechts auszuüben.

Diese Verantwortung ist ähnlich derjenigen, die öffentliche Stellen trifft, welche die Forschung durch Dritte zulassen oder sonst fördern, und die sich bei der Befragung solcher Personen bedient, die in einem öffentlich-rechtlich begründeten Verhältnis zu der betreffenden öffentlichen Stelle stehen.

(3) Misst man demnach die von der Hochschule im vorliegenden Fall gewünschte Datenübermittlung durch die Insolvenzverwalterin an diesen allgemeinen zivilrechtlichen Maßstäben - deren Einhaltung ich insoweit inzidenter zu beurteilen habe, unbeschadet der insoweit primär bestehenden Zuständigkeit der Aufsichtsbehörde nach § 38 BDSG, also in Sachsen der Regierungspräsidien - kommt man zu einem negativen Ergebnis:

Auch die einschlägige Vorschrift des § 40 Abs. 3 Nr. 4 BDSG setzt nämlich voraus, dass die Durchführung des Forschungsvorhabens davon abhängig ist, dass die Daten insoweit personenbezogen sind. Das ist aber vorliegend gerade nicht der Fall: Die Identität der Patienten spielt nach den Angaben der Betreuerin gerade keine Rolle. Abgesehen davon müsste man meiner Auffassung nach auch insoweit, als die Abrechnungsunterlagen nicht vom Arztgeheimnis umfasst sind, einen Verstoß gegen vertragliche Pflichten und einen Eingriff in das allgemeine Persönlichkeitsrecht der Empfänger medizinischer Leistungen annehmen, wenn die Gemeinschuldnerin oder die Insolvenzverwalterin solche personenbezogenen Daten der TU Dresden bzw. der Studentin zur Verfügung stellt.

(4) Vor dem Hintergrund, dass die Unterlagen nicht anonymisiert waren und die Herstellung von Ablichtungen, in denen all das geschwärzt wird, was einen Rückschluss auf konkrete Arbeitnehmer und Patienten zulässt, angesichts des Umfanges der Unterlagen (nach den Angaben der Insolvenzverwalterin immerhin 20 Leitzordner) mit einem hohen Arbeitsaufwand verbunden gewesen wäre, habe ich der Betreuerin mitgeteilt, dass sich die Insolvenzverwalterin bereit erklärt habe, gegen Erstattung der damit verbundenen Kosten die Unterlagen entsprechend den Bedürfnissen der Studentin zu bearbeiten. Eine Stellungnahme seitens der Betreuerin oder der Studentin dazu, ob dies ein gangbarer Weg wäre, ist nicht erfolgt.

Nachdem sie mein Schreiben erhalten hatten, haben weder die Studentin noch ihre Betreuerin an dem Verlangen nach Einsicht in die Unterlagen festgehalten; eine Einsichtnahme ist also nicht erfolgt. Wie ich von der Betreuerin erfahren habe, ist das Vorhaben, eine Diplomarbeit zu dem oben genannten Thema anzufertigen, fallen gelassen worden. Man sieht, es gibt Konstellationen, in denen das Grundrecht der Wissenschaftsfreiheit dem Datenschutz weichen muss, insbesondere dann, wenn eine Lösung nach „praktischer Konkordanz“ abgelehnt wird.

13.3 Diskriminierende Behandlung eines Universitätsprofessors durch den damaligen Sächsischen Staatsminister für Wissenschaft und Kunst und einen Universitätsrektor

Wegen der Schwere eines Verstoßes gegen das Persönlichkeitsrecht musste ich mich im Berichtszeitraum mit einer förmlichen Beanstandung gemäß § 27 Abs. 2 SächsDSG an den Sächsischen Landtag wenden. Der Beanstandung lag folgender Sachverhalt zu Grunde:

Ein Universitätsprofessor für Kardiochirurgie hatte mich um eine datenschutzrechtliche Bewertung einiger ihn betreffender Presseauskünfte des SMWK gebeten. Den Presseauskünften lag eine Auseinandersetzung zwischen dem Petenten und dem SMWK wegen seines weiteren Einsatzes als Universitätsprofessor zu Grunde: Der Petent war unmittelbar nach seiner Ernennung unter Berufung in das Beamtenverhältnis auf Lebenszeit zum Universitätsprofessor vom SMWK „für die Dauer seiner Tätigkeit“ in einer privaten Fachklinik beurlaubt worden. Dem Aufsichtsrat des Trägervereins dieser Fachklinik gehörten als Vorsitzender der Sächsische Staatsminister für Wissenschaft und Kunst sowie als Mitglied der Rektor der Technischen Universität Dresden an.

Nach einer 6-jährigen Tätigkeit in dieser Fachklinik wurde der Petent im Frühjahr 2001 vom Insolvenzverwalter der zum 1. Januar 2001 angeblich in Insolvenz geratenen Klinik entlassen. Daraufhin wandte sich der Petent schriftlich an den Staatsminister für Wissenschaft und Kunst mit dem Ziel, gemäß seiner beamtenrechtlichen Stellung als Universitätsprofessor eingesetzt zu werden.

Im Mai 2001 erteilte der Pressesprecher des SMWK unter anderem die in groß aufgemachten Presseberichten der Tagespresse zitierten Auskünfte zur Entlassung des Petenten und zu den dienstrechtlichen Folgen dieser Entlassung, so zum Beispiel: „Wir prüfen gerade, ob einer, der als Klinikdirektor ungeeignet, nicht auch als C 4-Professor in der Lehre und Forschung untragbar ist“.

Wenige Tage später untersagte der SMWK per Bescheid dem Petenten die Führung seiner Dienstgeschäfte und erteilte ihm Hausverbot. Auch das wurde veröffentlicht. Erst vier Monate später wurde der Professor durch das SMWK angehört; einen weiteren Monat später erst wurde ein förmliches Disziplinarverfahren gegen ihn eingeleitet.

Die durch die Presseauskünfte öffentlich vorgenommen Diskreditierungen des Petenten durch das SMWK habe ich datenschutzrechtlich wie folgt bewertet: Die Auskünfte stehen als Übermittlung personenbezogener Daten unter Gesetzesvorbehalt.

Nach § 4 Abs. 1 Satz 1 SächsPresseG sind „alle Behörden (...) verpflichtet, den Vertretern der Presse (...), die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen, sofern nicht dieses Gesetz oder allgemeine Rechtsvorschriften dem entgegenstehen“.

§ 4 Abs. 2 SächsPresseG beschränkt jedoch den Auskunftsanspruch der Presse, und zwar in erster Linie aus Gründen des Persönlichkeitsschutzes: Presseauskünfte dürfen nur in jeweils nach den Umständen des Einzelfalles zulässigen Umfang erteilt werden. Nur soweit besondere Gründe im Einzelfall nicht entgegenstehen, dürfen öffentliche Stellen spontan oder auf Anfrage Auskünfte erteilen. Dies gilt selbst dann, wenn ein Vorgang der Presse bereits aufgrund anderer Quellen nicht mehr unbekannt ist oder sich eine Behörde rechtfertigen zu müssen glaubt. § 4 Abs. 2 SächsPresseG nimmt hierauf keine Rücksicht. Die Vorschrift stellt vielmehr klar, dass „entgegenstehende“ Normen des Persönlichkeitsschutzes den Auskunftsanspruch der Presse stets beschränken. In welchem Umfang dies der Fall ist, hängt dabei von den jeweiligen Umständen des Einzelfalles ab. Solche können zum Beispiel sein:

- Art und Ausmaß einer amtlich festgestellten Pflichtwidrigkeit des Betroffenen,
- Grad der Erkenntnis (Tatverdacht, hinreichender Tatverdacht, gesicherte Erkenntnisse),
- Verfahrensstadium (Vorermittlungen, Untersuchung, Hauptverhandlung),
- Rechtsstellung des Betroffenen (Beamter, Arbeitnehmer)
- Bekanntheitsgrad und Ansehen des Beschuldigten (absolute/relative Person der Zeitgeschichte, Unbekannter, untadeliger Ruf),
- Gewicht des betroffenen Rechtsgutes,
- Art und Ausmaß des vorhersehbaren Schadens aus der Berichterstattung für das Persönlichkeitsrecht bzw. materielle Rechtspositionen des Betroffenen.

Unter diesen Voraussetzungen waren die durch das SMWK erteilten Presseauskünfte nicht von der grundsätzlich gebotenen Zurückhaltung gekennzeichnet. Sie waren verfrüht, trotz vager Vermutungen zu konkret formuliert, sie waren zu weit gehend und damit rechtswidrig. Gleiches gilt für die Verteilung des SMWK-Schreibens, in dem dem Petenten die weitere Führung seiner Dienstgeschäfte verboten wurde, an den Insolvenzverwalter der Fachklinik und deren Notvorstand: Für deren geschäftliche Befassung mit der Angelegenheit hätte es ausgereicht, allenfalls die bloße Tatsache des - vorläufigen und nicht bestandskräftigen - Verbotes mitzuteilen. Die Übermittlung der Begründung war nicht erforderlich.

Es wäre vielmehr die vornehme dienstliche Pflicht des Staatsministers gewesen, sich in der Öffentlichkeit schützend vor seinen Beamten zu stellen (§ 99 Satz 2 SächsBG - aber wer ist noch vornehm). Er hätte die sorgfältige und unvoreingenommene Prüfung der seitens des Leitungsorgans der Fachklinik erhobenen Vorwürfe mitteilen und im übrigen Zurückhaltung üben müssen. So ist es auch in anderen Fällen üblich und

rechtmäßig, wenn Vorwürfe gegen Beamte laut werden. Grundlage der damaligen Presseauskünfte waren im wesentlichen in Zusammenarbeit mit dem Insolvenzverwalter gefundene, noch nicht gesicherte Mutmaßungen und Übertreibungen. Ein förmliches Ermittlungsverfahren oder eine förmliche Anhörung des Petenten hatte bis dahin nicht stattgefunden. Indem der Staatsminister sein Schreiben zum Verbot der Führung der Dienstgeschäfte und zum Hausverbot dem Pressesprecher, der TU Dresden, der Medizinischen Fakultät, dem Insolvenzverwalter sowie dem Notvorstand des die Fachklinik tragenden Vereins zuleiten ließ, beschädigte er das Persönlichkeitsrecht des Petenten schwer und nachhaltig. Dieser Rundumschlag, mit dem der Staatsminister intern zu haltende Dienstgeheimnisse - nämlich die Begründung des Verbotes der Führung der Dienstgeschäfte und des Hausverbotes - streute, ist durch nichts zu rechtfertigen.

Der Staatsminister verletzte damit seine Fürsorge- und Schutzpflichten nach § 99 SächsBG gegenüber dem Petenten. Die nach § 4 Abs. 2 SächsPresseG vorzunehmende Bewertung und Abwägung des Informationsanspruchs der Öffentlichkeit auf der einen Seite und der Fürsorge- und Schutzpflicht zugunsten des Beamten, des Petenten, auf der anderen Seite hätte zwingend geboten, Auskünfte auf nicht unmittelbar personenbezogene Aspekte zu beschränken. Das er dies gleichwohl nicht getan hat, erklärt sich wohl nur aus seiner besonderen persönlichen Interessenlage, die aus seiner „Doppelrolle“ folgt: Er war Dienstvorgesetzter im beamtenrechtlichen Sinn und zugleich Vertreter wirtschaftlicher und auch medizinischer Interessen als Aufsichtsratsvorsitzender des Fachklinik-Trägervereins. In dieser Doppelrolle konnte er augenscheinlich nicht die unterschiedlichen Maßstäbe erkennen, die er bei der Datenverarbeitung zu beachten hatte, dort öffentlich-rechtliche, da privatrechtliche Bindung. Insoweit zeigte der Vorfall schlaglichtartig die Verstricktheit des damaligen Staatsministers in die unterschiedlichen Sphären des von ihm verantworteten Konstrukts von öffentlichen und handfesten privatwirtschaftlichen Interessen. Damit musste der Staatsminister es persönlich verantworten, dass der Grundsatz einer datenschutzrechtlich gebotenen (§ 9 SächsDSG) sauberen Trennung solcher unterschiedlichen Funktionen, mit denen das Potenzial eines Interessenkonfliktes verbunden ist, unbeachtet blieb. Oder einfach gesagt: Der Staatsminister hat den Schutz eines Beamten seinen Interessen als Aufsichtsrat der Fachklinik geopfert.

Der heutige Staatsminister für Wissenschaft und Kunst hat sich - nachdem ihm die Sache bekannt wurde - klar vom Verhalten seines Vorgängers distanziert.

Das kollusive Wirken des damaligen Ministers und des Universitätsrektors zulasten des Medizinprofessors war zuvor von langer Hand geplant worden; der meiner Beanstandung zugrunde gelegte Sachverhalt war bloß das erste zu Tage getretene Glied in der Kette der gegen den Petenten gerichteten Diskreditierungsmaßnahmen, wie ich einige Monate später bei einer datenschutzrechtlichen Kontrolle im SMWK und im Rektorat der Technischen Universität Dresden feststellen musste. In einem Schrei-

ben des Rektors der TU Dresden, der - wie oben bereits dargelegt - ebenfalls dem Aufsichtsrat des Fachklinik-Vereins angehörte, an den Sächsischen Staatsminister für Wissenschaft und Kunst erachtete es der Rektor schon im September 2000 in Bezug auf Herrn Professor (...) „für erforderlich,

... disziplinarrechtliche Schritte des Dienstherrn gegen seinen Landesbeamten einzuleiten, dabei sollte man lieber zu weit gehen, als zu zaghaft sein,
... seine wissenschaftliche Leistung zu evaluieren und die Einhaltung seiner Lehrverpflichtungen zu überprüfen, möglichst durch offizielle Peers von außen,
... alle Möglichkeiten prüfen, ihn als Hochschullehrer zu beurlauben und ihm den Professoren-Titel abzuerkennen...!“

Dieses Schreiben fand ich in den Sachakten des SMWK zum Fachklinik-Trägerverein und als Entwurf in den Akten des Rektorats der TU Dresden.

Der Inhalt dieses Schreibens war recht einfach zu verstehen: Der Rektor stellt fest, dass der Medizinprofessor die Interessen des Rektors und des Staatsministers im Trägerverein störe, und er folgert daraus, dass von ihm und dem Staatsminister zu teilende gemeinsame Ziel, man solle diverse Schritte im Bereich des universitären Wissenschaftsbetriebes und im Bezug auf das Beamtenverhältnis unternehmen, um den Petenten offen zu diskreditieren und aus dem Amt zu bringen.

Die vom Rektor vorgeschlagenen Datenverarbeitungsschritte, ich habe sie als „Zersetzungsplan“ bezeichnet, waren rechtswidrig. Sie beruhten nicht auf dem Vorwurf eines beamtenrechtlich - dienstlichen (Fehl-)Verhaltens im Bezug auf die universitären Pflichten des Petenten, sondern auf der Verärgerung über seine angebliche Aktivität im Trägerverein der Fachklinik.

Diese rechtswidrige Datennutzung war darauf zurückzuführen, dass der Rektor wie der Staatsminister jeweils eine Doppelstellung eingenommen hatten. Dabei kann dahinstehen, inwieweit es im dienstlichen Interesse lag, dass sowohl der Staatsminister als Vertreter des Freistaates als auch der Rektor als Vertreter der TU Dresden das Angebot angenommen haben, Mitglied im Trägerverein zu werden. Die Übernahme dieser Mitgliedschaft konnte die Pflichten und Befugnisse, welche dem Rektor der Universität und dem zuständigen Staatsminister im Hinblick auf den Universitätsprofessor und Beamten in der Person des Petenten zukamen, nicht ändern. Beide, Rektor und Staatsminister, durften ihr Amt nicht in den Dienst des Trägervereins stellen, sie durften nicht Vereinsinteressen mit dem durch die Gesetze definierten Staatswohl verwechseln. Erst recht durften sie nicht ihrer öffentlichen Amtsbefugnisse zu besonderen Formen und Inhalten der Datenverarbeitung in den Dienst des Vereins stellen. Dies war ein schwerer Amtsmissbrauch, nämlich eine zweckwidrige Nutzung dienstlicher Datenverarbeitungsbefugnisse zu Zwecken eines privaten Vereins und zur Lösung der dortigen Querelen.

Die Informationspartner, also der Rektor und der Staatsminister, hatten beide amtliche Vorgesetzteneigenschaften gegenüber dem betroffenen Universitätsprofessor und Landesbeamten. Die übermittelten Daten hatten Personalaktenqualität im Sinne des § 117 Abs. 1 Satz 2 SächsBG; sie hätten zu den Personalakten genommen werden müssen. Es wäre die Pflicht dieser Vorgesetzten gewesen, den Beamten gemäß § 119 SächsBG „zu den Beschwerden, Behauptungen und Bewertungen, die für ihn ungünstig sind oder die ihm nachteilig werden können, vor deren Aufnahme in die Personalakte zu hören". Dennoch erfolgte im vorliegenden Fall die Übermittlung der Daten heimlich. Die Daten wurden nicht zur Personalakte genommen, der Beamte wurde weder informiert noch gehört.

Das Beamtengesetz verlangt vom Vorgesetzten Fairness und Achtung der Menschenwürde gegenüber dem betroffenen Beamten. Dazu gehört es, dass Vorwürfen - stehen sie einmal im Raum - unverzüglich nachzugehen ist. Der Sachverhalt ist in Kenntnis des Beamten aufzuklären, die rechtsstaatlichen Formvorschriften und Verfahrenssicherungen des Disziplinarrechts sind einzuhalten. Es ist ein grober und menschenrechtswidriger Verstoß gegen die Grundlagen des Beamtenrechts, Informationen über Vorwürfe gegen einen Beamten heimlich zu sammeln, deshalb schwerwiegende, das beamtenrechtliche Grundverhältnis zerstörende Verfahren zu erörtern, anzuregen oder zu planen und die dies betreffenden Daten in einer Sachakte zu speichern, sie quasi „auf Halde" zu legen, ohne dem Beamten die Chance zu geben, sich dazu zeitnah zu äußern. Derartige Datenspeicherungen sind Handlungsformen rechtsstaatsfernen Denkens.

Auch wenn der Rektor „nur" der Urheber der Anwürfe und nicht der Disziplinarvorgesetzte war - dies war der Staatsminister -, so handelte er dennoch in der Kenntnis und Absicht, die Datenverarbeitung (Erhebung, Auswertung, Speicherung) abweichend von den vorgenannten Rechtsvorschriften vorzunehmen. Aufgrund § 58 Abs. 2 Sächsisches Hochschulgesetz sind dem Rektor einige Vorgesetztenfunktionen über die Hochschulprofessoren übertragen. Er kannte die Vorschriften und wollte dennoch, dass sein Schreiben wie geschehen vom Staatsminister behandelt wurde - nämlich heimlich -, und das war auch seine Absicht. Anders lässt sich z. B. die Formulierung „dabei soll man lieber zu weit gehen, als zu zaghaft sein" nicht interpretieren.

In meiner Beanstandung, die ich ebenfalls dem Sächsischen Landtag vorgelegt habe, konnte der Rektor der TU Dresden nicht mit seiner Argumentation gehört werden, er habe seinerzeit „getrennt von der Funktion als Rektor der TU Dresden gehandelt". Es waren nicht nur die Äußerlichkeiten seines Schreibens - vom Briefkopf über die bei der Anfertigung eingesetzten Schreibkräfte und den Postweg bis zur Aufbewahrung des Schreibens in den Amtsräumen -, die es ein amtliches Schreiben sein lassen: Es war auch gerade der Inhalt, nämlich die Verquickung der Interna des Trägervereins mit der universitären und dienstrechtlichen Sphäre, die das Schreiben zu einer amtlichen Stellungnahme des Rektors der TU Dresden machte.

Ferner wandte der Rektor ein, seine Schlussfolgerungen hätten keinen Personenbezug aufgewiesen. Auch mit diesem Argument konnte er nicht gehört werden. Natürlich hat er mit seinem Brief personenbezogene Daten verarbeitet. Gerade seine Vorschläge und Schlussfolgerungen sind eine Verarbeitung personenbezogener Daten im Sinne des § 3 Abs. 1 und 2 des SächsDSG. Denn personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, ohne dass es darauf ankommt, ob diese Angaben wahr oder falsch sind, ob sie bereits Realität sind oder lediglich Zukünftiges betreffen, ob sie spekulativ oder irreal sind. Auch Fragestellungen oder Vergleiche gehören zur Kategorie der Einzelangaben über persönliche oder sachliche Verhältnisse. Dies ist in Fachkreisen unbestritten, aber auch sachgerecht, denn gerade spekulative oder unwahre Angaben sind besonders geeignet, das Persönlichkeitsrecht des davon Betroffenen zu berühren und zu verletzen. Pläne für künftige Vorhaben personenbezogener Datenverarbeitung gehören ihrerseits ebenfalls zu Kategorie personenbezogener Daten.

Als Maßnahme der nach § 26 Abs. 1 SächsDSG vorzunehmenden Mängelbeseitigung habe ich das SMWK aufgefordert zu prüfen, ob und inwieweit der Zersetzungsplan des Rektors damals insbesondere für die - bereits mehrfach gesondert beanstandete - Vorgehensweise des damaligen Staatsministers nachweislich ohne Einfluss blieb. Sollten keine nachweisbar gegen einen solchen Einfluss Tatsachen oder Beweisanzeichen vorliegen, wäre - schon aus Gründen der beamtenrechtlichen Fürsorgepflicht des Vorgesetzten - davon auszugehen, dass das spätere Vorgehen des damaligen Ministers gegen den Petenten durch den Rektor angeregt und mitverursacht, zumindest psychisch gestützt wurde. Die Rechtswidrigkeit des Vorgehens des Rektors kann dann auf die Führung und Entscheidung des Disziplinarvorgangs nicht ohne Folgen bleiben. Das hier beanstandete Schreiben sowie eine etwa dazu vorliegende Aufforderung des damaligen Ministers ist daher zu den Disziplinarakten zu nehmen. Dem betroffenen Beamten sind die dazu notwendigen Verfahrensrechte zu gewähren. Auch ist der Beamte ferner durch den Untersuchungsführer von einer Beanstandung zu unterrichten.

Ich habe diesem Punkt meines Tätigkeitsberichts diesen breiten Raum gegeben, damit die persönlichkeitsfeindlichen Tendenzen im Verwaltungshandeln in ihrem Ausmaß deutlich werden. Wenn Inhaber hoher Ämter nicht davon ablassen, ihre öffentlich verliehenen und privaten Funktionen zum Nachteil anderer Menschen zu verwechseln und zu missbrauchen, wird das Rechtsgefühl der Bevölkerung, d. h. das Vertrauen in die Rechtsordnung, aus Enttäuschung nicht gedeihen können. Schlechte Vorbilder. Umso angenehmer ist es, dass der jetzige Minister sich meiner Kritik im Grundsatz angeschlossen hat; gleiches gilt für eine Reihe Abgeordneter - quer durch die Fraktionen.

14 Technischer und organisatorischer Datenschutz

14.1 Organisatorische Aspekte beim Einsatz der elektronischen Signatur in der öffentlichen Verwaltung

Es geht in diesem Beitrag nicht um eine allgemeine Einführung in den Themenkreis „elektronische Signatur und Verwaltung“ – dazu verweise ich auf die aktuelle und ausführliche Schrift des BMWA „Rechtskonformes E-Government“ vom Februar 2003 (Abschnitt 6.3 bis 6.8) -, sondern um eine Behandlung problematischer Aspekte, die sich bei der Implementierung der elektronischen Signatur in der Verwaltung negativ auswirken können. Ausdrücklich sei gesagt, dass es nicht darum geht, elektronische Signatur zu verhindern, sondern darum, ihren Einsatz praktikabel in den Verwaltungsvollzug einzupassen.

Im Folgenden werde ich der Einfachheit halber nicht den Begriff „qualifizierte elektronische Signatur mit Anbieter-Akkreditierung“ verwenden, sondern von der „akkreditierten elektronischen Signatur“ reden. Auch benutze ich den gängigeren Begriff „Trustcenter“, den ich inhaltsgleich zum „Zertifizierungsdiensteanbieter“ (§ 2 Nr. 8 SigG) verwende.

Aufmerksam zu machen ist am Anfang ebenfalls auf den Umstand, dass kryptographische Verfahren sowohl bei der Signatur und bei der Kommunikationsverschlüsselung eingesetzt werden. Bei der Anbietung von Signaturzertifikaten sowie bei den entsprechenden Anwendungen sind in der Regel (meist als integraler Bestandteil) auch Komponenten zur Kommunikationsverschlüsselung enthalten. Eine – theoretisch mögliche - vollständige Trennung beider Komplexe ist deshalb sowohl bei der Planung als auch bei der späteren Endanwendung nicht machbar.

14.1.1 Vorgaben bei der Signatur

Zertifikatsinhaber
Das Signaturgesetz geht von der Grundlage aus, dass jede qualifizierte elektronische (damit insbesondere auch die akkreditierte) Signatur, die ja der Unterschrift gleichgestellt ist (§ 3 a Abs. 2 VwVfG, § 126 a ff. BGB, s. a. § 6 Abs. 2 SigG), immer einer natürlichen Person zugeordnet ist. Der Prozess der Vergabe einer solchen Signatur (des Zertifikates) geht nach einem klar festgelegten Rahmen vor sich. Zu diesem gehören eine Feststellung der Identität der Person des Antragstellers durch das Trustcenter, ein genau definierter Prozess der Herstellung der Karte und die sichere Aushändigung der Karte und der PIN direkt an den Besitzer. Veränderungen in diesem Prozess bedürfen der Absprache mit dem Trustcenter und sind schwer durchsetzbar, weil das Verfahren rechtlich vorgegeben ist.

Behördenbezug
Organisationsbezogene Merkmale (z. B. Behördenzugehörigkeit, Vertretungsregelungen) lassen sich nur innerhalb des Hauptzertifikates (vergleichbar mit dem Stammdatensatz) oder im so genannten Attributzertifikat erfassen. Letzteres lässt sich ohne Änderung des Hauptzertifikates ändern, allerdings auch nur über das Trustcenter. Das Hauptzertifikat kann nur gesperrt werden. Bei notwendigen Veränderungen muss ein neues beantragt werden. Deshalb wird in der Regel empfohlen, möglichst wenig Daten innerhalb des Zertifikates zu speichern (Identifikationsdaten und Behördenzugehörigkeit), um notwendige Änderungen gering zu halten, denn diese sind sowohl mit Kosten- als auch mit Zeitaufwand verbunden.

Eine rein organisationsbezogene akkreditierte elektronische Signatur ist nicht möglich.

Beweiskraft der Signatur
Die Frage der Beweiskraft der elektronischen Signatur innerhalb der Rechtssprechung wird sich im Laufe der Zeit noch deutlicher zeigen. Zumindest bei Verwaltungsakten, die Schriftlichkeit erfordern, ist die akkreditierte Signatur ein entsprechendes Äquivalent für die Unterschrift. Bei niedrigeren Formen der elektronischen Signatur, z. B. der fortgeschrittenen elektronischen Signatur, kommt es auf die Würdigung der Gesamtumstände an. Dem Gericht muss die Gesamtheit der getroffenen Maßnahmen vorgelegt werden.

Trustcenter
Trustcenter sind in der Regel (bisher ausschließlich) private Unternehmen. Dies bietet den Vorteil des Wettbewerbes, schließt aber auf der anderen Seite alle Nachteile mit ein, die darin liegen, dass ein solches Unternehmen den marktwirtschaftlichen Risiken ausgesetzt ist. Da die Errichtung und Pflege eines Trustcenters mit einem gehörigen technischen und finanziellen Aufwand verbunden ist, sind die erbrachten Leistungen angemessenerweise auch nicht billig. Hinzu kommt, dass die auf der Seite des Anwenders liegenden Leistungen (Einbinden der elektronischen Signatur in die eigene IT-Welt) nicht im Grundpaket eines Trustcenters enthalten sind, sondern in der Regel von – meist mit dem Trustcenter verbundenen – Drittfirmen erbracht werden. Für den Konkursfall hat das Signaturgesetz zwar Vorkehrungen vorgesehen. Allerdings lässt sich damit das Risiko des Anwenders nicht ausräumen. Er kann zwar die bisher angeschafften Karten und Geräte auf dem erreichten Stand weiterverwenden. Eine Weiterentwicklung ist jedoch nicht möglich. Auch die Interoperabilität mit Produkten anderer Hersteller ist derzeit noch nicht gegeben. Hier wird hoffentlich die weitere Entwicklung Abhilfe schaffen.

Gültigkeit der Signatur
Elektronisch signierte Dokumente müssen signiert aufbewahrt werden; ansonsten verliert die elektronische Signatur ihre Gültigkeit. Den schriftlichen beglaubigten Ausdruck elektronisch signierter Dokumente regelt § 33 Abs. 4 VwVfG.

Im Unterschied zur Unterschrift haben elektronische Signaturen verfahrensbedingt eine Verfallsdauer. Wenn durch die technische Entwicklung die Möglichkeit existiert, dass sich der bei einer elektronischen Signatur verwendete Schlüssel innerhalb einer absehbaren Zeitspanne „knacken" lässt, so ist dieser Schlüssel nicht mehr sicher. Derzeit wird nach der Bekanntmachung der RegTP zur elektronischen Signatur (Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Bundesanzeiger Nr. 48, v. 11.03.2003, S. 4202 bis 4203) von einer Geltungsdauer der Schlüssel von mindestens 6 Jahren ausgegangen. Korrespondierend legt deshalb § 14 Abs. 3 SigV die Gültigigkeitsdauer eines qualifizierten Zertifikates auf maximal fünf Jahre fest. Ist die Gültigkeit der Signatur nicht mehr gewährleistet, ist ein digital signiertes Dokument (bzw. vorgegebene Teile davon) neu zu signieren oder es ist auszudrucken und zu beglaubigen. Ansonsten verliert es seine Signierung und die damit einhergehende Beweiskräftigkeit. Dieses Verfahren lässt sich mit einem gewissen Aufwand durch die Verwaltung bewerkstelligen. Ein Bürger, der gelegentlich und nicht geschäftsmäßig mit der Verwaltung kommuniziert, ist damit technisch überfordert. Dies bedeutet, dass auch abgesandte elektronisch signierte Dokumente durch die Verwaltung aufbewahrt werden sollten.

Einbettung in Verfahren
Bei der Signierung eines Dokumentes sind Vorgaben einzuhalten. § 17 Abs. 2 SigG schreibt vor, dass nur solche Signaturanwendungskomponenten eingesetzt werden können, „die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht." Demzufolge ist für jedes einzelne zu signierende Dokument eine spezielle Signierungshandlung durch den Signierenden zu vollziehen und zwar unter Kenntnis des Inhaltes. In der o. g. Schrift „Rechtssicheres E-Government" (S. 89) werden so genannte Signaturserver oder Sicherheitsboxen erwähnt. Diese böten als Alternative zu eine chipkartenbasierten Signaturerzeugung eine Möglichkeit der Zentralisierung des Signaturvorganges und eine Massenabfertigung von Dokumenten. Aber auch hier ist eine automatische Signierung nicht gestattet.

Praktikabilität
Kritische Fragen bei Normaleinsatz ergeben sich derzeit noch in Detailfragen des Einsatzes. Wie sieht es mit der physischen Stabilität der Karten aus (Bruchfestigkeit, äußerer Verschleiß)? Wie kann man sich bei Kartenverlust absichern? Ist die derzeitige Sperrung nach 3-maligen Fehlversuch, die zwingend zur Anschaffung einer neuen Karte führt, handhabbar? Welche Zeitspanne vergeht, bis man eine Ersatzkarte erhält (ein Arzt, der seine Karte verloren hat, kann nicht 8 Wochen warten, bis er eine neue erhält und in der Zwischenzeit keine Befunde und Arztbriefe signieren!)?

Besitz
Das Signaturgesetz geht von einem Vertragsverhältnis zwischen Zertifikatsinhaber und Trustcenter aus. Eine Behörde kann nur Einfluss auf die Merkmale und Attribute

nehmen, für die sie zuständig ist, die sie also bestätigen muss oder die sie sperren kann. Da der Inhaber aber stets eine natürliche Person ist, kann die Behörde nicht Antragsteller für die Zertifikate der Bediensteten und auch nicht Besitzer der Karte mit den Signaturschlüsseln sein. Selbst das Trustcenter zieht nicht die Karte sein, sondern sperrt nur das Zertifikat (d. h. bei einer Überprüfungsabfrage im Trustcenter wird mitgeteilt, dass die Gültigkeit des Zertifikates erloschen ist). Dies erfordert bei einem dienstlichen Einsatz der akkreditierten Signatur die ständige Pflege und Aktualisierung der Attribute durch die Personalverwaltung, um zum einen möglichen Missbrauch (z. B. bei Entlassung), aber auch die Ungültigkeit von Verwaltungsakten (z. B. bei Versetzung und noch andauernder Verwendung eines Zertifikates mit der alten Behördenbezeichnung) zu verhindern. Zusätzlich gibt es noch gravierende Erschwernisse bei gleichzeitiger Verwendung als Sichtausweis. Da eine Signaturkarte Eigentum des Zertifikatsinhabers ist, kann sie nicht eingezogen werden. Verbunden mit der Frage des Besitzes ist die Frage der Finanzierung. Derzeit bestehen die Angebote der Trustcenter aus zwei Bestandteilen, den einmaligen Anschaffungskosten und den weiteren Pflegekosten (für das Vorhalten der Überprüfungsmöglichkeit im Trustcenter). Hier stellt sich die Frage, wer beim Anschaffen zahlt (der Bedienstete mit Kostenerstattung?) Wie sieht die weitere Bezahlung aus, z. B. bei Versetzung oder Verlassen der Behörde? Können Bedienstete in solchen Fällen privat (nach Sperrung der dienstlichen Attribute) ihre elektronische Signatur weiter nutzen, wenn sie die Kosten tragen? Generell ist hier wohl über finanzielle Rahmenverträge zwischen Behörde und Trustcenter nachzudenken, in die die Bediensteten dann eintreten können.

14.1.2 Vorgaben bei der Organisation

Bei der Einführung IT-gestützter Verfahren ist die Verwaltung herausgefordert, das bisherige Verwaltungshandeln zu überdenken und anzupassen, aber auf der anderen Seite bewährte Grundsätze nicht einfach „über den Haufen zu werfen“. Es kann kein „Diktat der Informationstechnik“ geben, sie ist Dienstleister und bietet Hilfestellung und Verbesserung. Die Einführung der elektronischen Signatur, die ja als Äquivalent zur Unterschrift eingesetzt werden soll, greift tief in das Verwaltungsgeschehen ein. Es ist deshalb zu prüfen, inwieweit

- *der Informations- und Entscheidungsfluss innerhalb der Verwaltung und die damit verbundene Unterschriftsberechtigung abgebildet werden kann.*
  Wer signierte Dokumente verschickt, muss (zur Überprüfung der Signatur) auch den öffentlichen Signaturschlüssel seines Zertifikates allgemein zugänglich machen. Derzeit ist damit auch die Bereitstellung des öffentlichen Schlüssels zur Kommunikationsverschlüsselung verbunden. Benutzt der Empfänger eines signierten (und in der Regel auch verschlüsselten) Dokumentes für seine Antwort diese Schlüssel des Versenders und verschlüsselt seinerseits das Antwortdokument, so kann kein anderer Bediensteter dieses Dokument entschlüsseln, es sei denn,

er ist im Zertifikat des Versenders als Vertreter benannt. Dies bedeutet, dass die Dienststelle in einem solchen Fall nur noch „persönlich-vertrauliche“ Post erhält, die niemand anders als der Bedienstete selbst öffnen kann. Sämtliche bisherige Steuerungen durch Poststelle und Organisationshierarchien wie Abteilungs- und Referatsführung wären ausgehebelt. Das kann ja wohl nicht sein.

- *für die Gültigkeit des Verwaltungshandelns die akkreditierte elektronische Signatur notwendig ist.*
  Eine Vielzahl von Verwaltungsunterlagen ist bereits jetzt ohne Unterschrift gültig. Entscheidend ist, ob Schriftlichkeit verlangt ist. Nur dort wäre die qualifizierte oder gar die akkreditierte elektronische Signatur notwendig (zum Unterschied zwischen qualifizierter elektronischer Signatur und akkreditierter Signatur vgl. die Tabelle auf S. 69 bis 71 in „Rechtskonformes E-Government“).

- *es auf den Personenbezug eines Dokumentes oder eines Verwaltungsaktes ankommt*
  Für die Gültigkeit eines schriftlichen Verwaltungsaktes, ist in der Regel nicht ausschließlich die Unterschriftsleistung des Behördenleiters notwendig, sondern diese Unterschriftsleistung kann delegiert werden. Entscheidend ist, dass er als Schreiben der Behörde erkennbar ist und die Unterschrift eines Bediensteten trägt, der in der Auftragshierarchie steht. Das Verwaltungsverfahrensgesetz hat dies auch auf elektronische Dokumente übertragen (§ 37 Abs. 3 VwVerfG). Dies ist die Regel. Nur in wenigen Fällen (z. B. bei der Befundung durch Ärzte im Krankenhaus) kommt es im Außenverhältnis nicht auf die Stelle, sondern auf die wirklich damit befasste Person an, die deshalb persönlich zu signieren hat.

- *Personalmaßnahmen abbildbar sind*
  Personalmaßnahmen, die zum ständigen Geschäft einer Personalverwaltung gehören, wie z. B. Versetzung, Vertretung, Ausscheiden, müssen mit vertretbaren Aufwand auch bei der elektronischen Signatur eingepflegt werden können. Die im Falle der Verwendung der akkreditierten elektronischen Signatur für eine Vielzahl von Bediensteten ständig notwendige Kommunikation mit einem Trustcenter ist m. E. durch die Personalverwaltung nur schwer umsetzbar und wohl auch mit erheblichen Kosten (Neubeantragung oder Sperrung von Zertifikaten!) belastet.

Weithin wird bei der Einführung der elektronischen Signatur wegen der populären Gleichstellung mit der Unterschrift immer davon ausgegangen, dass jeder Bedienstete ein akkreditiertes Zertifikat besitzen müsse, da er ja auch unterschreiben müsse. Dieses Postulat ist in Frage zu stellen, ansonsten wäre der normale Verwaltungsvollzug selbst in Frage gestellt. Die akkreditierte elektronische Signatur ist ferner als innerbehördliches Statussymbol völlig ungeeignet.

14.1.3 Umsetzung

Die oben beschriebenen Voraussetzungen lassen für mich nur eine einzige mögliche Lösung zu: die Beschränkung des Einsatzes der akkreditierten elektronischen Signatur auf die Fälle, wo sie wirklich notwendig ist; ansonsten die Verwendung der fortgeschrittenen elektronischen Signatur (§ 2 Abs. 2 SigG) in der Verwaltung.

Dies ließe sich in folgendem Modell verwirklichen:

- In einer Behörde existiert eine *Signaturstelle*, über die alle einlaufenden elektronisch signierten und alle auslaufenden zu signierenden Dokumente gehen. Sie besteht aus mehreren Mitarbeitern, so dass bei Abwesenheit oder Ausscheiden eine Ent- und Verschlüsselung sowie eine Signierung möglich ist. Nur diese Mitarbeiter befinden sich im Besitz einer *akkreditierten* elektronischen Signatur mit gegenseitigen Vertretungsregelungen und Behördenattributen. Alle eingehende Post wird von ihnen entschlüsselt und signaturüberprüft; alle ausgehende Post von ihnen nach Überprüfung der internen fortgeschrittenen Signaturen (Wer hat was unterzeichnet?) signiert, verschlüsselt und verschickt. Nur ihre Schlüssel werden (de facto als organisationsbezogene Schlüssel) veröffentlicht.

- *Innerhalb* der Behörde wird ansonsten mit einer *fortgeschrittenen* Signatur gearbeitet. Diese kann kompatibel zur akkreditierten Signatur der Signaturstelle gestaltet werden. Sie wird ausschließlich intern verwendet. Ihre Schlüssel werden nicht veröffentlicht.

Ausnahmen von diesem Grundsatz bestehen nur dort, wo es auf die direkte Signatur durch den Bearbeiter ankommt). Hier darf allerdings bei Außenwirkung nur die elektronische Signatur, nicht die Verschlüsselung verwendet werden. Sollte auch diese notwendig sein z. B. bei ärztlichen Befunden, so muss der erhöhte Aufwand in Kauf genommen werden und die technischen Schutzmaßnahmen sind an den Empfangsplatz zu verlagern.

Rechtlich führt dieses Modell zu keinen Einschränkungen, denn beim Verwaltungsakt kommt es darauf an, dass das Zertifikat „die erlassende Behörde erkennen lassen“ muss (§ 37 Abs. 3 VwVfG). Dies ist durch die Signaturstelle gewährleistet, deren Bedienstete als Beauftragte des Behördenleiters tätig würden. Sie brauchen – bevor sie ein Dokument signieren, evtl. verschlüsseln und versenden - zu ihrer Absicherung das Vorliegen der entsprechenden internen fortgeschrittenen Signaturen der Unterzeichnungsberechtigten. Diese internen fortgeschrittenen Signaturen bleiben bei der Verwendung der akkreditierten elektronischen Signatur erhalten und lassen sich ggf. bei einem gerichtlichen Verfahren durch eine geeignete Dokumentation nachweisen.

Organisatorisch bietet dieses Modell mehrere Vorteile:

- Der Aufwand bei der Verwaltung der akkreditierten elektronischen Signaturen, die ausschließlich bei der Signaturstelle vorhanden sind, bleibt gering.
- Der bei einer akkreditierten elektronischen Signatur notwendige zusätzliche finanzielle Aufwand beschränkt sich auf die Signaturstelle.
- Die Risiken beim Einsatz eines privaten Externen (Trustcenter) minimieren sich.
- Der Einsatz der fortgeschrittenen Signatur im inneren Bereich der Behörde kann frei gestaltet werden. Er unterliegt nicht den rechtlichen Beschränkungen der akkreditierten Signatur. Es ist keine ständige Kommunikation mit einem externen Trustcenter notwendig. Die Finanzierung kann unkomplizierter gestaltet werden. Der Besitz der Karte (Behördenausweis!) durch die Behörde und die damit verbundene Hoheit über die Karte ist möglich. Der Aufbau und die Verwendung kann entsprechend den eigenen Organisationsformen ausgestaltet werden. Veränderungen können zeitnah gepflegt werden (z. B. bei Verlust), Abbildung von Vertretungsregelungen und Verwendung wirklicher organisationsbezogener Signaturen ist möglich.
- Technische Schutzmaßnahmen für eingehende elektronische Post lassen sich noch aufrecht erhalten. Bei einer Verschlüsselung bis an den Arbeitsplatz wären sie ausgehebelt.

Damit gekoppelt und notwendiger Bestandteil dieses Modells ist ein bei der virtuellen Signaturstelle angesiedeltes zentrales Archiv aller eingehenden und ausgehenden elektronisch signierten Dokumente. Nur so kann die notwendige Gültigkeit der Dokumente gesichert werden. Sowohl die einzelnen Organisationseinheiten wie der mit der Verwaltung kommunizierende Bürger wären mit den notwendigen technischen Vorkehrungen (s. o.) überfordert.

Aus datenschutzrechtlichen Gründen – auf der einen Seite Sicherung der Vertraulichkeit und Authentizität , die zum Einsatz der akkreditierten Signatur führen, auf der anderen Seite aber Sicherung der Verfügbarkeit, der Transparenz und der Integrität, die in diesem kombinierten Modell möglich ist – sehe ich nur bei der Berücksichtigung dieser Aspekte die realistische Chance für ein Gelingen der Einführung der elektronischen Signatur in der Verwaltung.

14.2 Hochwasserhilfe - Datenbank PHOENIX

14.2.1 Entstehung

Schon während der Flutkatastrophe im August 2002 wurden erste Hilfeleistungen verteilt. Schnell wurde klar, dass die Spenden- und Fördermittelverteilung an die

von der Katastrophe Betroffenen rechtlich und technisch angepackt werden musste. Ich wurde vom Landrat des Kreises Grimma, der ein erstes Spendenverteilungsprogramm entwickelt hatte, auf dieses Problem angesprochen. Zeitgleich kam die Leitstelle „Wiederaufbau“ in der Staatskanzlei mit der Bitte um Beratung auf mich zu, die ihrerseits bereits mit dem DRK-Landesverband Kontakt hatte. Dieser setzte ein Programm ein, das technisch auf der Mitgliederverwaltung des Landesverbandes beruhte. Da von Anfang an bei allen Beteiligten klar war, dass die staatliche Spendenverteilung in Sachsen koordiniert mit den vielen anderen öffentlichen und privaten Spendenaktionen erfolgen sollte, musste eine landesweit einsetzbare IT-Lösung geschaffen werden. Schnell zeigte sich, dass die Brandenburger Erfahrungen mit dem Oderhochwasser sich nicht eigneten, da die Dimensionen beider Katastrophen zu sehr unterschiedlich voneinander waren. Nach einer Prüfung der beiden bisher bekannten IT-Lösungen (Landkreis Grimma und DRK) fiel die Entscheidung, das Programm des DRK weiterzuentwickeln, da es technisch besser für einen überregionalen Einsatz geeignet war. Die in Grimma gewonnenen Erfahrungen flossen jedoch in diese Arbeit maßgebend ein. In einem Kraftakt brachte ein kleines Team - der zuständige Referent in der Staatskanzlei, der Landesgeschäftsführer des DRK, der Direktor der SAKD und mein Stellvertreter - unter Mitwirkung der Firma, die die ursprüngliche Mitgliederverwaltung des DRK entwickelt hatte, sechs Wochen nach der Flut eine tragfähige und landesweit einsetzbare Lösung zum Laufen. In den nachfolgenden Wochen und Monaten hat das Team in ständiger Rückkopplung mit den Nutzern eine IT-Anwendung erarbeitet und entwickelt, die ihre Bewährungsprobe mit Bravour bestanden hat. Dass die Auszahlung weitgehend transparent und zügig erfolgte, liegt nicht zuletzt auch an der technischen Infrastruktur, die so schnell dafür vorhanden war. Auf gewisse Probleme, die hauptsächlich der drängenden Lage am Anfang geschuldet waren, werde ich im Folgenden eingehen.

14.2.2 Datenschutzrechtlicher Rahmen

In der Datenbank PHOENIX (*P*rogramm zur *H*ilfe und zur *O*rganisation *e*ines *N*euaufbaus *i*m *K*atastrophenfall in *S*achsen) werden Daten unterschiedlicher öffentlicher und nicht-öffentlicher Stellen, die im Zusammenhang mit dem Hochwasser Leistungen an Betroffene erbringen, verarbeitet. Dabei werden zum einen personenbezogene Daten bei Betroffenen erhoben, zum anderen solche Daten bei anderen Stellen, also Dritten, erhoben bzw. dorthin übermittelt (nichts anderes ist datenschutzrechtlich die Nutzung einer gemeinsamen Datenbank).

Eine rechtliche Spezialgrundlage für diese Datenverarbeitung existiert nur in einigen Fällen; ansonsten kommt das jeweilige datenschutzrechtliche Auffanggesetz zur Anwendung - für sächsische öffentliche Stellen das Sächsische Datenschutzgesetz, für die Diakonie das „Kirchengesetz über den Datenschutz der Evangelischen Kirche in

Deutschland (DSG-EKD)“, für die Caritas die „Anordnung über kirchlichen Datenschutz - KDO“, für die übrigen Stellen das Bundesdatenschutzgesetz.

Bei der o. g. Datenverarbeitung sind drei Fälle zu betrachten:

1. Will eine öffentliche Stelle Spenden verteilen, muss sie wissen, wer bedürftig ist. Die Stelle erhebt Daten direkt beim Betroffenen. Dies tut sie entweder aufgrund einer spezialgesetzlichen Grundlage (z. B. die Fördermittel verwaltenden Stellen nach § 44 SäHO) oder nach § 11 Abs. 2 SächsDSG, wenn sie diese Daten zu ihrer Aufgabenerledigung braucht (§ 11 Abs. 1 SächsDSG, z. B. bei Verteilung von Spenden).

2. Will eine öffentliche Stelle Spenden verteilen, so muss sie - wegen der Gerechtigkeit - wissen, welcher Empfänger schon etwas von Dritten bekommen hat. Die Stelle erhebt dann Daten bei Dritten. Dies kann sie beim Vorhandensein einer spezialrechtlichen Grundlage tun (z. B. § 4 Abs. 1 SächsFöDaG). Falls der Dritte selbst eine öffentliche Stelle ist, setzt dies in der Regel eine entsprechende Übermittlungsvorschrift von Seiten des Dritten voraus (z. B. § 6 SächsFöDaG). Existiert keine spezialgesetzliche Grundlage, so ist § 11 Abs. 4 SächsDSG (und natürlich ebenfalls Abs.1) zu beachten. Für den vorliegenden Fall kommt nur Nr. 2 – die Einwilligung des Betroffenen – in Betracht. Personenbezogene Daten von Hochwasseropfern können also mit deren Einwilligung von den leistungserbringenden Stellen bei Dritten erhoben werden.

3. Andere Spendenverteiler fragen aber auch ihrerseits bei der öffentlichen Stelle nach, welcher Bedürftige von wem bereits wie viel bekommen hat. Darüber muss - für alle ausreichenden Stellen offen - „Buch geführt“ werden. Für diesen Fall muss für die öffentliche Stelle eine Rechtsgrundlage gefunden werden (besser: existieren), die zur Datenübermittlung befugt. Sofern keine spezialrechtliche Regelung existiert, sind für eine Übermittlung an Dritte die §§ 13 bis 15 SächsDSG zu beachten. Diese gehen für den vorliegenden Fall alle drei in einer Verweiskette auf § 11 Abs. 4 SächsDSG zurück (die in § 14 SächsDSG verlangte Feststellung des SMK liegt für Caritas und Diakonie vor). Eine Übermittlung an andere Stellen ist demnach zulässig, wenn die gleichen Voraussetzungen wie bei einer Erhebung bei Dritten vorliegen, also wenn der Betroffene eingewilligt hat. Eine entsprechende Formel wurde mit Ausnahme des SAB-Antrages (der bereits vorbildlich schnell veröffentlicht war; hier ging Schnelligkeit in der Tat vor Genauigkeit!) für die Beseitigung von Hochwasserschäden bei kleinen und mittelständigen Unternehmen (KMU) bei allen mir vorliegenden Antrags- und Erfassungsformularen der an PHOENIX beteiligten Stellen eingefügt. Dabei war zu beachten, dass die Einwilligung in die Datenübermittlung auch gegenüber dem Empfänger der Übermittlung - der nach Fall 2 erhebenden Stelle – abgegeben werden kann.

Zusammenfassend ist festzustellen, dass für eine Bearbeitung in der Datenbank PHOENIX in jedem Fall die Einwilligung der Betroffenen notwendig war. In Absprache mit mir sind durch die „Leitstelle Wiederaufbau“ der Staatskanzlei für Erfassungs- und Antragsformulare sowohl für einen Datenabgleich mit der Versicherungswirtschaft als auch für einen Datenabgleich mit erhaltenen Spendenleistungen folgende Formulierungen vorgeschlagen worden:

„Ich willige ein, dass die Versicherungsgesellschaften, von denen ich Leistungen in Zusammenhang mit einer durch das Hochwasser verursachten Schadensregulierung erhalten habe oder gegenüber denen ich im Zusammenhang mit dem Hochwasser Ansprüche auf Schadensregulierung erworben habe, den zuständigen öffentlichen Stellen im Freistaat Sachsen die Höhe der erbrachten Leistungen sowie die Höhe der bestehenden Ansprüche mitteilen.

Ich bin darüber informiert worden, dass die hier erhobenen Daten für die Antragsbearbeitung verwendet werden und stimme der Verwendung dieser Daten zum Abgleich mit anderen Zuwendungs- und Leistungsgebern ausdrücklich zu.“

Zu beachten war und ist (!), dass andere Stellen die Daten für andere Zwecke (z. B. die Finanzämter für steuerrechtliche Angelegenheiten) nur dann erhalten können, wenn die Betroffenen in eine solche zweckändernde Verarbeitung eingewilligt haben, sonst nicht!

14.2.3 Die Datenbank

Vorgaben
Die im Verein „Sachsen helfen“ organisierten und an der Spendenverteilung beteiligten Stellen hatten sich geeinigt, koordiniert und aufeinander abgestimmt vorzugehen. Damit standen wir - d. h. das Team (SK, DRK, SAKD und SächsDSB) - vor der Aufgabe, eine IT-Lösung zu entwickeln, die mehrere Bedingungen erfüllen musste:
- die Zahl der Betroffenen stieg ständig; es war von Zehntausenden auszugehen,
- ebenso stieg die Zahl der beteiligten Stellen; eine feste Nutzergruppe bestand nicht, die eingesetzten Mitarbeiter wechselten,
- die IT-Ausstattung der Stellen bewegte sich auf unterschiedlichem Niveau,
- die Bearbeitung musste in Echtzeit erfolgen; lokale Zwischenspeicherungen waren nicht möglich, ansonsten hätte es Diskrepanzen bei der Bearbeitung ein und desselben Antrages durch verschiedene Stellen geben können,
- es gab unterschiedliche Einsatzprofile, sowohl stationäre wie mobile Bearbeitung; dies hatte Auswirkungen auf die Performance, d. h. auf Schnelligkeit und Handhabbarkeit des Programms,
- die Lösung musste schnell implementierbar sein,
- bereits vorhandene Datensammlungen mussten importiert werden,

- das Datenmodell musste die Grundanforderungen aller Beteiligten – die durchaus unterschiedliche Bearbeitungskriterien hatten – erfüllen,
- eventuell notwendige Änderungen mussten schnell eingearbeitet werden können.

Technische Realisierung und Zugang
PHOENIX wurde dann eine klassische Application-Service-Providing-Lösung auf MySQL-Basis, die vollständig auf einem zentralen, durch das DRK gemanagten Server lief. Die Benutzer konnten mittels eines Browsers auf den Server zugreifen. In Anbetracht der Dringlichkeit und unter Beachtung dessen, dass § 9 Abs.1 SächsDSG *angemessene* Maßnahmen zur Gewährleistung des Datenschutzes verlangt, habe ich angesichts der notwendigen schnellen Realisierung und des begrenzten Einsatzzweckes Folgendes vorgeschlagen:

„1. Zugriffskonzept

In der Datenbank müssen sich Zugriffsrechte sowohl nutzerbezogen gestaffelt (bis auf die Gemeindebene hinunter) als auch objektbezogen (Ausblendung einzelner Datenfelder, Beschränkung der Auswertbarkeit) realisieren lassen. Die Vergabe von Nutzerkennungen muss in der Anwendung nicht personenbezogen sein, sondern kann über pauschale organisationsbezogene Gastzugänge geschehen. Die Personenbeziehbarkeit der Zugänge ist in der Organisation schriftlich festzuhalten.

2. Übermittlung der Daten

Bei einer Webanbindung ist eine SSL-Verschlüsselung einzusetzen.

3. Ende der Verarbeitung

Die Benutzung der Datenbank ist zeitlich dadurch begrenzt, dass sie verwendet werden darf, solange sie der Aufgabenerfüllung dient. Es ist klar die Verantwortlichkeit festzulegen, wer über diesen Zeitpunkt entscheidet. Die Daten der beteiligten Organisationen sind dann zu trennen und zurückzuführen. Sollten in diesem Zusammenhang Datenübermittlungen vorgesehen sein, weise ich darauf hin, dass diese einer gesetzlichen Grundlage bedürfen."

Die Punkte 1 und 2 wurden so umgesetzt; Punkt 3 wird so erfolgen.

Datenmodell und Programmstruktur
Bereits am Anfang zeigte sich, dass eine Ausrichtung auf die Adresse der Antragsteller/Betroffenen eine Sackgasse war. Ausgangspunkt und einzige Konstante war vielmehr der Schadensort (mit Höhe und Art des Schadens), der dann auch zur Grundlage des Datenmodells wurde. Er wurde mit den Daten des Antragstellers verknüpft. Sowohl

beim Antragsteller als auch beim Schadensort erfolgte eine Weiterverzweigung. Hinter dem Antragsteller/Betroffenen standen die weiteren Familienangehörigen und soziale Angaben, die für die Spendenverteilung wichtig waren, wie z. B. das Haushaltseinkommen.

In die Datenbank gelangt der Nutzer nur mit der Eingabe eines bestimmten Betroffenen. Ist der Betroffene bereits in der Datenbank erfasst, wird der Datensatz angezeigt, ansonsten ein neuer angelegt. Die Suche erstreckt sich in diesem Fall auch über die Familienangehörigen. Damit werden Doppelerfassungen von Personen einer Familie vermieden.

An den Schadensort angehängt wurden die Leistungen, an diese wiederum die Leistungserbringer. Gewährleistet wurde über Zugriffsrechtsvergabe, dass die Leistungen nur vom jeweiligen Leistungserbringer schreibend bearbeitet werden konnten, es sei denn, es war eine Ersterfassung. Hier konnten die Beteiligten auch Leistungen anderer Stellen eintragen. Allerdings erlosch ihre Veränderungsberechtigung, sobald der eigentliche Leistungserbringer erstmals das Datum anfasste. Damit war die Validität der Daten gesichert.

Im Laufe der Entwicklung wurde deutlich, dass auch Bearbeitungsangaben wie Zeitpunkt der Antragstellung, Verhältnis von Schadenshöhe und erbrachten Leistungen u. ä. enthalten sein mussten.

Da sich in der Datenbank auch sehr in die Tiefe der persönlichen Verhältnisse gehende Daten befinden, waren wir bei der Auswertung sehr restriktiv. Technisch waren Auswertungen am Anfang nur auf den Einzelfall beschränkt möglich (um den Spendenbeiräten eine Entscheidungsgrundlage zu ermöglichen). Später kamen allgemeine Abfragen dazu, um eine breitere Verteilung steuern zu können. Generell sind Abfragen nur als PDF-Files möglich, da mit diesem Format eine technische Weiterverarbeitung außerhalb der Datenbank am besten vermieden werden konnte.

Eine Datenbank bei rund 60000 erfassten Datensätzen und mit in Hochzeiten bis zu 1000 Nutzern braucht gleiche Kriterien bei der Erfassung in der Datenbank, sonst sind die Angaben nicht vergleichbar und damit nutzlos. Es wurden deshalb in der Regel Katalogfelder, die die mögliche Auswahl begrenzen und eine Auswertbarkeit ermöglichen, verwendet. Freifelder wurden Plausibilitätsprüfungen unterworfen. Nur an zwei Stellen waren freie Textfelder zugelassen. In einem wurden Altdaten abgespeichert, die für die Bearbeitung wichtig waren, aber nicht in die Datenbank übernommen werden konnten. Es war für weitere Veränderungen gesperrt. Das andere diente Leistungserbringern als Möglichkeit, nähere Angaben zu den ursprünglichen Spendern zu machen. Bei erklärungsbedürftigen Feldern wurden Hilfestellungen eingefügt, die in der unteren Zeile des Browsers erscheinen (z. B. Definition des Haushaltseinkommens). Darüber hinaus gab es weitere Hilfestellungen. Auf der Startseite

wird der Nutzer über Neuerungen informiert; ein Nutzerhandbuch ist abrufbar; eine E-Mail-Adresse zur Online-Hilfe ist angegeben. Bei kritischen Feldern haben die Nutzer die Möglichkeit, eine Email an den letzten Bearbeiter zu senden, der dieses Feld verändert hat.

Abzuwehren hatten wir Bestrebungen, das Programm mit Textverarbeitungsmodulen und anderen Erweiterungen anzureichern. Dies hätte sofort die Systemvoraussetzungen verschärft und die Programmstabilität gefährdet. Wir haben uns deshalb bewusst auf die reine Datenbanklösung mit zentraler Speicherung, Echtzeitbetrieb und reinem Browserzugang beschränkt und das Datenmodell so einfach wie möglich gehalten.

14.2.4 Datenschutzrechtliche organisatorische und technische Rahmenbedingungen

Bereits am Anfang der Bearbeitung habe ich in einem Schreiben die Nutzer auf folgendes hingewiesen:

„Allgemeines:
- Mitarbeiter, die Umgang mit personenbezogenen Daten im Zusammenhang mit PHOENIX haben, sind nach § 6 SächsDSG auf das Datengeheimnis zu verpflichten. Ist dies bereits geschehen, so sind sie nochmals darauf hinzuweisen.
- Eine nicht zweckgebundene Verwendung der Antragsdaten sowie unbefugte Abrufe von Daten aus der Datenbank sind Verletzungen des Datenschutzes, die zu rechtlichen Konsequenten führen können.

Erheben der Daten:
- Es dürfen nur die Daten erhoben und die Nachweise verlangt werden, die erforderlich sind, um den Antrag zu bearbeiten und um erforderliche Prüfungen durchzuführen. Dabei ist abzuwägen, inwieweit die Vorlage der Nachweise ausreichend ist, oder ob die Nachweise als Kopie zu den Antragsunterlagen zu nehmen sind. Insbesondere müssen persönliche Angaben wie Name, Vorname, Geburtsdatum, Wohnanschrift *durch Vorlage* des Personalausweises oder Reisepasses geprüft werden. Kopien der Personaldokumente sind nicht notwendig.

Verwendung der erhobenen Daten:
- Die im Antragsverfahren erhobenen Daten und Unterlagen dürfen nur für die Spenden- bzw. Leistungsverwaltung im Zusammenhang mit dem Hochwasser verwendet werden (Antragsbearbeitung, Prüfung entsprechend der Vergabekriterien, Verwendung der ausgezahlten Mittel, Datenbank PHOENIX).

Nutzerberechtigungen bei PHOENIX:
- Nutzerberechtigungen werden über die Landratsämter eingerichtet. Sollte die

Vergabe nicht personenbezogen sein (z. B. bei Verwendung abstrakter organisationsbezogener Zugänge innerhalb einer Stelle), so ist durch die Stelle schriftlich festzuhalten, wer in welchem Zeitraum die Nutzerkennung benutzt hat.

Übermittlung von Daten an eingebende Stellen/Umgang mit Post:

- Werden die Daten zentral (z. B. im Landratsamt) in die Datenbank eingegeben, so ist die Post so zu adressieren, dass sie die zuständigen Bearbeiter direkt erreicht (Angabe der zuständigen Dienststelle und/oder die Umschläge mit dem Stichwort „Hochwasserhilfe“ oder dgl. versehen). Bei Übermittlung per Fax (nur wenn die zuständige Stelle ein eigenes Fax hat!) ist die Sorgfaltspflicht bei der Fax-Nummerneingabe zu beachten. Per E-Mail dürfen die personenbezogenen Daten für die Abgleichsdatenbank nicht versandt werden, sofern kein Verschlüsslungsverfahren zur Anwendung kommt.
- Der Zugang zur Datenbank erfolgt über eine verschlüsselte Internet-Verbindung. Der berechtigte Nutzer muss sich mit Benutzername und Passwort anmelden. Die üblichen Regeln für einen sorgsamen Umgang mit dem Zugangspasswort (insbesondere Geheimhaltungspflicht) sind zu beachten.
- Mitarbeiter, die für die Abgleichsdatenbank zugriffsberechtigt sind, dürfen Inhalte der Datenbank nur von der Dienststelle aus abrufen. Abrufe von privaten PCs oder Stellen aus sind nicht zulässig. Die Mitarbeiter sind entsprechend zu belehren.
- Informationen aus der Abgleichsdatenbank dürfen nur im Rahmen der Bearbeitung der Anträge zur Hochwasserhilfe abgerufen werden.

Recherchen:

- Auswertungsmodule werden durch die Sächsische Staatskanzlei in Abstimmung mit dem Sächsischen Datenschutzbeauftragten autorisiert.
- Für personenbezogene Auswertungen aus PHOENIX sowohl in ausgedruckter als auch in elektronischer Form gelten die gleichen datenschutzrechtlichen Bedingungen wie für Bearbeitungsunterlagen.

Löschen/Vernichten von Daten/Antragsunterlagen:

- Antragsunterlagen und Daten sind nach Ablauf der allgemeinen Aufbewahrungsfristen (5 Jahre für alle Unterlagen und Daten bis auf Nachweise mit Buchungsfunktion - hier gelten 10 Jahre) datenschutzgerecht zu vernichten.
- Den Anträgen beigefügte Nachweise zu Vermögenswerten und Kreditverbindlichkeiten sind nach Abschluss der Antragsbearbeitung (Bewilligungsbescheid und Auszahlung der Mittel bzw. nach Ablehnung einer Bewilligung) zu vernichten.
- Nach Abschluss der Antragsbearbeitung sind die Daten und Unterlagen bis zum Ablauf der Aufbewahrungsfristen verschlossen bzw. vor Zugriff geschützt aufzubewahren.
- Wurden Daten erhoben, die für die Antragsbearbeitung nicht erforderlich sind,

unterliegen diese Angaben einem Verwertungsverbot. Wurden die Daten elektronisch gespeichert, sind sie umgehend zu löschen.

Ende der Verarbeitung:
- Die Datenbank PHOENIX darf nur solange betrieben werden, wie sie der Aufgabenerfüllung dient. Die Daten der beteiligten Organisationen sind dann zu trennen und zurückzuführen. Einzelheiten werden durch die Staatskanzlei und die mitwirkenden Stellen unter Einbeziehung des Sächsischen Datenschutzbeauftragten bestimmt. Sollten in diesem Zusammenhang Datenübermittlungen für andere Zwecke vorgesehen sein, bedürfen diese einer gesetzlichen Grundlage bzw. der Einwilligung der Betroffenen."

Wie bereits oben gesagt, konnten wir uns wegen der Dringlichkeit des Vorhabens nur auf einem relativ niedrigen technisch-organisatorischem Datenschutzlevel bewegen. Wir haben uns deshalb entschieden, im Gegenzug eine vollständige Bearbeitungshistorie zu speichern, so dass zumindest im Nachhinein genau festgestellt werden kann, wer wann was gemacht hat. Dies ist auch allen Nutzern bekannt gewesen. Im Übrigen ist bis jetzt auch kein Fall des Missbrauchs der Datenbank bekannt geworden, was für die datenschutzrechtliche Aufklärung und das Problembewusstsein der vielen Nutzer spricht.

14.2.5 Fazit

Wegen des notwendigerweise schnellen Starts, sind einige Maßnahmen unterblieben, die bei einem zukünftigen Einsatz von PHOENIX unbedingt realisiert werden sollten:

- *eindeutiges Identitätsfeststellungsmerkmal*
  Die Erfassung von Name und Adresse allein (am Anfang meist auch ohne Geburtsdatum und in differierenden Schreibweisen) führte zu erheblichen Zuordnungsproblemen und Nachbesserungsaufwand. Es sollte von Anfang an ein eindeutiges Identitätsfeststellungsmerkmal erfasst werden. Dieser Anforderung würde die Personalausweisnummer (also eine bloße Ordnungsnummer, die keine Inhalte hat) genügen. Damit würde auch der erhebliche Aufwand einer Prüfung bei Namensähnlichkeiten, der zu Performanceverlusten führen würde, nicht notwendig.
- *Computerauthentifizierung*
  Durch die Gestaltung des Zuganges war keine Beschränkung auf bestimmte Rechner möglich. Hier ist zu überlegen, ob durch elektronische Signaturzertifikate nur bestimmten Rechnern der Zugang zur Datenbank erlaubt wird. So könnten die Nutzer z. B. nur von Arbeitsplatzrechnern zugreifen.
- *Digitale Signatur*

Sofern künftig elektronische Signaturen in der öffentlichen Verwaltung und der Privatwirtschaft stärker verbreitet sein werden, können auch diese in die Anwendung integriert werden. Dies wäre eine bedeutende Erleichterung bei der Authentisierung der Nutzer.

Die Ideen zur Perfektionierung müssen aber im Zweifel zugunsten dessen zurückstehen, dass jedenfalls in einer ersten Phase der Katastrophe einfache und flexible Zugänge zum Datenverarbeitungssystem auch dann eröffnet bleiben müssen, wenn Teile der Infrastruktur durch Feuer, Kontaminierung, Wasser oder Tod ausgefallen sind.

Im Augusthochwasser 2002 haben eine Vielzahl von öffentlichen und nichtöffentlichen Stellen untereinander abgestimmt Mittel verteilt und ausgereicht. Wie oben geschildert war die einzige rechtliche Grundlage für die Verarbeitung personenbezogener Daten die Einwilligung der Betroffenen. Unzureichende und nichtvorhandene Einwilligungsklauseln erschwerten Verfahrensabläufe erheblich. Da diese Probleme auch bei zukünftigen Katastrophenfällen auftreten können, muss eine ausreichende gesetzliche Grundlage geschaffen werden. Ich werde im Gesetzgebungsprozess zur Novellierung des Sächsischen Katastrophenschutzgesetzes darauf drängen, dass eine entsprechende Regelung für die Spenden- und Fördermittelverteilung aufgenommen wird.

Die Erfahrungen, die wir in diesem Projekt gesammelt haben, lassen sich für eine bestimmte Art von IT-Vorhaben durchaus verallgemeinern. Wer schnell mit einfachen Mitteln eine Vielzahl von Nutzern an eine auf ein eingrenzbares Ziel ausgerichtete Datenbank anbinden will, sollte sich PHOENIX anschauen. Es konnten abgeordnete Mitarbeiter der Gemeindeverwaltung in ihrem schnell eingerichteten Arbeitsraum genauso wie die Geschäftsführerin des privaten Hilfevereins von dem einzigen ihr zur Verfügung stehenden Computer wie der Mitarbeiter des Wohlfahrtsverbandes vor Ort mit Notebook und Mobiltelefon auf die Datenbank zugreifen und damit arbeiten.

Eine entscheidende Voraussetzung für das gute Gelingen dieses Vorhabens war die Kommunikation der Beteiligten untereinander. So gab es einen ständigen Kontakt der Entwickler und Betreuer zu den Nutzern. Auf mehreren Workshops wurden von Seiten des Entwicklerteams das Programm erläutert, weitere Entwicklungen angezeigt und der rechtliche Rahmen geschildert. Die Nutzer brachten durchaus kritisch wichtige Veränderungs- und Verbesserungsvorschläge ein. Auch außerhalb dieser Veranstaltungen waren die Nutzer dazu aufgerufen, sich zu Wort zu melden, was sie intensiv taten. Ohne diese Rückkopplung wäre eine praxisgerechte Einführung und Fortentwicklung des Programms nicht möglich gewesen.

Weiterer notwendiger Bestandteil der Kommunikationsbeziehungen war die Abstimmung der beteiligten Organisationen; sie musste allen technischen Einführungen und Veränderungen vorangehen. Hier war hilfreich, das einige Beteiligte des Entwickler-

teams auch in den Koordinierungsgremien der spenden- und fördermittelverteilenden Organisationen saßen und daher Anregungen nach beiden Seiten übermitteln konnten.

Mittlerweile wollen andere deutsche und europäische Länder PHOENIX offiziell bei ihren Katastrophenbewältigungen einsetzen. Dies ist für Sachsen die Chance, einen substantiellen Dank zurückzugeben für die großzügig erhaltene Hilfe bei der Flutkatastrophe.

14.3 Datenschutzrechtliche Bewertung der Auskunftserteilung aus dem Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV) mit dem Pilotprojekt ZEUGE

Das Pilotprojekt ZEUGE - ein Akronym, das sich aus den Anfangsbuchstaben der Worte „*Z*StV-*E*rmittlungs*U*nterstützung auf der *G*rundlage von *E*OSS“ zusammensetzt - ist eine IT-Lösung, mit deren Hilfe die Steuerfahndungs- und Bußgeld-/ Strafsachen–Stellen in den dafür zuständigen Finanzämtern Informationen über Beschuldigte und Mitbeschuldigte erhalten, gegen die in der Bundesrepublik Deutschland strafrechtliche Ermittlungsverfahren laufen. Dafür richten sie Anfragen an das bundesweite Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) in Berlin. Für die datenschutzrechtliche Bewertung war entscheidend, ob die Rückauskunft vom ZStV an den Empfänger übermittelt wird oder ob dieses die Informationen zum Abruf gemäß § 8 SächsDSG bereithält.

Gesetzliche Grundlage zur Auskunftserteilung aus dem ZStV ist Artikel 4 Nr. 11 des „Gesetz zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz)“ vom 28.10.94 (BGBl. I S. 3186). Sie ist für die Steuerverwaltung bei selbständig geführten Ermittlungsverfahren nach §§ 399, 386 AO und Ermittlungsverfahren nach § 402 AO gegeben. Auskunftsersuchen und Übermittlung sind in Nr. 7 der Allgemeinen Verwaltungsvorschrift über die Errichtungsanordnung für das länderübergreifende staatsanwaltschaftliche Verfahrensregister geregelt.

Eine Übermittlung der Daten darf auf Ersuchen der Strafverfolgungsbehörden erfolgen. Zu diesen gehören z. B. Staatsanwaltschaften und Finanzbehörden, soweit sie das Ermittlungsverfahren führen. Die Auskünfte sollen (elektronisch) „per Leitung“ (Nr. 7.3) übermittelt werden. Nur in Ausnahmefällen sind auch telefonische oder fernschriftliche Datenübermittlungen zulässig.

Ablauf der Auskunftserteilung:
Um den Informationsfluss effizient zu gestalten, wurden auf Landesebene so genann-

te „Kopfstellen“ eingerichtet, die die Informationen bündeln. Anfragen der Stellen innerhalb eines Landes richten sich immer an die Kopfstelle. Nur die Kopfstellen kommunizieren mit dem ZStV in Berlin.

Als Anwendungsoberfläche für das Verfahren ZEUGE werden herkömmliche Browser (Internet Explorer, Netscape) verwendet.

- Der Sachbearbeiter meldet sich beim IT-Verfahren an. Nach der Berechtigungsprüfung wird das ZEUGE–Hauptfenster angezeigt. Die Benutzeroberfläche ist abhängig von den dem Nutzer eingeräumten Rechten gestaltet. Die Buttons zeigen nur aktive Funktionalitäten an.
- Aus dem angezeigten Menü wählt der Nutzer das „Auskunftsersuchen” aus. Der Sachbearbeiter kann abhängig vom Auskunftsumfang und von der Eilbedürftigkeit Anfragen (Standard-, Eil-, Mitbeschuldigten- und Sonderanfragen) auswählen.
  Das IT-Verfahren unterstützt die Daten-Erfassung mit Aufklapplisten und Plausibilitätskontrollen.
- Das elektronisch ausgefüllte Erfassungsformular kann anschließend gesendet, gespeichert, gelöscht oder gedruckt werden.
- Wird das Erfassungsformular an die Landeskopfstelle (über eine HTTP-Netzverbindung) gesendet, wird dieses mit weiteren Anfragen eines Bundeslandes über einen konfigurierbaren Zeitraum in der Kopfstelle gesammelt, registriert, aufbereitet, fehlerbehandelt, protokolliert und als Sammeldatei per Filetransfer oder als E-Mail an die Registerbehörde (ZStV) übermittelt.
- In der Registerbehörde werden die eingehenden Nachrichten entgegengenommen. Die Sendeberechtigung und die Behördenkennzeichen der anfragenden Stellen werden auf ihre Zulässigkeit geprüft. Anschließend wird in der ZStV-Datenbank nach Registereinträgen mit Personen gesucht, die denen der Anfrage gleich oder ähnlich sind. Das Suchergebnis oder eine Fehlermitteilung wird in einer Sammeldatei für das jeweilige Land gespeichert. Per Filetransfer oder E-Mail wird diese Sammeldatei an die Landeskopfstelle übermittelt.
- Nach dem Eingang der ZStV-Sammeldatei bereitet die Landeskopfstelle die empfangenen Informationen auf, ordnet sie den Anfragen zu, ändert den Status (beantwortet, fehlerhaft,...) und protokolliert die Verarbeitung.
  Die Kopfstelle übermittelt die vom ZStV gelieferten Auskünfte nur an den anfragenden Sachbearbeiter weiter. Die Auskünfte werden nicht landesweit bereitgestellt.
- Der Sachbearbeiter erkennt an einer Statusänderung, ob eine Antwort vom ZStV eingegangen ist. Er kann das Suchergebnis ansehen und ggf. drucken.

Bewertung aus datenschutzrechtlicher Sicht
Bei dem IT-Verfahren ZEUGE werden die Anfragen und Auskünfte nicht wie bisher üblich per Telefon, Fax oder Brief angefordert und beantwortet, sondern auf elektronischem Weg (ohne Medienbruch) übermittelt. Die Kommunikation mit ZStV erfolgt

zweistufig. Es gibt eine Kommunikationsverbindung (HTTP) zwischen den befugten Finanzämtern und der Kopfstelle eines Bundeslandes und eine Kommunikationsverbindung (Filetransfer oder E-Mail) zwischen der Kopfstelle und dem ZStV in Berlin.

Es gibt *keine* Online-Verbindung zwischen dem Finanzamt und der Registerbehörde. Ein automatisierter Abruf aus dem ZStV durch den Sachbearbeiter ist daher nicht möglich. Auch die Landeskopfstelle, die alle elektronischen Anfragen in einem konfigurierbaren Zeitraum sammelt und diese per Filetransfer oder E-Mail an das ZStV weiterleitet, kann nicht selbst auf die ZStV-Applikation zur Datenbanksuche zugreifen. Die Registerbehörde bestimmt *allein*, ob und wenn ja, welche personenbezogenen Daten (z.B. Auskunftssperre, eingeschränkte „Beauskunftung“) zur Verfügung gestellt werden. Die Registerbehörde ist als „Herr der Daten“ für die Zulässigkeit der Übermittlungen verantwortlich.

Das Auskunftsverfahren nutzt die elektronische Erfassung, Übermittlung, eine automatisierte Bearbeitung und Auskunftserteilung ohne Medienbruch. Die Auskünfte werden von der Registerbehörde über die Landeskopfstelle an den Empfänger weitergegeben, nicht zum Abruf im Sinne des § 8 SächsDSG bereitgehalten. Damit ist für den Datenaustausch zwischen den öffentlichen Stellen des Landes keine spezialrechtliche Grundlage zum automatisierten Abruf notwendig.

Aus datenschutztechnischer Sicht sollten Verschlüsselungsverfahren zur sicheren Datenübermittlung eingesetzt werden, die wegen der heterogenen Zusammensetzung der Benutzergruppen und unterschiedlicher Systemumgebung zurzeit noch nicht eingesetzt sind.

14.4 Empfehlungen zum Gebrauch von Passwörtern

Bei unserer Kontroll- und Beratungstätigkeit stelle ich immer wieder fest, dass beim Gebrauch von Passwortverfahren häufig noch die notwendige Sensibilität fehlt, vor allem dann, wenn der Zugriff auf besonders zu schützende personenbezogene Daten ausschließlich durch Passwörter abgesichert wird. Wiederholt musste ich feststellen, dass die verwendeten Passwortlängen und die Zeichenmenge, aus der das Passwort zusammengesetzt ist, nicht ausreichend sind. Ein zu kurzes nur aus Buchstaben gebildetes Passwort kann z. B. relativ schnell durch systematisches Ausprobieren oder Erraten gefunden werden, wenn die Zahl der Fehlanmeldungen nicht begrenzt ist oder wenn Log-Protokolle nicht regelmäßig ausgewertet werden.

Passwörter sind auch heute noch das am meisten genutzte Verfahren zur Authentifizierung von Benutzern. Auch wenn andere Verfahren zur Authentifikation im Einsatz sind, wie z. B. Chipkarten, Token oder biometrische Merkmale, so stellen diese meist

nur eine Ergänzung zur konventionellen Benutzerkennung und Passwort und keinen Ersatz für diese dar.

Mit der Eingabe des geheimen Passwortes weist sich der Benutzer gegenüber dem informationsverarbeitenden System als berechtigt aus. Das System prüft, ob die Benutzerkennung existiert und ob das eingegebene Passwort zur Benutzerkennung gehört. Wenn die Eingaben mit den im System hinterlegten Einträgen übereinstimmen, kann der Benutzer im Rahmen seiner Berechtigungen auf Anwendungsprogramme und Ressourcen zugreifen. Ansonsten wird der Benutzer vom System mit einer Fehlerausschrift abgewiesen.

Gängige Praxis ist es, als Benutzerkennung den Familiennamen der Beschäftigten einzutragen. Da dieser auch den anderen Benutzern bekannt ist, gewährleistet einzig und allein das geheime Passwort den geforderten Zugriffsschutz, zumal zusätzliche Authentifizierungsmöglichkeiten (z. B. Chipkarte, Prüfung von Terminalnummer oder IP-Adresse) meist nicht genutzt werden.

Der Versuch, sich im internen Netz als ein anderer Benutzer auszugeben und Passworte auszuprobieren, wird dann nicht bemerkt, wenn Fehlanmeldungen nicht protokolliert werden, wenn nach einer bestimmten Zahl von Fehlversuchen die Benutzerkennung nicht gesperrt wird oder Log-Protokolle nicht regelmäßig ausgewertet werden.

Das Risiko erhöht sich noch, wenn das Passwort leicht zu erraten ist und durch systematisches Ausprobieren gefunden werden kann. Dies ist vor allem dann der Fall, wenn das Passwort nur aus wenigen Zeichen (Buchstaben) besteht und Bezug auf den Benutzer (Vor-, Kose-, Ortsnamen, Namen von Freunden, Sternzeichen, usw.) besitzt.

Grundsätzlich können alle Authentisierungssysteme, die auf Passwörtern basieren, durch systematisches Probieren gebrochen werden. Dies ist abhängig von der Passwortlänge, der Zeichenmenge (Groß-Buchstaben, Groß- und Kleinbuchstaben, alle Zeichen), aus der das Passwort zusammengesetzt ist, und dem eingesetzten Betriebssystem.

Der Hamburger Datenschutzbeauftragte hat Messungen zur Passwortentschlüsselung per Brute-Force-Methode durchgeführt. Dazu können Informationen von der Webseite des Hamburger Datenschutzbeauftragten unter Informationsmaterial, Tipps und Hinweise zur Datensicherheit oder unter der URL http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationsmaterial/informationstechnik/tipps.html zum Download abgerufen werden.

Der Realzeit-Aufwand zur Passwortermittlung ist von der Passwortlänge, der Zeichenmenge, aus der sich das Passwort zusammensetzt und dem Zeitaufwand zur Überprüfung eines einzelnen Rateversuchs abhängig. Die Messergebnisse des Hamburger Datenschutzbeauftragten zeigen, dass Passwörter mit einer Länge von 6 Zei-

chen bereits nach einer geringen Zeit (z.B. unter Windows mit 26 möglichen Zeichen bereits nach 48 Sekunden, mit 52 möglichen Zeichen nach 51 Minuten und mit 95 möglichen Zeichen nach 31 Stunden) ermittelt werden können. Bei einer Passwortlänge von 8 Zeichen ergibt sich ein deutlich höherer Aufwand zur Ermittlung eines Passwortes (z. B. unter Windows mit 26 möglichen Zeichen nach 9 Stunden, mit 52 möglichen Zeichen nach 95 Tagen und mit 95 möglichen Zeichen nach 32 Jahren).

Daher ist eine Passwortlänge von 6 Zeichen nicht mehr ausreichend. Das Gleiche gilt fast vollständig auch für die Länge 7. Daraus folgt, dass wenigstens 8 Zeichen und eine vollständige Zeichenmischung (Groß- und Kleinschreibung sowie Ziffern bzw. Sonderzeichen) für Passwörter verwendet werden sollten.

Wird ein Passwort längere Zeit verwendet, so steigt auch die Wahrscheinlichkeit, dass das Passwort oder ein Teil davon beim Blick über die Schulter erspäht wird. Hat der Angreifer das entsprechende Passwort durch Ausprobieren gefunden, kann er die Zugriffsrechte missbräuchlich nutzen. Die unbefugte Eingabe, sowie die unbefugte Kenntnisnahme oder Löschen, Kopieren oder Entfernen von personenbezogenen Daten wären unbeobachtet möglich. Das ist ein Verstoß gegen die Speicher-, Benutzer- und Zugriffskontrolle (§ 9 Abs. 2 Nr. 3 bis 5 SächsDSG).

Um diese Risiken zu vermeiden, sind die Beschäftigten auf einen sicheren Gebrauch von Passwörtern hinzuweisen und auf die Einhaltung datenschutzrechtlicher Anforderungen zu sensibilisieren. Deshalb sollen hier auch die bisherigen Empfehlungen des Sächsischen Datenschutzbeauftragten zur Passwortgestaltung, die noch auf dem Erkenntnisstand des Jahres 1993 beruhen, angepasst und ergänzt werden.

Bei der Nutzung von Passwörtern sind folgende Sicherheitsgrundsätze zu beachten:

1. Jede Person erhält eine eigene Benutzerkennung, die mit einem Passwort zu schützen ist.
2. Passwörter dürfen nur dem Benutzer bekannt sein (selbst vergeben, selbst ändern, nirgends notieren, niemandem mitteilen, nicht leicht zu erraten). Sie sind geheim zu halten.
3. Das Passwort darf sich nicht auf den Passwortinhaber beziehen (Name, Vorname, Freundin usw.).
4. Die Eingabe des Passwortes sollte unbeobachtet stattfinden und nicht auf dem Bildschirm angezeigt werden. Das Passwort sollte möglichst nicht auf dem PC gespeichert werden.
5. Der gesamte verfügbare Zeichenvorrat ist auszuschöpfen (Buchstaben, Ziffern, Sonderzeichen). Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist. Empfehlenswert ist der Einsatz von Akronymen (z. B. Anfangsbuchstaben der Wörter eines Merksatzes).
6. Als Mindestlänge von Passwörtern sind möglichst acht Stellen vorzusehen. Es muss getestet werden, wie viele Stellen eines Passwortes das Betriebssystem bzw. der Rechner überprüft.

7. Voreingestellte Passwörter der Hersteller sind durch individuelle Passwörter zu ersetzen.
8. Zu vermeiden sind Passwörter, die aus in einem Wörterbuch vorkommenden, die mit der Nutzerkennung verbunden sind (z. B. ThGiesen) und Trivialpasswörter, die mit leicht zu erratenden Methoden gebildet werden (z. B. nebeneinander liegende Tasten wie 12345..., Datumsangaben wie 10Mai2003 usw.).
9. Passwörter dürfen nicht auf programmierbare Funktionstasten gelegt werden.
10. Passwörter sollten zugriffssicher gespeichert werden, zum Beispiel mittels Einwegverschlüsselung.
11. Ein Passwortwechsel ist vorzusehen:
    - turnusmäßig (etwa alle drei Monate),
    - sofort nach bekannt werden des Passworts,
    - nach Wartungsarbeiten.
12. Das neue Passwort darf mit dem alten nicht identisch sein und sollte eine Bestätigung mit einer wiederholten Eingabe anfordern, damit eine unbewusste Falscheingabe sofort auffällt.
13. Es ist festzulegen, wie zu verfahren ist, wenn ein Benutzer sein Passwort vergessen hat.
14. Passwörter sollten nur dann aufgezeichnet werden, wenn für den Vertretungsfall (z. B. Urlaub oder Krankheit) keine Stellvertreter-Konten eingerichtet werden können. In diesem Fall sind die Passwörter in einem verschlossenen Briefumschlag sicher aufzubewahren.
15. Das Passwort ist gegen Ausprobieren durch Begrenzung der Fehlversuche zu schützen.
16. Erfolglose Login-Versuche sollten auf jeden Fall protokolliert werden.
17. Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, die nach einmaligem Gebrauch durch selbst gewählte Passwörter zu ersetzen sind.
18. Zeitweise nicht genutzte Kennungen sind zu sperren bzw. zu deaktivieren. Kennungen von ausgeschiedenen Mitarbeitern sind unverzüglich zu löschen bzw. zu sperren.
19. Bei der Authentisierung in vernetzten Systemen sollten Passwörter nur verschlüsselt übertragen werden.

Folgende Maßnahmen sind darüber hinaus zu empfehlen:

1. Die letzte Systemnutzung sollte dem Benutzer automatisiert bei der aktuellen Anmeldung angezeigt werden.
2. Außerhalb der Arbeitszeit sollte das IT-System keine Anmeldung von Benutzern annehmen.
3. Die Vergabe von Gruppenpasswörtern ist zu vermeiden. Die Einrichtung von Gruppen bzw. Gruppenrechten sollte dazu dienen, die Benutzer mit ihrer persönlichen Kennung den jeweiligen Gruppen mit gleichen Zugriffsrechten zuzuordnen.

14.5 Datenschutz bei Windows XP Professional[1]

1. Einleitung

Windows XP wird in zwei Versionen angeboten: Windows XP Home und Windows XP Professional. Wie schon der Name vermuten lässt, ist Windows XP Professional für den professionellen Gebrauch besser geeignet als die Home Version, da bestimmte Funktionen mit der Home-Version nicht ausführbar sind (siehe Punkt 13). Die nachfolgenden Ausführungen beziehen sich deshalb hauptsächlich auf Windows XP Professional.

Die Orientierungshilfe richtet sich deshalb auch in erster Linie an versierte Anwender wie Administratoren aus dem Bereich der professionellen Datenverarbeitung, denen der Umgang mit Windows vertraut ist und die somit auch die Schwachstellen älterer Windows-Betriebssysteme bereits kennen. Das Papier ist im Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder beraten und zustimmend zur Kenntnis genommen worden.

Windows XP Professional tritt die Nachfolge von Windows 2000 Professional an. Die neue Benutzeroberfläche, die erweiterte Hilfe und viele Assistenten sind die auf den ersten Blick auffälligsten Veränderungen bei Windows XP. Die Assistenten sollen den gestiegenen administrativen Aufwand eingrenzen. Insbesondere für erfahrene Benutzer sind sie gewöhnungsbedürftig und oft etwas zuviel des Guten, zumal automatisierte Vorgänge schlechter nachvollziehbar und dadurch undurchsichtiger werden. Die enge Anbindung an das Internet macht das Betriebssystem besonders leicht angreifbar.

Im Mittelpunkt dieser Betrachtung des neuen Betriebssystems von Microsoft sollen datenschutzrelevante Aspekte stehen. Der Benutzer soll auf bestehende Mängel in der Sicherheit des Betriebssystems aufmerksam gemacht werden. Es sollen Hinweise gegeben werden, wie diese Mängel eingeschränkt oder umgangen werden können. Darüber hinaus werden wesentliche Sicherheitsaspekte des Betriebssystems erklärt, damit bestimmte sicherheitsrelevante Einstellungen vorgenommen werden können.

2. Was ist neu bei Windows XP

2.1 Neue Benutzeroberfläche

Das Startmenü ist vollkommen neu gestaltet, bietet den Zugriff auf den Programmpfad und auch auf häufig genutzte Programme.

---

[1] Orientierungshilfe des Landesdatenschutzbeauftragten Mecklenburg-Vorpommern

2.2 Hilfe und Supportcenter

Mit dem Hilfe- und Supportcenter wurde der Zugriff auf die Onlinehilfe intensiviert.

2.3 Vereinfachungen für die Administration

Da der administrative Aufwand sehr gestiegen ist, werden Assistenten bereitgestellt.

2.4 Schneller Benutzerwechsel

Mehrere Benutzer können sich gleichzeitig anmelden, der Desktop und alle Tasks bleiben erhalten.

2.5 Neue Sicherheitsmechanismen

Mit Windows XP Professional wartet das Betriebssystem mit zahlreichen neuen Sicherheits-Funktionen auf. Zu den Wichtigsten zählen:

- die Verschlüsselung von Dateien und Ordnern auch für mehrere Benutzer,
- Analysefunktionen für Angriffe, Firewallfunktionen,
- automatische Konfiguration sicherheitsrelevanter Einstellungen.

Eine weitere aus datenschutzrechtlicher Sicht bedeutende Neuerung bei Windows XP ist die so genannte Produktaktivierung (siehe Punkt 5).

3. Vorteile und Nachteile von Windows XP

3.1 Vorteile

Durch die neue Treiberarchitektur wurde die Stabilität des Betriebssystems verbessert. Die veränderte Benutzeroberfläche ist eher umstritten. Für Computerneulinge vereinfacht sie sicher die Nutzung, für erfahrene Benutzer ist sie jedoch gewöhnungsbedürftig, weil vieles völlig anders als bisher ist. Immerhin kann auch die gewohnte, klassische Windows-Oberfläche gewählt werden. Da der administrative Aufwand gestiegen ist, werden einige erleichternde Hilfen durch Windows zur Verfügung gestellt:

- mehr Assistenten für Basisaufgaben,
- Zusammenfassung von Verwaltungsaufgaben in der Managementkonsole,
- kontextorientierte Aufgabenlisten in den Standardordnern,
- neue Ansicht der Systemsteuerung,
- Verlagerung von bestimmten Aufgaben in das Hilfe- und Supportcenter.

3.1.1 Verbesserte Hilfe

Die Suchfunktion ist deutlich leistungsfähiger als seine Vorgänger. So kann über den Suchdialog direkt nach Dokumenten, Computern, Druckern oder Personen gesucht werden. Neu ist der Start der Suchfunktion für das Internet. Die enge Verflechtung mit dem Internet spart zwar Zeit und Arbeit, ist jedoch nicht ganz unbedenklich. Nachteilig ist allerdings, dass kein Handbuch mehr zur Verfügung gestellt wird.

3.1.2 Verbesserte Systemwiederherstellung

Die Systemwiederherstellung kann im Falle eines Systemproblems einen früheren Zustand des Computers wiederherstellen, ohne dass die persönlichen Datendateien (z. B. Dokumente, Internetfavoriten und E-Mail) verloren gehen. Die Systemwiederherstellung überwacht Änderungen auf dem Computer und erstellt regelmäßig leicht identifizierbare Wiederherstellungspunkte. Darüber hinaus kann der Nutzer selbst jederzeit eigene Wiederherstellungspunkte erstellen und benennen.

3.1.3 Onlineunterstützung

Mit Hilfe der Remoteunterstützung kann anderen Personen gestattet werden, eine Verbindung mit dem eigenen Computer über das Internet herzustellen, sich in einem Chat mit dem Nutzer zu unterhalten und dessen Computerbildschirm einzusehen. Außerdem kann dieser Assistent nach entsprechender Zustimmung die Tastatur des Nutzers und dessen Maus steuern und somit bei der Problembehandlung helfen. Zusätzlich werden auch die Dateisysteme des Client-Geräts auf den Windows XP Rechner übertragen, damit dieser Rechner auf die Laufwerke des Clients zugreifen kann (siehe dazu auch Punkt 6.4). Die Supportseite ermöglicht es, sich direkt an den Computerhersteller oder, falls Windows XP separat erworben wurde, an Microsoft zu wenden. In der Support-Newsgroup kann der Austausch von Informationen und Hilfe mit anderen Benutzern erfolgen.

3.1.4 Offline-Unterstützung

Falls keine Internetverbindung zur Verfügung steht, können andere Tools für die Problembehandlung genutzt werden: Die so genannten Computerinformationen zeigen Informationen über die zurzeit installierte Software und Hardware an. Die erweiterten Systeminformationen und das Systemkonfigurationsprogramm bieten technische Details, mit denen Mitarbeiter vom technischen Support Probleme beheben können.

3.1.5 Schnelle Benutzerumschaltung

Windows XP führt mit Hilfe der Terminaldiensttechnologie eindeutige Benutzersitzungen aus, wodurch die Daten der einzelnen Benutzergruppen eindeutig voneinander getrennt bleiben. Durch das verwendete Benutzerkennwort werden die Daten separat voneinander geschützt, sofern sie sich auf einer NTFS-Partition befinden. Die schnelle Benutzerumschaltung ist nur bei Computern einer Arbeitsgruppe oder bei eigenständigen Computern möglich. Gehört der Computer zu einer Domäne, erfolgen die Optionen für die Anmeldung nach den vom Administrator festgelegten Richtlinien (siehe auch Punkt 9).

Die neue Benutzerumschaltung ermöglicht es, schnell zwischen Benutzern umzuschalten, ohne sich am Computer abzumelden. Mehrere Benutzer können einen Computer gemeinsam nutzen und ihn gleichzeitig verwenden, wobei die Benutzer wechseln können, ohne die Programme, die sie ausführen, zu schließen (z. B. ein Computer für alle Mitarbeiter einer Lagerverwaltung).

3.2 Nachteile

Windows XP ist das wohl neugierigste Betriebssystem aller Zeiten. Der Internet-Explorer suchte schon vor XP automatisch nach Updates. Aber in keiner der vorherigen Windows-Versionen hat Microsoft so viele Komponenten eingebaut, die über das Internet Kontakt mit den Microsoft-Servern aufnehmen, wie z. B. das Windows-Update, die Fehlerberichterstattung und die Zeitsynchronisation. Den Messenger von Microsoft musste sich bisher jeder auf seinen PC laden, der ihn einsetzen wollte. Bei XP sind jetzt diese Anwendungen und Funktionen Standard. Windows XP schreibt einen Fehlerbericht, sobald ein Programm abstürzt, und gibt dem Anwender die Möglichkeit, diesen per Internet an Microsoft zu senden (siehe Abb.1). Immerhin könnte der Anwender davon indirekt profitieren, da Microsoft mit der so entstehenden Datenbank unter anderem natürlich auch das Betriebssystem verbessern kann.

Abb.1

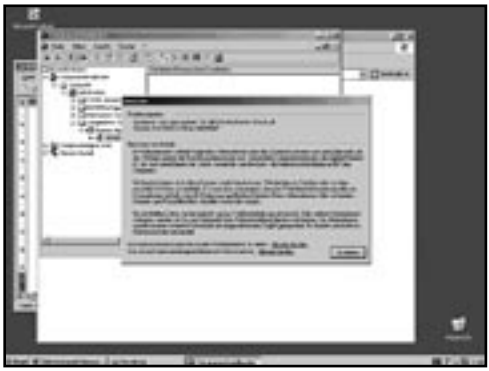


Abb. 1 zeigt eine typische Fehlermeldung mit Hinweisen zu den übertragen Daten. Mit dem Hinweis, dass die Informationen „auf einer sicheren Datenbank mit eingeschränktem Zugriff gespeichert werden“ und dass der „Bericht nicht zu Werbezwecken verwendet wird“ soll möglicherweise der datenschutzgerechte Umgang mit diesen Daten suggeriert werden, nachprüfbar ist jedoch keine dieser Aussagen.

Der über das Netz übertragene Fehlerbericht enthält folgende Informationen:

- Informationen über den Zustand der Datei zum Zeitpunkt, als das Problem auftrat,
- die Betriebssystemversion und die verwendete Computerhardware,
- die digitale Produkt-ID die zum Identifizieren der Lizenz verwendet werden kann,
- die Internetprotokolladresse (IP).

Es kann aber auch vorkommen, dass der Fehlerbericht kundenspezifische Informationen enthält, wie z. B. Daten aus geöffneten Dateien. Diese Informationen, falls vorhanden, können zum Feststellen der Identität verwendet werden.

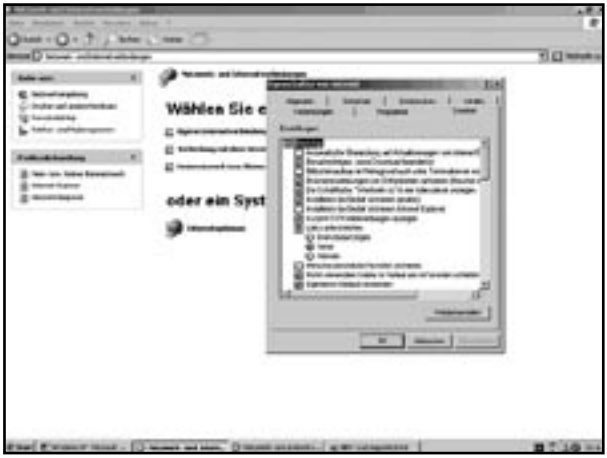
3.2.1 So schützen Sie sich

Grundsätzlich gilt: Alle genannten Funktionen lassen sich über die Systemsteuerung abschalten (siehe Abb. 2)

Automatische Aktualisierung abschalten

Die Automatische Aktualisierung lässt sich über Systemsteuerung/Netzwerk und Internetverbindungen/Internetoptionen auf der Karte erweitert abschalten. Wurden die automatischen Aktualisierungen nicht abgeschaltet, können sie über Systemsteuerung/Software jederzeit wieder entfernt werden. Alle Aktualisierungen werden dort verwaltet.

Abb. 2

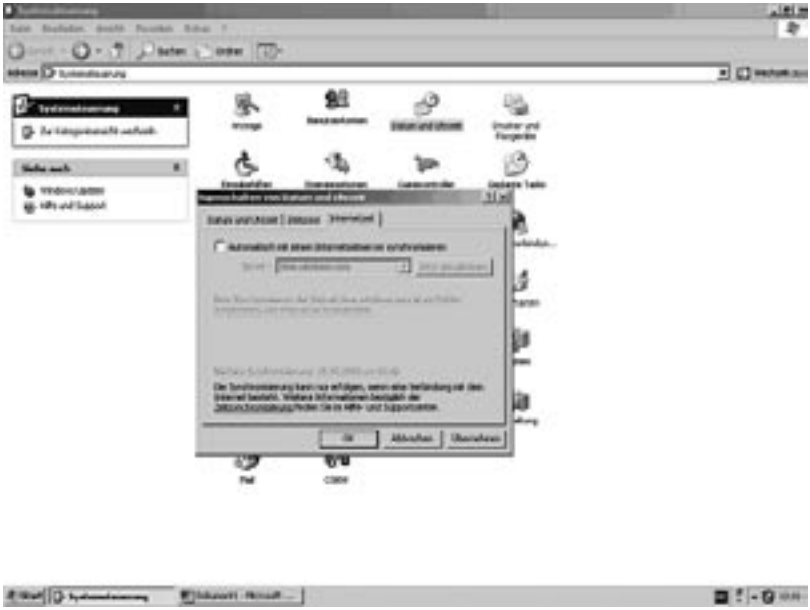


Empfehlung: Die automatische Überprüfung auf Aktualisierungen vom Internet Explorer sollte deaktiviert sein.

Abschalten der Zeitsynchronisation

Bei der Funktion Zeitsynchronisation stimmt Windows XP die Uhrzeit des PCs mit einer Uhr im Internet ab. Dazu wird ein Internet-Server von Microsoft kontaktiert. Als Standardserver kann jedoch auch ein anderer Server eingetragen werden. Ein Entfernen des Häkchens bei „Automatisch mit einem Internetserver synchronisieren" verhindert diese ständigen Kontaktaufnahmeversuche (siehe Abb. 3).

Abb. 3

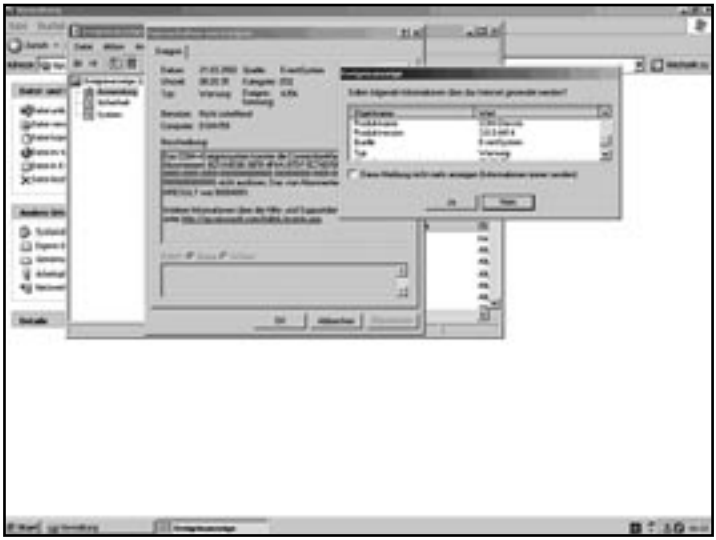


Die Zeitsynchronisation lässt sich unter *Datum und Uhrzeit* abschalten oder auf einen anderen Internet-Server umlenken.

Fehlerprotokoll aufrufen/Kontrolle der übertragenen Daten über die Hilfe und Supportdienste

Zur besseren Kontrolle der übertragen Daten sollte die entsprechende Mitteilung immer angezeigt bleiben (siehe Abb. 4). Nur so lässt sich einschätzen, welche Informationen wann übertragen werden.

Abb. 4

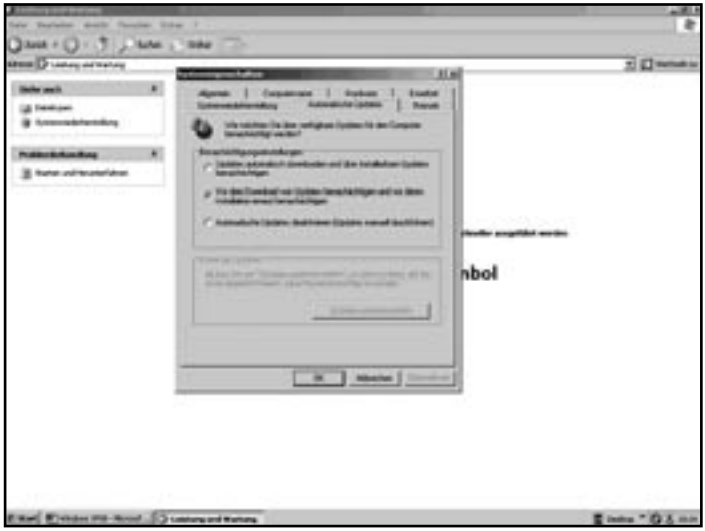


Empfehlung: Das Feld „Diese Meldung nicht mehr anzeigen“ sollte deaktiviert bleiben.

Automatische Updates

Auch Updates können so eingestellt werden, dass sie nicht automatisch erfolgen, und der Nutzer den Überblick behält, wann welches Update erfolgt (siehe Abb. 5).

Abb. 5



Empfehlung: Automatische Updates sollten deaktiviert sein, mindestens jedoch sollte vorher eine Benachrichtigung erfolgen.

3.2.2 Softwareunterstützung

Einen guten Überblick über die in Punkt 3.2.1 genannten datenschutzrelevanten Einstellungen kann man sich auch mit Hilfe zusätzlicher Software verschaffen. Das – allerdings nur für die private Nutzung kostenlos – aus dem Internet herunter zu ladende Programm XPAntiSpy beispielsweise ermöglicht ein sehr komfortables Konfigurieren dieser Systemeinstellungen über die Windows-Oberfläche oder im Befehlszeilenmodus.

4. Die Installation von Windows XP

4.1 Anforderungen an Hardware

Folgende Mindestvorrausetzungen bzw. Empfehlungen für die Hardware sollten berücksichtigt werden, um flüssiges Arbeiten zu gewährleisten:

Hardware	*Mindestanforderungen*	*Empfohlen*
CPU	266 MHz Pentium	500 MHz Pentium III
RAM	64 MB	256 MB
Festplatte	2 GB; min.1,2 GB Frei	Ab 4 GB
Netzwerk	PCI 10 MBit	PCI 100 MBit
Grafikkarte	PCI-Grafikkarte	AGP-Grafikkarte
CD-ROM	12-fach	32-fach
Floppy	1,44 MB	1,44 MB

Das Vorhandensein der Maus ist Bedingung.

Es gibt drei verschieden Möglichkeiten, Windows XP zu installieren: Update-, Neu-, und Parallelinstallation. Für die Parallelinstallation muss für Windows XP eine eigene Partition eingerichtet sein.

Die Produktaktivierung kann telefonisch oder online über das Internet erfolgen (siehe Punkt 5).

Alle Benutzer, die bereits während der Installation von Windows XP eingerichtet wurden, erhalten zunächst automatisch die Rechte eines System-Administrators. Es sind nicht nur „Benutzer“, wie das dazugehörige Dialogfenster vermuten lässt, sondern „Administratoren“ mit entsprechenden Privilegien. Diese lassen sich zwar im Nachhinein einschränken, besser ist es aber, bestimmte Rechte von vornherein auszuschließen. Dabei ist jedoch zu berücksichtigen, dass sich einige Applikationen ohne Administrator-Rechte nicht sinnvoll betreiben lassen. Eine Abwägung zwischen Produktivität und Sicherheit ist deshalb immer notwendig.

4.2 Automatisierte Installation

Die komplette Installation vieler identischer Computer bedeutet hohen zeitlichen Aufwand und entsprechend hohe Kosten. Der schnellstmögliche Ersatz bei Ausfall eines Computersystems in einem Unternehmen ist ein weiterer Grund für eine Arbeitserleichterung auf diesem Gebiet.

Für die automatisierte Installation gibt es mehrere Möglichkeiten:

- *Mit Hilfe von Antwortdatei für WINNT.EXE/WINNT32.EXE*
  - Über Antwortdateien wird das Setup von Windows XP gesteuert. In normalen Textdateien werden in einer bestimmten Syntax die Antworten eingetragen, die normalerweise durch den Benutzer eingegeben werden. Das automatisch ablaufende Setup verkürzt die benötigte Zeit für die Installation. Das Administratorkennwort wird unverschlüsselt im Klartext in der Antwortdatei (siehe Punkt 4.2) abgelegt und kann damit leicht missbräuchlich genutzt werden. Man sollte deshalb hier noch kein reales, sicherheitsrelevantes Passwort festlegen, sondern zunächst nur eines für den jeweiligen lokalen Zugriff auf den Computer definieren und nach Abschluss der Installation sofort ändern.
- *Mit Hilfe von Verteilung von Disk-Images*
  - Bei dieser Methode wird über spezielle Programme ein bitweises Abbild (Image) der spezifizierten Partition erzeugt, welches auf einem anderen Computersystem wieder auf der Festplatte eingefügt werden kann.
- *Über Remoteinstallationsdienste* (siehe auch Punkt 3.1.3)

5. Produktaktivierung

5.1 Produktaktivierung

Windows XP lässt einen Start ohne Produktaktivierung nur während der ersten 30 Tage zu. Danach muss das Produkt durch entsprechende Registrierung aktiviert werden. Diese Zwangsaktivierung soll Microsoft vor Raubkopieren schützen. Bei der

Produktaktivierung wird ein 50-stelliger Code per Web oder Telefon an Microsoft übermittelt. Darin sind verschiedene Merkmale des Computers gespeichert. Die 50 Stellen reichen allerdings nicht aus, um das genaue Modell zu übermitteln.

Folgende Daten prüft und verschickt Windows XP:

- Seriennummer der Windows-Partition
- MAC-Adresse der Netzwerkkarte
- CD-ROM-ID-Nummer
- Grafikkarten-ID-Nummer
- Prozessor-ID-Nummer
- Festplatten-ID-Nummer
- SCSI-Adaptter-ID-Nummer
- IDE-Controller-ID-Nummer
- Modell des Prozessors
- Größe des RAM.

Nachdem Windows XP aktiviert wurde, dürfen laut Hersteller nur noch geringfügige Änderungen am System vorgenommen werden, bevor eine erneute Aktivierung fällig wird. Dabei ist wichtig, ob am normalen PC oder am Notebook mit Dockingstation gearbeitet wird. Am normalen PC sind bis zu drei Änderungen möglich, am Notebock können es bis zu sechs Änderungen an der Hardware sein. (Bei einem Notebook, das an eine Docking-Station anschließbar ist, werden Grafikkarte und SCSI-Host-Adapter nicht in die Berechnung einbezogen.)
Die Microsoft Produktaktivierung ist bei Paket-, OEM-, System Builder-Produkten und Lizenzen für Schüler, Studierende und Lehrkräfte erforderlich. Die Microsoft Volumenlizenzprogramme sind hiervon ausgenommen, das heißt, sie müssen nicht aktiviert werden.

5.2 Übertragung personenbezogener Daten bei der Produktaktivierung

Der TÜViT hat im Auftrag der Microsoft Deutschland GmbH die Produktaktivierung der Microsoft Produkte Windows XP, Office XP und Visio 2002 geprüft. Dabei sind die Mitarbeiter zu folgendem Resultat gekommen:

In den untersuchten Programmteilen wurden keinerlei Anhaltspunkte gefunden, dass personenbezogenen Daten automatisch über das Internet übertragen werden. Erst wenn ein Benutzer auch eine freiwillige Registrierung durchführt, werden nach Abfrage der expliziten Zustimmung personenbezogene Daten übertragen. Dies gilt entsprechend auch für eine telefonische Registrierung.
Der Technische Überwachungsverein stellte dem Betriebssystem Windows XP in Bezug auf die Produktaktivierung zwar eine Unbedenklichkeitsbescheinigung in Sachen

Datenschutz aus. Fragwürdig bleibt diese Zwangsregistrierung dennoch, insbesondere weil Microsoft nichts zur Art und Weise der künftigen Verwendung der gesammelten Informationen sagt. Dass die Nutzung vieler verbesserter Merkmale von Windows XP eine Internet-Verbindung quasi zwingend voraussetzt, macht viele Anwender zusätzlich skeptisch, da Sicherheitsprobleme bei der Internetanbindung die Schwachstelle des Systems zu sein scheinen.

6. Sicherheit im Netzwerk

6.1 Schutz nach außen

Der Schutz vertraulicher Daten bei der Übermittlung über das Internet von einem lokalen Computer oder einem Büronetzwerk ist heute zunehmend schwierig. Durch Festverbindungen und Flatrates sind Ports auf lokalen Rechnern mit entsprechender Software wie Portscannern leicht zu orten. Auch dynamische IP-Adressen bieten keinen Schutz davor, dass inzwischen ganze Netzwerke gescannt werden. Es ist beobachtet worden, dass bereits nach 20 Minuten Online-Zeit erste Scannerzugriffe erfolgten. Erkennt der Angreifer dann offene Ports, die Systemdienste anbieten, kann er darüber versuchen, Zugriff auf das System zu erlangen.

Grundsätzlich gilt: Je länger die Verbindung, desto größer die Angriffswahrscheinlichkeit.

Gefährdet sind Computer und Netzwerke aber auch oft durch mangelnde Sensibilität der Anwender. Die Meinung: „Wer sollte mich schon angreifen?“ ist nach wie vor sehr verbreitet, angesichts der Möglichkeiten von Windows XP jedoch völlig fehl am Platz. Die zahlreichen, scheinbar ziellosen Portscans zeigen, dass zunächst keine auf bestimmte Personen bezogene Angriffe gefahren werden. Oft werden einfach irgendwelche offene Computer gesucht, um dort trojanische Pferde zu installieren. Diese schaden nicht zwangsläufig direkt den befallenen Computer, sondern greifen nach entsprechender Anweisung von außen das eigentliche Opfer an. Selbst stark abgesicherte Systeme sind angreifbar, indem extrem viele Anfragen, möglichst mit fehlerhaften Paketen, gestartet werden (Denial-of-Service-Attacken). Dass hierbei die Angriffe von unwissenden Anwendern weltweit verteilt sind, macht eine Abwehr fast unmöglich. Dem Angegriffenen bleibt oft keine andere Wahl als den Server abzuschalten.

6.2 Sicherheitsprotokolle für das Netzwerk

6.2.1 Kerberos – sichere Authentifizierung

Wie schon Windows 2000, so verwendet auch XP zur sicheren Authentisierung im Netzwerk das Kerberos-Protokoll. Kerberos ist als zentraler Sicherheitsstandard in

Windows 2000/XP und in Active Directory (siehe auch Punkt 11) implementiert. Kerberos verwendet zum einen ein Verschlüsselungsverfahren für die Schlüssel selbst, zum anderen so genannte Zeittickets, die den Ablauf der Übertragung kontrollieren. Microsoft hat den Kerberos-Standard weiter entwickelt, so dass nun auch Zertifikate mit öffentlichen Schlüsseln eingesetzt werden können. Diese Schlüssel werden mit dem Zertifikatserver erstellt, der nur in der Windows 2000 Server-Familie verfügbar ist.

6.2.2 Sicherer Datentransfer – IPSec

Mit IPSec (IPSecurity) ist in Windows XP wie bereits in Windows 2000 eine Technologie implementiert, die Daten auf IP-Ebene verschlüsselt, und somit vor Abhörangriffen und unbefugten Veränderungen schützen soll. Für Applikationen bleibt dieser Vorgang transparent. IPSec erlaubt den einfachen Aufbau sicherer Verbindungen auf Betriebssystemebene, ohne dass die Anwendungen speziell dafür ausgelegt sein müssen. Mit IPSec lässt sich der Datenverkehr im LAN (Lokal Network Area) und im WAN (Wide Area Network) schützen. Es schützt gleichermaßen vor den Angriffen Interner und Externer. Diese Dienstesammlung basiert auf der DES (Data Encryption Standard) – oder 3DES-Verschlüsselung und kann auch auf getunnelte Verbindungen wie z. B. L2TP (Layer 2 Tunneling Protocol) aufsetzen (siehe auch Punkt 6.2.3). IPSec bietet ein höheres Maß an Sicherheit als PPTP (Point to Point Tunneling Protocol) und wird wohl langfristig PPTP ablösen. IPSec bietet zwei verschiedene Betriebsmodi: den Transportmodus und den Tunnelmodus. Im Transportmodus wird nur der Datenteil des zu transportierenden IP-Paketes verschlüsselt, im Tunnelmodus wird das komplette IP-Paket verschlüsselt und mit einem neuen IP-Kopf und dem IPSec-Kopf versehen.

6.2.3 L2TP (Layer 2 Tunneling Protocol)

Das Tunneling von Datenpaketen über IP gewinnt immer mehr Bedeutung für den Aufbau Virtueller Privater Netzwerke (VPN). Der Transport von Daten erfolgt hierbei über das Netzwerk in abgeschlossenen (privaten) Einheiten. Damit die Daten auch sicher sind, werden sie einzeln verpackt und über TCP/IP-Protokoll „getunnelt“ verschickt. Bisher wurde bei Windows das Point-to-Point Tunneling Protocol (PPTP) verwendet. Da andere Systeme aber auch mit anderen Standards arbeiten, unterstützt Microsoft mit Windows XP neben PPTP jetzt auch L2TP. Da dieses Protokoll von sich aus keine Verschlüsselung unterstützt, kann hierbei IPSec zum Einsatz kommen (siehe auch Punkt 6.2.2).

Vergleich von PPTP gegenüber L2TP

L2TP unterscheidet sich nur in wenigen Punkten von PPTP. PPTP und L2TP verwenden die Datenverbindungsschicht (Ebene 2) und packen die Datenpakete in Frames

des Punkt-zu-Punkt-Protokolls. L2TP unterstützt mehrere Tunnel. PPTP arbeitet nur über IP-Netzwerke. Der Vorteil von L2TP gegenüber PPTP ist, dass es direkt über die verschiedenen WAN übertragen werden kann, aber optional auch über den Umweg IP funktioniert.

6.3 Internetverbindungsfirewall

Die Internetverbindungsfirewall soll den Computer schützen, auf dem sie aktiviert ist. Bei den meisten Heim- bzw. kleinen Büronetzwerken ist dies der so genannte ICS-Hostcomputer (Internet Connection Sharing), also der Computer, der die DFÜ-Verbindung zum Internet herstellt. Ohne dass weitere DFÜ-Verbindungen aufgebaut werden müssen, können alle Computer im Heim- oder im kleinen Büronetzwerk mit dem Internet verbunden werden, da sie die vom ICS-Host aufgebaute Verbindung gemeinsam nutzen können. Eine Internetverbindung über die vorhandene DFÜ-Verbindung können andere Computer im Netzwerk nur dann herstellen, wenn ICS auf dem ICS-Host aktiviert ist. Die Adressen der Clientcomputer erscheinen nicht im Internet, nur der gemeinsam genutzte Host ist öffentlich sichtbar.

Die Firewall schützt dann bei Aktivierung jede beliebige Internetverbindung. Die Firewall speichert Kommunikationsdaten, Sende- und Empfangsadressen von jeder Verbindung zwischen dem Internet und dem Computer und verwaltet sie in einer Tabelle. Daten von nicht erwarteten Adressen werden abgewiesen. Sind Zugriffe auf den Computer aus dem Internet beispielsweise über http, ftp oder andere Dienste gewollt, so müssen diese extra konfiguriert werden.

Die Remoteunterstützung wird hingegen nicht eingeschränkt (siehe auch Punkt 6.4). Sie ist immer in beiden Richtungen möglich. Während eines Remotezugriffs ist der Schutz durch die Firewall weitgehend aufgehoben, und das gesamte System ist dadurch verwundbar.

Die Windows XP Firewall bietet kleinen Netzwerken, die mit dem Internet verbunden sind, nur eine sehr trügerische Sicherheit. Wird nämlich der Windows Messenger oder andere MS Software gestartet, dürfen Multimedia-Dateien die Firewall ungehindert passieren. Das Desinteresse ausgehenden IP-Paketen gegenüber stellt ein erhebliches Sicherheitsrisiko dar. Ins System eingedrungene Trojaner können trotz der integrierten Firewall ungehindert eine Verbindung ins Netzwerk oder Internet aufnehmen. Der Schutz durch die integrierten Firewall ist zwar besser als gar kein Schutz. Trotzdem sollte das System zusätzlich mit einer externen Firewall abgesichert werden, die auch ausgehende Daten kontrolliert, damit beide Richtungen abgesichert sind.

Standardmäßig ist die in Windows XP integrierte Firewall abgeschaltet. Unter *Systemsteuerung/Netzwerk- und Internetverbindungen/Netzwerkverbindungen* rechte Maustaste *Eigenschaften* Registrierkarte *Erweitert* sollte sie zugeschaltet werden.

6.4 Remote Zugriff

Bei der Remoteunterstützung wird einem bestimmten autorisierten Personenkreis gestattet, über das Web, auf den entfernten Computer zuzugreifen.

http://windows.microsoft.com/RemoteAssistance/RA.asp

Die Autorisierung der Remotebenutzer erfolgt in den *Systemeinstellungen/Leistung* und Wartung/System Registerkarte Remote unter Remotedesktop, Remotebenutzer auswählen.

Voraussetzungen für einen Remote-Zugriff sind:

- Der Clientcomputer sowie der Remotecomputer müssen entweder Windows Messenger oder ein MAPI-kompatibles E-Mail-Konto, wie z. B. Microsoft Outlook oder Outlook Express, verwenden.
- Der Clientcomputer sowie der Remotecomputer müssen über eine Internetverbindung verfügen, während Sie die Remoteunterstützung verwenden.

Externe Firewalls können bei entsprechender Konfiguration die Remoteunterstützung verhindern.

Eine Anmeldung ohne Kennwort kann bei Windows XP nur direkt an der Konsole des physischen Computers erfolgen. Standardmäßig können Konten mit leeren Kennwörtern nicht mehr für eine Remoteanmeldung an dem Computer verwendet werden. Die Einschränkung, die eine Anmeldung über ein Netzwerk verhindert, kann aufgehoben werden, indem einem lokalen Konto ein Kennwort zugewiesen wird.

Remoteinstallation

Über die Remotinstallationsdienste kann Windows XP Professional auf einem Computer über das Netzwerk installiert werden. Der zu installierende Client-PC wird über eine bootfähige Netzwerkkarte oder eine spezielle Bootdiskette gestartet und kann nach der Verbindung mit dem RIS-Server (Remote Installation Services) mit Windows XP installiert werden.

Risiken eines Remotezugriffs

Schon allein die zusätzliche Schnittstelle gefährdet die Sicherheit und Zuverlässigkeit der Ressourcen, unabhängig vom verwendeten Remote System. Zum einen besteht eine erhöhte Virengefahr, zum anderen ein erhöhtes Risiko des Zugriffs durch unbefugte Benutzer auf das Unternehmensnetzwerk. Neben der obligatorischen Authentisierung durch Benutzernamen und Passwort sollten unbedingt weitere Möglichkeiten zum Schutz der Ressourcen genutzt werden (z. B. Smartcards). Wichtig ist in diesem Zusammenhang auch der Schutz offen zugänglicher Telefonanschlüsse, die zum übertragen von Codes genutzt werden.

Ein Remotezugriff sollte nur dann eingerichtet werden, wenn dies zwingend erforderlich ist und nach Abwägung der damit verbundenen Risiken vertretbar ist.

6.5 Der Internet Explorer 6

Da der Internet Explorer 6 standardmäßig mit Windows XP ausgeliefert wird, folgt hier eine kurze Sicherheitsbetrachtung.

Der Internet Explorer unterteilt das Internet in Zonen, so dass jeder Web-Seite eine Zone mit einer geeigneten Sicherheitsstufe zugewiesen werden kann. Bei dem Versuch, Inhalte aus dem Web zu öffnen oder herunter zu laden, überprüft der Internet Explorer die Sicherheitseinstellungen für die Zone dieser Web-Seite. Das Einstellen der *Internetoptionen* erfolgt auf der Registrierkarte SICHERHEIT.

Es gibt vier verschiedene Zonen:

- Internet
- Lokales Intranet
- Vertrauenswürdige Sites
- Eingeschränkte Sites

Für jede Zone gibt es Sicherheitsstufen von „SEHR NIEDRIG“ bis „HOCH“ sowie „BENUTZERDEFINIERT“. Unter anderem lässt sich einstellen, ob aktive Inhalten ausgeführt werden dürfen. Da kaum nachvollzogen werden kann, welche Auswirkungen aktive Inhalte haben können, sollten sie grundsätzlich deaktiviert werden. Je mehr Sicherheitsfunktionen zur Minimierung Sicherheitsrisiken aktiviert werden, um so stärker können natürlich die Nutzmöglichkeiten einiger Websites eingeschränkt werden.

6.6 Cookies

Auf der Registerkarte DATENSCHUTZ können Sie das Verhalten des Internetexplorers gegenüber Cookies einstellen. Folgende Cookieeinstellungen sind verfügbar:

ALLE ANNEHMEN	Alle Cookies werden ohne Rückfrage akzeptiert.
NIEDRIG	Cookies, die nicht zur aufgerufenen Webseite passen, werden abgelehnt.
MITTEL	Cookies, die nicht zur aufgerufenen Webseite passen, werden abgelehnt. Außerdem werden Betreiber der Website gesperrt, wenn bekannt ist, dass diese persönliche Informationen verwenden.

MITTELHOCH	Cookies werden abgelehnt, wenn Drittanbieter, die nicht zur aufgerufenen Website passen, keine ausdrückliche Zustimmung des Benutzers anfordern.
HOCH	Ebenso wie MITTELHOCH, jedoch auch für den Betreiber der aufgerufenen Website selbst geltend.
ALLE SPERREN	Alle Cookies werden gesperrt.

Die automatische Verwaltung von Cookies sollte aus Sicherheitsgründen abgeschaltet werden.

7. Passport - der Weg zum gläsernen Internet-Surfer?

Um die Einwahl in verschieden Internetdienste zu vereinfachen, bietet Windows XP die Anmeldung über den Dienst „Passport“ an. Durch einen Passport kann dann ausschließlich durch Verwendung einer E-Mail-Adresse auf alle MSN Internetzugangs-Websites und anderen Dienste und Websites, die Passports unterstützen, zugegriffen werden. Passport implementiert einen Anmeldedienst, der es ermöglicht, mit einem Benutzernamen und einem Kennwort alle .NET-Passport-kompatiblen Dienste nutzen.

Die Nutzung von Passport ist aus datenschutzrechtlicher Sicht nicht unbedingt zu befürworten. Hier teilen sich alle Anbieter ein und dieselbe Datenbank, denselben Login-Mechanismus und dieselbe Sicherheitstechnik. Die Weiterleitung im Browser erfolgt ohne SSL, was bereits ausreicht, um in einen Account einzudringen.

Experten warnen davor, bei der Passport-Anmeldung die geforderten persönlichen Daten einzugeben. Damit könnte Microsoft jeden Computernutzer zusammen mit der eindeutigen 64-Bit-Nummer identifizieren. Sobald sich der Verbraucher bei einer Website anmeldet, die mit Microsoft kooperiert, wird seine Identifizierung an den Betreiber dieser Website übermittelt. Hinzu kommt, dass das Netz der über diesen Dienst zugänglichen Anbieter noch nicht sehr weit ausgebaut ist, so dass es sich für den Nutzer bisher kaum lohnt, diesen Dienst in Anspruch zu nehmen.

Wenn der Passport-Dienst nicht genutzt wird, stehen alle weiteren Funktionen von Windows XP uneingeschränkt zur Verfügung.

8. Gravierendes Sicherheitsleck: UPnP (Universal Plug and Play)

UPnP gehört zu den Innovationen, die den Umgang mit Hardware im Netzwerk vereinfachen sollen. Vernetzte Geräte teilen automatisch ihre Anwesenheit anderen UPnP-fähigen Geräten mit, die sich daraufhin bereitwillig auf die Zusammenarbeit

einlassen. UPnP wird bei jeder Standard-Installation von Windows XP eingerichtet und aktiviert, und kann auch Microsofts früheren Betriebssystemversionen Windows 98, 98SE oder ME manuell hinzugefügt werden.

UPnP erfordert keinerlei Interaktion mit dem Benutzer. Aufgrund schwerwiegender Fehler in der UPnP-Implementierung in Windows XP kann ein Angreifer durch einen Puffer-Überlauf uneingeschränkte Kontrolle über das System erlangen, Daten lesen und löschen, Programme installieren und DDoS-Angriffe ausführen, sogar ohne in das System einzudringen. Von diesem Problem ist laut Microsoft jede Installation von Windows XP betroffen, denn die UPnP-Funktionalität ist standardmäßig aktiviert. Der Hersteller selbst veröffentlichte am 20. Dezember 2001 eine deutschsprachige Reparatursoftware für XP für diesen von unabhängigen IT-Sicherheitsforschern entdeckten Fehler.

Der von Microsoft zur Verfügung gestellte Patch kümmert sich jedoch lediglich um die Verwundbarkeit; UPnP wird dadurch nicht deinstalliert. Am sichersten ist es UPnP vollständig zu entfernen und die Ports 5000 und 1900 zu schließen.

9. Interne Sicherheit

9.1 SmartCards

Unter XP ist die Unterstützung von SmartCards *direkt* im Betriebssystem integriert. Die kleinen scheckkartengroßen Kärtchen eignen sich beispielsweise zum Speichern von Sicherheitszertifikaten, Anmeldekennwörtern, privaten Schlüsseln sowie anderen persönlichen Informationen. Im Gegensatz zu einem Kennwort wird die PIN, die den Zugriffsschutz zur SmartCard realisiert, niemals im Netzwerk weitergeleitet, und bietet somit einen höheren Schutz als ein herkömmliches Kennwort. SmartCards lassen nur eine beschränkte Anzahl von fehlgeschlagenen Versuchen zur Eingabe der richtigen PIN zu. Dann werden sie gesperrt und funktionieren dann auch bei Eingabe der richtigen PIN nicht mehr. Der Benutzer muss sich zum Entsperren der Karte an den Systemadministrator wenden.

Vorteil bei der Verwendung dieser Technologie ist die stark vereinfachte Authentifizierungsprozedur, besonders wenn im Active Directory (siehe Punkt 11) die Anmeldung für verschiedenste Dienste zusammengefasst wird.

9.2 Integrierte „Sandbox“

Windows XP verfügt über eine integrierte „Sandbox“, um Anwendungen in einem geschützten Bereich ablaufen zu lassen und somit Manipulationen und Beschädigungen am System zu verhindern.

9.3 Windows-Dateischutz

Bei Windows-Versionen vor Windows 2000 war nicht auszuschließen, dass bei der Installation von Software, die zusätzlich zum Betriebssystem gebraucht wurde, freigegebene Systemdateien, z. B. Dynamic Link Libraries (DLL-Dateien) und ausführbare Dateien (EXE-Dateien), ohne jede Nachfrage überschrieben wurden. Wenn Systemdateien überschrieben werden, wird die Leistung des Systems unvorhersehbar, Programme können sich fehlerhaft verhalten und das Betriebssystem kann versagen.

In Windows 2000 und Windows XP verhindert der Windows-Dateischutz, dass geschützte Systemdateien, z. B. Dateien mit den Erweiterungen SYS, DLL, OCX, TTF, FON und EXE, überschrieben werden. Der Windows-Dateischutz wird im Hintergrund ausgeführt und schützt alle Dateien, die durch das Windows Setup-Programm installiert wurden. Der Windows-Dateischutz erkennt auch Versuche von anderen Programmen, eine geschützte Systemdatei zu ersetzen oder zu verschieben. Um festzustellen, ob es sich bei der neuen Datei um die korrekte Microsoft-Version handelt, wird ihre digitale Signatur vom Windows-Dateischutz überprüft. Falls die Datei nicht die korrekte Version aufweist, ersetzt der Windows-Dateischutz diese Datei entweder durch die Sicherungskopie, die im Ordner *Dllcache* gespeichert ist, oder durch die entsprechende Datei von der Windows-CD. Wenn der Windows-Dateischutz die entsprechende Datei nicht finden kann, werden Sie aufgefordert, den Speicherort anzugeben. Zusätzlich wird der versuchte Dateiaustausch vom Windows-Dateischutz im Ereignisprotokoll aufgezeichnet.

Der Windows-Dateischutz ist standardmäßig aktiviert und ermöglicht es, vorhandene Dateien durch digital signierte Windows-Dateien zu ersetzen. Derzeit werden signierte Dateien auf folgenden Wegen bereitgestellt:

- Windows Service Packs,
- Hotfix-Distributionen,
- Betriebssystemupdates,
- Windows-Aktualisierung,
- Windows Geräte-Manager/Klasseninstallationsprogramm.

9.4 Offline Dateien

Offline Dateien werden verwendet, um auf dem Netzwerk gespeicherte Dateien und Programme auch dann noch nutzen zu können, wenn keine Internetanbindung mehr besteht. Temporäre Offlinedateien werden auch als automatisch zwischengespeicherte Dateien bezeichnet. Diese freigegebenen Netzwerkdateien werden automatisch gespeichert. Diese Dateien müssen nicht gesondert offline verfügbar gemacht werden.

Windows kann sie jederzeit von Ihrem lokalen Cache entfernen, wenn mehr Speicherplatz für weitere temporäre Dateien benötigt wird. Die freigegebenen Netzwerkdateien, die ausdrücklich offline verfügbar gemacht worden sind, stehen immer zur Verfügung. Diese Dateien werden erst dann vom Computer entfernt, wenn sie gelöscht werden. Wenn man sichergehen will, dass z. B. bei Übergabe eines Notebooks an eine andere Person keine Daten im Offline-Cache verbleiben, sollte der Cache gelöscht werden.

9.5 EFS (Encrypting File Systems)

Mit Hilfe von EFS können Daten auf der Festplatte vor unbefugtem Zugriff wirksam geschützt werden. Eine direkte Integration in den Windows Explorer gestattet die einfache Nutzung der Datenverschlüsselungsfunktion. Allein das Aktivieren des entsprechenden Kontrollkästchens reicht aus, um einen Ordner oder eine Datei verschlüsseln zu lassen. Dabei arbeitet der Dateisystemfilter des EFS völlig transparent, Ver- und Entschlüsselungsvorgänge laufen unsichtbar im Hintergrund ab.

Die verschlüsselte Datei kann nur noch durch die berechtigten Benutzer geöffnet, umbenannt, kopiert oder verschoben werden. Alle anderen Benutzer werden abgewiesen. Neu ist bei Windows XP, dass Sie mehr als einem Benutzer den Zugriff auf eine EFS-verschlüsselte Datei gestatten können.

Beim EFS wird die Datei zunächst symmetrisch mit einem FEK (File Encryption Key) verschlüsselt. Der FEK wird wiederum mit einem öffentlichen Schlüssel aus dem öffentlichen/privaten Schlüsselpaar des Anwenders verschlüsselt. Um eine Wiederherstellung verschlüsselter Daten auch ohne den privaten Schlüssel des Anwenders zu ermöglichen, z. B. nach Verlust des Schlüssels oder dem Ausscheiden eines Mitarbeiters, wird der FEK auch mit dem öffentlichen Schlüssel des öffentlichen/privaten Schlüssels des Wiederherstellungsagenten verschlüsselt. Entschlüsseln können diese Daten nur autorisierte Benutzer und designierte Wiederherstellungsagenten. Die Datei selbst kann auch vom Nutzer mit Administratorrechten nicht geöffnet werden, wenn er nicht als Wiederherstellungsagent bestimmt wurde.

Das Wiederherstellungsrecht besitzt unter Windows XP der Administrator standardmäßig. Für eine Sicherung der verschlüsselten Dateien vor dem Zugriff des Administrators kann das Wiederherstellungszertifikat des Administrators gelöscht werden. Dann sind die verschlüsselten Dateien eines Benutzers nur noch mit dessen Zertifikat entschlüsseln. Zusätzlich oder alternativ zu den genannten Administratoren können weitere Benutzer als Wiederherstellungs-Agenten bestimmt werden; dies geschieht durch Eintragen in der Sicherheitsrichtlinie unter *Richtlinien öffentlicher Schlüssel/Agenten für Wiederherstellung verschlüsselter Daten*. Als Wiederherstellungs-Agenten können nur einzelne Benutzer, nicht jedoch ganze Gruppen bestimmt werden. Zur Sicherheit sollten so wenig Wiederherstellungsagenten eingerichtet

werden wie möglich. Im Regelfall ist eine entsprechende Berechtigung ausreichend. In der verschlüsselten Datei kann der Benutzer unter Eigenschaften/erweitert/Details Verschlüsselungsdetails einsehen, Zugriffsrechte für weitere Benutzer festlegen und Informationen zum den Wiederherstellungsagenten erhalten.

Alle EFS-Vorgänge werden auf dem Computer ausgeführt, auf dem sie gespeichert sind. Beim Kopieren einer verschlüsselten Datei über das Netzwerk wird sie entschlüsselt und im Zielordner wieder verschlüsselt. Sie ist damit auf dem Transportweg über das lokale Netzwerk oder die Datenfernverbindung prinzipiell lesbar. Für einen sicheren Netztransfer sollte deshalb beispielsweise IPSec genutzt werden (siehe Punkt 6.2.2).

10. ASR (Automated System Recovery)

In regelmäßigen Abständen sollten zur eigenen Sicherheit automatische Systemwiederherstellungssätze im Rahmen eines Gesamtplanes zur Systemwiederherstellung bei Systemversagen erstellt werden.

ASR ist ein zweiteiliges Wiederherstellungssystem, das aus den Teilen ASR-Sicherung und ASR-Wiederherstellung besteht. Die Sicherung erfolgt durch den Assistenten für die automatische Systemwiederherstellung, der im Sicherungsdienstprogramm zu finden ist. Der Assistent sichert Systemstatus, Systemdienste und alle mit den Betriebssystemkomponenten verknüpften Datenträger. Er erstellt auch eine Datei mit Informationen zur Sicherung, zur Datenträgerkonfigurationen (einschließlich Basisvolumes und dynamischer Volumes) und zur Durchführung einer Wiederherstellung.

Die automatische Systemwiederherstellung sollte erst als letztes Mittel zur Systemwiederherstellung eingesetzt werden, wenn andere Möglichkeiten, wie Starten im abgesicherten Modus und Wiederherstellen der letzten als funktionierend bekannten Konfiguration, nicht greifen.

Um Datenverluste zu vermeiden, sollten Dateien, die nicht dem von Microsoft vorgeschriebenen Dateitypen entsprechen bzw. nicht in den von Microsoft dargebotenen Verzeichnissen gespeichert werden, auf einer anderen Partition gespeichert werden, die dann von der Wiederherstellung ausgenommen wird.

11. Active Directory

Active Directory ist ein Verzeichnisdienst, der Informationen zu Objekten und Subjekten in einem Netzwerk speichert, und diese Informationen Benutzern und Netzwerkadministratoren zur Verfügung stellt. Active Directory ermöglicht Netzwerkbenutzern über einen einzigen Anmeldevorgang den Zugriff auf zugelassene

Ressourcen im gesamten Netzwerk. Es stellt Netzwerkadministratoren eine anschauliche, hierarchische Ansicht des Netzwerkes und einen einzigen Verwaltungspunkt für alle Netzwerkobjekte zur Verfügung.

Zur Pflege des Directorys gehören das Erstellen, Löschen, Ändern und Verschieben von Objekten sowie das Festlegen von Berechtigungen für Objekte, die im Verzeichnis gespeichert sind. Diese Objekte umfassen Organisationseinheiten, Benutzer, Kontakte, Gruppen, Computer, Drucker und freigegebene Dateiobjekte. Für die Wahrung der Sicherheit im Active Directory sollte die entsprechende primäre Netzwerkanmeldung mit den betreffenden Gruppenrichtlinien abgestimmt sein.

Die dem Active Directory (AD) zugrunde liegenden Überlegungen führen mitunter zu sehr umfassende AD-Strukturen. So werden in zunehmendem Maße landesweite, ressortübergreifenden AD angelegt. Dabei können Client-Server-Systeme, die bislang unabhängig voneinander zum Teil von der Verwaltung und zum Teil auch von externen Dienstleistern administriert wurden, in einer Administrationsstruktur zusammengefasst werden. Die Active Directory Technik sieht standardmäßig die Rolle der so genannter Enterprise-Administratoren vor. Diese haben Administrationsberechtigungen für das gesamte AD. Damit können die Enterprise-Administratoren auf sämtliche Daten zugreifen, die in den angeschlossenen Client-Server-Systemen gespeichert sind. Zwar kann man die damit verbundenen Zugriffsberechtigungen einschränken, jedoch können sich die Enterprise-Administratoren die entsprechenden Zugriffsberechtigungen jederzeit wieder selbst gewähren. Es ist daher notwendig, die Nutzung der „allmächtigen“ Enterprise-Administrator-Kennungen einzugrenzen. Dazu bieten sich mehrere Ansatzpunkte:

- Verzicht auf „integrative” AD, in denen bislang separat administrierte Client-Server-Systeme zusammengefasst werden,
- möglichst weitgehender Verzicht auf Enterprise-Administrator-Kennungen im Tagesbetrieb; stattdessen werden dafür Kennungen mit (beschränkten) Administrationsrechten verwendet; ob die damit einhergehenden funktionalen Beschränkungen tragbar sind, ist von Fall zu Fall zu entscheiden,

- sollen nur zwei bislang unabhängig voneinander administrierte Client-Server-Systeme in einem AD zusammengefasst werden, kann als organisatorische Maßnahme die Nutzung der Enterprise-Administrator-Kennung nach dem Vier-Augen-Prinzip in Betracht kommen.

12. Sicherheitsempfehlungen

Nutzer sollten der Benutzergruppe für Remotedesktop auf dem eigenen Computer angehören. Sie müssen keinesfalls als Administrator angemeldet sein, um Remotezugriff auf den Computer zu haben. Standardnutzer sollten prinzipiell nicht der Gruppe

Administratoren angehören und den Computer nicht als Administrator starten, es sei denn, sie müssen Aufgaben wahrnehmen, für die Administratorrechte erforderlich sind. Für die meisten Computeraufgaben reicht jedoch die Mitgliedschaft in der Gruppe *Benutzer* oder *Hauptbenutzer*. Wenn jedoch eine administratorspezifische Aufgabe ausgeführt werden muss, sollte man sich so kurzzeitig wie möglich als Administrator anmelden, und sofort nach der Erledigung der entsprechenden Aufgabe abmelden.

Alle Remotedesktopbenutzer sollten sich nur mit einem sicheren Kennwort anmelden. Dies ist besonders wichtig, wenn Ihr Computer direkt über ein Kabelmodem oder eine DSL-Verbindung an das Internet angeschlossen ist.

12.1 Warum man sich an seinem Computer nicht standardmäßig als Administrator anmelden sollte

Wenn Windows 2000 oder Windows XP mit Administratorrechten gestartet wird, ist das System besonders hohen Sicherheitsrisiken ausgesetzt. Viren oder trojanische Pferde könnten auf dem System dann wesentlich schwerwiegendere Probleme verursachen, als bei einer weniger hoch privilegierten Anmeldung.

Wenn man sich als Mitglied der Gruppe *Benutzer* anmeldet, kann man bereits sehr viele Routineaufgaben durchführen, wie das Ausführen von Programmen und das Besuchen von Internetseiten, ohne den Computer einem unnötigen Risiko auszusetzen. Als Mitglied der Gruppe *Hauptbenutzer* können neben diesen Routineaufgaben auch Programme installiert, Drucker hinzugefügt und die meisten Programme der Systemsteuerung verwendet werden. Administratoraufgaben, wie das Aktualisieren des Betriebssystems oder das Konfigurieren von Systemparametern, können dann nur durchgeführt werden, nachdem sich der Anwender als Standardnutzer abgemeldet und erneut als Administrator anmeldet hat.

12.2 Tipps zum Testen der Systemsicherheit

Mit einem simulierten Angriff von außen können Sicherheitseinstellungen des Systems schnell getestet werden. Bevor man mit der Konfiguration beginnt, sollte beispielsweise folgende Website besucht werden: *https://grc.com/x/ne.dll?bh0kyd2* (Testseite der Gibson Research Corporation). Auf dieser Seite kann mit den Funktionen „TEST MY SHIELDS“ oder „PROBE MY PORTS“ die Sicherheit des Systems getestet werden. Der gesamte Test dauert – über eine DSL-Verbindung – nur wenige Sekunden. Genauso schnell wäre bei entsprechender Fehlkonfiguration auch ein Angreifer über alle Schwachstellen des Systems im Bilde. Der Test eignet sich auch gut zur Kontrolle der Protokollierungsfunktion der Firewall, da die IP-Adressen, von denen der simulierte Angriff erfolgt, offen gelegt werden. Dadurch ist gut nachvoll-

ziehbar, wann die Aktion vom berechtigten Nutzer ausgelöst und welche Wirkung erzielt wurde.

Weitere Hinweise zu Selbsttests sind auch beim „Landesbeauftragten für den Datenschutz Niedersachsen“ unter *www.lfd.niedersachsen.de/service/service_selbstt.html/* oder beim Schweizer Datenschutzbeauftragten unter *www.datenschutz.ch* zu erhalten.

13. Windows XP Home

Um die Sicherheit der Version XP Home einschätzen zu können, sollte man wissen, dass die folgenden im vorangegangenen Text beschriebenen Merkmale nicht zur Verfügung stehen:

- EFS
- Kerberos
- IPSec
- Internet Information Server
- Remotedesktop
- Automatische Installation
- Remotinstallationsdienste
- Offline-Dateien und Ordner
- Gruppenrichtlinien
- Managementkonsole

14 Der Windows XP Media Player

Der Media Player dient der Wiedergabe vielfältiger Sound- und Videoformate. Der Einsatz des XP Media-Players bietet Microsoft die Möglichkeit, über die Internetverbindung seinen Nutzer zu identifizieren. Microsofts Mediaplayer für Windows XP verrät, welcher Anwender welche Musikstücke und Videos abspielt. Die Software identifiziert zugleich mit dem Anmeldenamen des jeweiligen Windows-Benutzers die abgespielten Stücke, und schreibt diese Informationen hinter dem Rücken des Anwenders in eine Logdatei auf die Festplatte. Das geht einen Schritt weiter als etwa Office-Programme, die sich maximal neun zuletzt bearbeitete Dokumente merken, um dem Anwender das wiederholte Eintippen von Dateinamen zu ersparen.

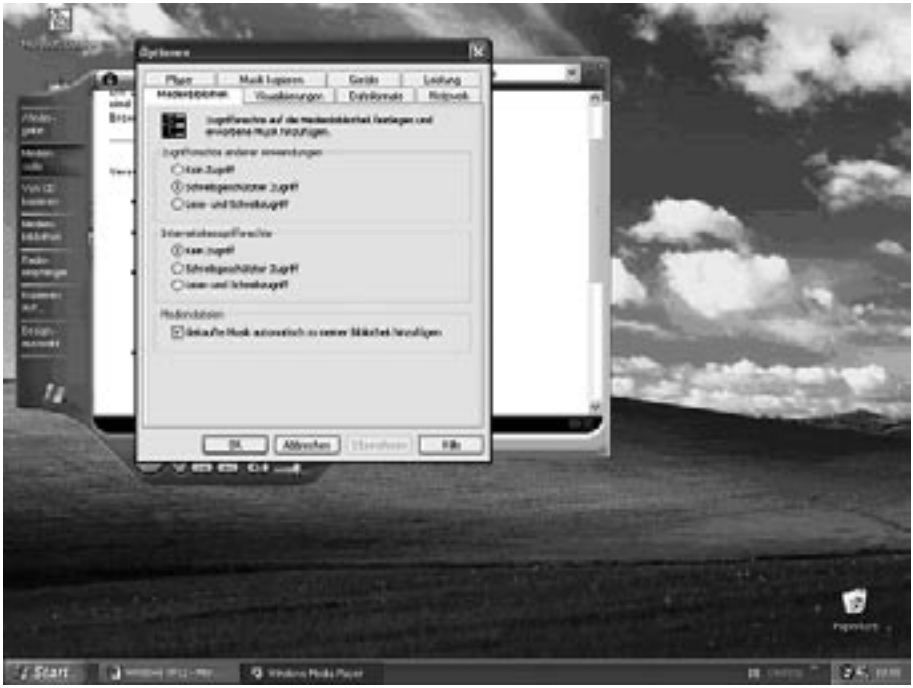
14.1 Welche Daten erhält Microsoft tatsächlich?

Der Multimediaplayer zieht sich aus dem Netz die Angaben zum gespielten Titel und zum entsprechenden Künstler. Gleichzeitig verschickt das Programm die Medien-ID

der eingelegten CD, den der Mediaplayer von der CD ausliest, sowie die Identifikationsnummer des installierten Mediaplayers. Die Übermittlung der Identifikationsnummer gibt zunächst keine Auskunft über den Benutzer und verstößt somit nicht gegen Datenschutzauflagen. Bedenklich ist jedoch, dass dieselbe Identifikationsnummer z. B. bei der Anmeldung für den Windows Media Newsletter zusammen mit Name und E-Mail Adresse genutzt wird, und auf diesem Wege sehr wohl personenbezogene Daten preisgibt.

Microsoft Sprecher Jonathan Usher erklärte, der Konzern plane derzeit nicht, gesammelte Daten über die Seh- und Hörgewohnheiten von Kunden zu vermarkten, wolle das aber für die Zukunft auch nicht ausschließen. Vor diesem Hintergrund sollte die Nutzung eines anderen Players erwogen werden. Wer nicht auf den Multimediaplayer von Windows XP verzichten will oder kann, sollte wenigstens die CD-Datenbankabfrage deaktivieren. Allerdings kann der Benutzer erst dann wieder im Internet surfen, wenn diese Einstellung aufgehoben ist. Sicherheit vor ungewollter Datenübertragung bietet da nur das Abschalten des Internetzugriffsrechts unter Extras/Optionen/ Medienbibliothek (siehe Abb. 5)

Abb.5



15. Fazit

Bisher gibt es zum Thema XP sehr viele widersprüchliche Aussagen. Es ist nicht völlig klar, welche Daten tatsächlich an Microsoft übertragen werden und ob sich aus diesen Daten Nutzungsprofile der Anwender erstellen lassen. Deshalb sollte insbesondere bei der Nutzung des Internet sorgfältig zwischen einer höheren Benutzerfreundlichkeit und Einbußen bei der Sicherheit abgewogen werden.

Die Vielfalt, mit der das Betriebssystem versucht, mit dem Hersteller Kontakt aufzunehmen, macht es schwierig, wirklich alle risikobehafteten Funktionen abzuschalten und dabei noch effizient zu arbeiten. Natürlich wird die Sicherheit beim Nutzen von Windows XP größer, wenn der Zugang zum Internet völlig gesperrt wird. Aber gerade die enge Verknüpfung mit dem Internet soll ja den Vorteil gegenüber älteren Systemen ausmachen.

Die enge Verzahnung mit der vielfältigen Nutzung des Internets und mit dem Active Directory führen dazu, dass sich beim Einsatz von Windows XP komplexe datenschutzrechtliche Problemstellungen ergeben können, für die vor dem Einsatz von Windows XP angemessene Lösungen gefunden werden müssen. Bei der Einsatzplanung von Windows XP wird deshalb die Erstellung eines Sicherheitskonzepts empfohlen.

Quellen

Der Hamburgische Datenschutzbeauftragte: Datenschutz bei Windows 2000, 2002.

Uwe Brünning, Jörg Krause - Windows XP Professional - Carl Hanser Verlag

http://www:heise.de/newsticker/data/hps-21.02.02-000/ Verlag Heinz Heise, 2002.

http://www.microsoft.com/windows/windowsmedia/windowsxpwhatsnew.asp

http://www.sun.de/SunPR/Pressemitteilungen/2001/PM01

Martins/Kobylinska -„Auf IP-Nummer sicher“,“Sicherheit an Bord“- PC INTERN 02/02

14.6 Datenschutz und Telemedizin - Anforderungen an Medizinnetze[1]

I. Einleitung

Zur Steigerung von Qualität und Effizienz in der Gesundheitsversorgung sowie zur Kosteneinsparung spielt die einrichtungsübergreifende elektronische Kommunikation eine immer größere Rolle. Kommunikationsnetze und Kommunikationsdienste sollen dazu beitragen, die Kommunikation zwischen den Institutionen zu verbessern und die Leistungsprozesse zu optimieren. Wegen der hohen Sensibilität der im Gesundheitswesen verarbeiteten Daten kommt dem Datenschutz und der Datensicherheit eine besondere Bedeutung zu.

Die folgenden Ausführungen sollen eine Hilfestellung zur Formulierung und Umsetzung einer datenschutzgerechten Sicherheitspolitik für die elektronische Kommunikation und Datenverarbeitung im Gesundheitswesen bieten. In Kapitel II werden zunächst die allgemeinen datenschutzrechtlichen Anforderungen aufgezeigt. Diese bilden den rechtlichen Rahmen, an dem sich medizinische Datenverarbeitung zu orientieren hat. Darauf aufbauend werden in Kapitel III grundlegende Sicherheitsanforderungen für Systeme definiert, die patientenbezogene Daten verarbeiten. Kapitel IV diskutiert basierend auf der Form der Datenhaltung vier Architekturszenarien für Systeme zur einrichtungsübergreifenden Kommunikation. Damit verbunden ist die Erwartung, dass sich alle Systeme zur einrichtungsübergreifenden Kommunikation nach diesen Architekturansätzen kategorisieren lassen bzw. eine Kombination aus diesen Architekturen darstellen. Insofern sind die zu den Szenarien gemachten Aussagen auf andere Kommunikationsarchitekturen entsprechend übertragbar. In Kapitel V werden für die in Kapitel IV dargestellten Szenarien spezielle Maßnahmen zur Datensicherheit erläutert, die erforderlich sind zur Realisierung der in Kapitel III formulierten Sicherheitsziele und die die hohen Anforderungen an die medizinische Datenverarbeitung berücksichtigen. In Kapitel VI werden schließlich exemplarisch zwei konkrete Ansätze zur Kommunikation im Gesundheitswesen beschrieben.

II. Allgemeine datenschutzrechtliche Anforderungen

Für die Verarbeitung personenbezogener Patientendaten im Rahmen telemedizinischer Anwendungen gelten grundsätzlich die allgemeinen rechtlichen Rahmenbedingungen, die für die Verarbeitung personenbezogener Patientendaten außerhalb telemedizinischer Anwendungen gelten. Die Einführung telemedizinischer Anwendungen darf nicht zu einer rechtlichen oder faktischen Verschlechterung der Patientenrechte führen. Die Durchsetzung bzw. Konkretisierung der Patientenrechte unter

[1] erarbeitet vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten

den veränderten technischen Bedingungen bedarf teilweise neuer datenschutzrechtlicher Konzepte.

Rechtsgrundlagen
Für die Verarbeitung von Patientendaten durch niedergelassene Ärzte gelten die Vorschriften des BDSG. Für die Verarbeitung von Patientendaten durch die Krankenhäuser gelten in Bund und Ländern unterschiedliche Rechtsvorschriften. In einzelnen Ländern liegen sog. bereichsspezifische Regelungen der Verarbeitung personenbezogener Daten in Krankenhäusern (Landeskrankenhausgesetze, Gesundheitsdatenschutzgesetze etc.) vor. Soweit keine bereichsspezifischen Regelungen vorhanden sind, gelten die allgemeinen datenschutzrechtlichen Vorschriften. Die Religionsgesellschaften treffen für ihren Bereich zum Teil Regelungen in eigener Zuständigkeit. Darüber hinaus sind die Regelungen der Berufsordnung und des Strafgesetzbuchs zu beachten.

Auf der Grundlage des Behandlungsvertrages in Verbindung mit den jeweils maßgeblichen datenschutzrechtlichen Vorschriften darf der Arzt die für die Durchführung der Behandlung erforderlichen Daten verarbeiten. Soweit die Verarbeitung der Daten nicht für die Durchführung der Behandlung erforderlich ist (z.B. zusätzliche Datenerhebungen für ein Forschungsvorhaben), bedarf es einer besonderen Einwilligung des Patienten.

Unabhängig vom verwendeten Datenträger muss der Arzt parallel zu den datenschutzrechtlichen Vorschriften die in der Berufsordnung und in § 203 StGB normierte Schweigepflicht beachten, ferner das in § 5 BDSG und den entsprechenden landesrechtlichen Bestimmungen geregelte Datengeheimnis. Gehilfen des Arztes unterliegen ebenfalls der ärztlichen Schweigepflicht.

Dokumentationspflicht
Nach der Berufsordnung ist der Arzt verpflichtet, die erforderlichen Aufzeichnungen über die in Ausübung seines Berufs gemachten Feststellungen und getroffenen Maßnahmen anzufertigen. Es handelt sich um eine unselbständige vertragliche Nebenpflicht aus dem Behandlungsvertrag. Ist die Dokumentation lückenhaft, kann dies im Haftungsprozess eine Umkehr der Beweislast zugunsten des Patienten nach sich ziehen, wenn die Aufklärung des Sachverhalts für den Patienten insgesamt erschwert wird.

Befugnis zur Übermittlung bzw. Weitergabe von Patientendaten
Der Arzt darf personenbezogene Patientendaten nur im Rahmen der datenschutzrechtlichen Vorschriften und befugt i.S.v. § 203 StGB offenbaren. Eine Befugnis zur Offenbarung kann sich insbesondere aus einer gesetzlichen Regelung (z. B. Krebsregistergesetze, Infektionsschutzgesetz, Sozialgesetzbuch V), aus dem Behandlungsvertrag oder der speziellen Einwilligung des Patienten ergeben. Die ärztliche Schweigepflicht

gilt grundsätzlich auch zwischen Ärzten. Eine Übermittlung personenbezogener Daten an einen vor-, mit- oder nachbehandelnden Arzt bedarf daher der Einwilligung des Patienten.

Nach den datenschutzrechtlichen Regelungen müssen Einwilligungen bestimmte Anforderungen erfüllen, um rechtswirksam zu sein. Insbesondere muss die Freiwilligkeit der Einwilligung gewährleistet sein und der Betroffene muss zuvor über Umfang und Zweck der geplanten Verarbeitung seiner Daten, die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung informiert werden (vgl. z. B. § 4 a Abs. 1 Satz 1 und 2 BDSG). Pauschale Einwilligungserklärungen, deren Tragweite der Betroffene nicht übersehen kann, sind daher unzulässig. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände im Einzelfall eine andere Form angemessen ist (vgl. z. B. § 4 a Abs. 1 Satz 3, Abs. 2 BDSG). Die Landeskrankenhausgesetze enthalten bez. Datenübermittlungen an vor-, mit- und nachbehandelnde Ärzte und an Angehörige zum Teil hiervon abweichende Regelungen (z. B. Widerspruchsrecht des Patienten nach Information über die geplante Datenübermittlung).

Spezialregelungen zur Einwilligung des Versicherten sind insbesondere im SGB V enthalten. Durch das GKV-Gesundheitsreformgesetz 2000 wurden Regelungen zur verstärkten Kooperation und Kommunikation zwischen den Leistungserbringern in das SGB V aufgenommen:

- § 73 Abs. I b SGB V enthält eine Spezialregelung zur zentralen Dokumentation beim Hausarzt. Ein Hausarzt darf mit schriftlicher (widerruflicher) Einwilligung des Versicherten bei Leistungserbringern, die einen seiner Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die behandelnden Leistungserbringern sind verpflichtet, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten die Behandlungsdaten und Befunde zum Zwecke der bei diesem durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln; die behandelnden Leistungserbringer sind berechtigt, mit schriftlicher (widerruflicher) Einwilligung des Versicherten, die für die Behandlung erforderlichen Behandlungsdaten und Befunde bei dem Hausarzt und anderen Leistungserbringern zu beschaffen und für die Zwecke der von ihnen zu erbringenden Leistungen zu verarbeiten und zu nutzen.

- In § 140 a ff. SGB V sind Regelungen zur sog. integrierten Versorgung enthalten. Die Teilnahme der Versicherten an den integrierten Versorgungsformen ist freiwillig. Die Vertragspartner müssen u.a. die Gewähr dafür übernehmen, dass sie eine an dem Versorgungsbedarf orientierte Zusammenarbeit zwischen allen an der Versorgung Beteiligten sicherstellen, einschließlich der Koordination zwischen den verschiedenen Versorgungsbereichen und einer ausreichenden Dokumen-

tation, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss. Der Leistungserbringer darf aus der gemeinsamen Dokumentation die den Versicherten betreffenden Behandlungsdaten und Befunde nur dann abrufen, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat, die Information für den konkret anstehenden Behandlungsfall genutzt werden soll und der Leistungserbringer zu dem Personenkreis gehört, der nach § 203 StGB zur Geheimhaltung verpflichtet ist.

Das Vorzeigen der Krankenversichertenkarte durch den Patienten beim behandelnden Arzt kann nicht als Einwilligung in die Anforderung bzw. den Abruf von medizinischen Daten bei anderen Ärzten qualifiziert werden, da der Patient in jedem Fall beim behandelnden Arzt seine Krankenversichertenkarte zum Nachweis der Leistungsberechtigung vorlegen muss.

Eine pauschale Einwilligung des Patienten, eine Krankenversichertenkarte mit medizinischen Daten zu verwenden, die bei jedem Arztbesuch vorgezeigt werden muss, ist nach den dargelegten rechtlichen Anforderungen an Einwilligungen unzulässig. Entsprechendes gilt für eine pauschale Einwilligung des Patienten, dass ein Teil seiner Krankheitsdaten in einem zentralen Datenbestand zum Abruf durch andere Ärzte bereitgehalten werden darf.

Informationsrechte des Patienten
Nach der Rechtsprechung des BGH hat der Patient grundsätzlich ein Recht auf Einsicht in seine Krankenunterlagen, soweit sie sog. objektive Daten betreffen. Es handelt sich um einen Nebenanspruch aus dem Behandlungsvertrag. Für den Bereich der Psychiatrie hat die Rechtsprechung Ausnahmen formuliert. Die - gegenüber der Rechtsprechung vorrangigen - datenschutzrechtlichen Regelungen (Landeskrankenhausgesetze, Gesundheitsdatenschutzgesetze, allgemeine datenschutzrechtliche Regelungen) legen zum Teil weitergehende Rechte der Patienten auf Information, Auskunft und Einsicht fest.

Im Bereich der Telemedizin ist es besonders wichtig, dass der Patient in allen Verarbeitungsphasen ausreichend informiert ist über die Verarbeitung seiner personenbezogenen Daten. Dies setzt voraus, dass das ihn informierende Personal ebenfalls ausreichend informiert ist. Es muss insbesondere auch gewährleistet sein, dass dem Patienten bei Vertragsabschluss bzw. Einwilligung Umfang, Zweck und Rechtsgrundlage der Verarbeitung seiner Daten sowie ggf. die Grundzüge des technischen Verfahrens der Verarbeitung (z. B. bei Chipkartenverfahren) bekannt gegeben worden sind.

Datenverarbeitung im Auftrag durch externe Dritte
In zunehmendem Ausmaß werden personenbezogene medizinische Patientendaten durch externe Dritte verarbeitet. Wenn ein Arzt personenbezogene Patientendaten

für eine Auftragsdatenverarbeitung (z. B. Mikroverfilmung, Schreibarbeiten, externe Archivierung) an einen externen Dritten weitergibt, so ist dies keine Datenübermittlung im Sinne der datenschutzrechtlichen Regelungen, da der Arzt als Auftraggeber datenverarbeitende Stelle bleibt. Da die Weitergabe der personenbezogenen Patientendaten an einen externen Dritten jedoch eine Durchbrechung der ärztlichen Schweigepflicht darstellt, benötigt der Arzt für diese Datenweitergabe eine rechtliche Befugnis i. S. v. § 203 StGB. Einige Landeskrankenhausgesetze sehen z. B. die Möglichkeit einer Auftragsdatenverarbeitung für die Krankenhäuser vor. Sofern keine Rechtsvorschrift als Rechtsgrundlage für eine befugte Offenbarung der Patientendaten an einen externen Dritten vorhanden ist, kommt grundsätzlich nur eine Einwilligung der Betroffenen als Rechtsgrundlage für die Datenweitergabe in Betracht.

Wenn sichergestellt werden kann, dass der externe Dritte (Auftragnehmer) keine personenbezogenen medizinischen Daten zur Kenntnis nehmen kann (z. B. bei Konzepten zur digitalen externen Archivierung, bei denen eine Verschlüsselung aller Informationen vorgesehen ist), liegt keine Durchbrechung der ärztlichen Schweigepflicht vor.

Auch wenn eine Rechtsgrundlage für eine Datenweitergabe zur Auftragsdatenverarbeitung vorliegt, müssen die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit getroffen werden. Dies bedeutet insbesondere auch, dass der Kreis derjenigen Personen, die personenbezogene Patientendaten zur Kenntnis erhalten, soweit wie möglich begrenzt werden bzw. u. U. sogar eine Kenntnisnahme der personenbezogenen Patientendaten ausgeschlossen werden muss.

Die beim Arzt gespeicherten Patientendaten unterliegen dem Beschlagnahmeverbot i. S. v. § 97 Abs. 1 StPO. Das Beschlagnahmeverbot schützt das Vertrauensverhältnis zwischen dem zeugnisverweigerungsberechtigten Arzt und dem Betroffenen. Das Beschlagnahmeverbot erstreckt sich nur auf Gegenstände, die sich im Gewahrsam des Zeugnisverweigerungsberechtigten befinden. Wenn sich die Patientendaten nicht im Gewahrsam des Zeugnisverweigerungsberechtigten befinden, sondern im Gewahrsam eines externen Dritten, findet das Beschlagnahmeverbot des § 97 StPO keine Anwendung, d. h. der Schutz der Patientenrechte verschlechtert sich. Fraglich ist, ob das Beschlagnahmeverbot ausnahmsweise auch bei Gewahrsam eines externen Dritten Anwendung findet, wenn der externe Dritte (Auftragnehmer) ein Arzt ist. Mangels einer gerichtlichen Entscheidung kann dies nicht als gesichert angesehen werden, denn der Arzt wird hier nicht als behandelnder Arzt tätig, sondern übernimmt eine kommerzielle Tätigkeit.

Abruf von Patientendaten über ein Datennetz

Patientendaten können nach Erteilung einer Einwilligung des Patienten im Einzelfall für einen Zugriff durch den Berechtigten freigegeben werden. Ein Zum - Abruf - Bereitstellen (vgl. z. B. § 10 BDSG) von Patientendaten durch einen Arzt über ein

Datennetz ist nach der gegenwärtigen Rechtslage grundsätzlich nicht zulässig. Ein Arzt ist verpflichtet, vor einer Übermittlung zu prüfen, ob eine Befugnis zur Offenbarung der Daten an den Empfänger vorliegt. Würde ein Arzt die Patientendaten für einen Abruf durch andere Behandlungseinrichtungen bereithalten und käme es dann zu einem Abruf, der rechtlich nicht (z. B. durch eine Einwilligung des Patienten) legitimiert ist, so hätte sich der speichernde Arzt nach § 203 StGB strafbar gemacht. Eine Offenbarung von Patientendaten kann auch dadurch vorgenommen werden, dass nicht verhindert wird, dass die Daten durch externe Dritte abgerufen werden können.

III. Grundlegende Sicherheitsanforderungen

Das Bundesdatenschutzgesetz verlangt in § 9 allgemein technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten. Die in der Anlage zu § 9 BDSG beschriebenen Regelungen (die auch denen einiger Länderdatenschutzgesetze entsprechen) definieren Sicherheitsmaßnahmen und haben im Wesentlichen die technischen Komponenten von Datenverarbeitungsanlagen zum Gegenstand. Dadurch sind sie stark technologieabhängig und anpassungs- bzw. erläuterungsbedürftig. Deshalb empfiehlt es sich, sich - wie im Folgenden - zukünftig auf einem abstrakteren Niveau an primär an den Daten ausgerichteten Sicherheitszielen zu orientieren. Dies ist bereits im Rahmen der Novellierung des Datenschutzrechtes in einigen Ländergesetzen geschehen. Sofern andere gesetzliche Regelungen noch den herkömmlichen Katalog der „Zehn Gebote des Datenschutzes“ enthalten, sind diese bei Beachtung der Grundziele und ihrer Umsetzung innerhalb eines Datenschutzkonzeptes in jedem Fall abgedeckt.

Im Folgenden werden die grundlegenden Sicherheitsziele definiert, die von Systemen zur medizinischen Datenverarbeitung gewährleistet werden müssen:

1. Vertraulichkeit

„Wer sich in Behandlung begibt, muss und darf erwarten, dass alles, was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim bleibt und nicht zur Kenntnis Unberufener gelangt. Nur so kann zwischen Patient und Arzt jenes Vertrauen entstehen, das zu den Grundvoraussetzungen ärztlichen Wirkens zählt, weil es die Chancen der Heilung vergrößert und damit – im ganzen gesehen – der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient.“ (BVerfGE 32, 373, 380). Die in der ärztlichen Berufsordnung und dem Strafgesetzbuch normierte ärztliche Schweigepflicht schützt das Vertrauensverhältnis zwischen Patient und Arzt. Der Arzt muss die Vertraulichkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten gewährleisten, d. h. nur Befugte dürfen personenbezogene Daten zur Kenntnis erhalten bzw. davon Kenntnis nehmen können.

Auch die datenschutzrechtlichen Regelungen, die das Recht des Patienten auf informationelle Selbstbestimmung konkretisieren, schützen die Vertrauensbeziehung zwischen Patient und Arzt. Eine Kenntnisnahme medizinischer Daten durch Unbefugte (z. B. Arbeitgeber, Versicherungen, Pharmaindustrie) kann erhebliche soziale bzw. materielle Folgen für den Patienten nach sich ziehen.

2. Authentizität (Zurechenbarkeit)

Die Authentizität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d. h. der Urheber von patientenbezogenen bzw. der Verantwortliche für patientenbezogene Daten sowie der Auslöser eines Verarbeitungsvorgangs bzw. der Verantwortliche für einen Verarbeitungsvorgang muss jederzeit eindeutig feststellbar sein. Gegebenenfalls kann auch die Art und Weise der Erhebung der Daten von Bedeutung sein (z. B. Datenerhebung durch ein medizinisches Gerät). Medizinische Dokumente, die ihren Urheber bzw. Verantwortlichen nicht erkennen lassen, sind als Grundlage für Behandlungen und Begutachtungen ungeeignet.

3. Integrität

Die Integrität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d. h. personenbezogene Daten müssen während aller Phasen der Verarbeitung unversehrt, vollständig, gültig und widerspruchsfrei bleiben. Der Behandlungsauftrag in Einrichtungen des Gesundheitswesens umfasst eine sorgfältige Diagnose und Therapie mit dem Ziel der Heilung des Patienten. Die Echtheit, Korrektheit und Vollständigkeit der Daten, vor, während und nach der Bearbeitung und Übertragung ist für die Erfüllung des Behandlungsauftrags von großer Bedeutung. Eine Verfälschung oder Unvollständigkeit der Daten kann zu falschen medizinischen Entscheidungen mit u. U. lebensbedrohenden Folgen für den Patienten führen, verbunden mit rechtlichen Konsequenzen für den Mediziner.

4. Verfügbarkeit

Die Verfügbarkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d. h. personenbezogene Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Die zeitgerechte Verfügbarkeit medizinischer Informationen kann entscheidend sein für eine erfolgreiche Erfüllung des Behandlungsauftrags. Nicht oder nicht rechtzeitig zur Verfügung stehende Daten können zur Handlungsunfähigkeit bzw. zu einem zu späten Handeln oder Behandlungsfehlern des Mediziners führen und u. U. lebensbedrohende Folgen für den Patienten sowie rechtliche Konsequenzen für den Mediziner haben. Die Verfügbarkeit der Daten impliziert natürlich die Verfügbarkeit der zur ordnungsgemäßen Verarbeitung erforderlichen Komponenten (Hard- und Software) des IT-Systems.

5. Revisionsfähigkeit

Die Revisionsfähigkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d. h. die Verarbeitungsprozesse müssen lückenlos nachvollzogen werden können und es muss festgestellt werden können, wer wann welche patientenbezogenen Daten auf welche Weise verarbeitet hat. Für den Arzt bzw. das Krankenhaus besteht nach der Berufsordnung die Pflicht zur Dokumentation der Behandlung. Sie ist eine unselbständige Nebenpflicht aus dem Behandlungsvertrag. Eine lückenhafte Dokumentation kann im Haftungsprozess eine Beweislastumkehr zugunsten des Patienten nach sich ziehen. Es muss nachvollziehbar sein, wer welche Diagnose gestellt und welche Therapie verordnet hat und aufgrund welcher Daten ein Arzt seine Entscheidung über Behandlungsmaßnahmen getroffen hat. Eine notwendige Voraussetzung für die Gewährleistung der Revisionsfähigkeit ist die Sicherstellung der Authentizität.

6. Validität

Die Validität der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten muss gewährleistet sein, d. h. personenbezogene Daten müssen aktuell in der für den Nutzungszweck angemessenen Qualität verarbeitet werden. Diese Forderung betrifft insbesondere Bilddaten, bei denen es auf Qualitätsmerkmale wie Bildauflösung und Farbechtheit ankommt. Die Validität wird von der Integrität nicht umfasst, da die Daten zwar integer im Sinne von vollständig und unversehrt sein können, die Darstellungsqualität und Aktualität aber dennoch für medizinische Nutzungszwecke unzureichend sein kann.

7. Rechtssicherheit

Für jeden Verarbeitungsvorgang und dessen Ergebnisse ist der Verursachende bzw. Verantwortliche beweiskräftig nachweispflichtig. Ist die Rechtssicherheit nicht gegeben, können Patienten eventuelle Schadensansprüche u. U. nicht geltend machen bzw. können Mediziner u. U. die Korrektheit ihres Handelns nicht nachweisen. Die notwendige Voraussetzung für die Gewährleistung der Rechtssicherheit ist die Gewährleistung der Revisionsfähigkeit. Die Revisionsfähigkeit alleine gewährleistet aber noch nicht die beweiskräftige Überprüfbarkeit von Verarbeitungsvorgängen in gerichtlichen Verfahren.

8. Nicht-Abstreitbarkeit von Datenübermittlungen

Die Nicht-Abstreitbarkeit des Sendens und des Empfangens von patientenbezogenen Dokumenten muss gewährleistet sein. D. h. einerseits ist zu gewährleisten, dass der Sender eines patientenbezogenen Dokuments sicher sein kann, dass das Dokument seinen Empfänger erreicht hat, und er darf nicht abstreiten können, genau dieses Dokument an genau den Empfänger gesendet zu haben. Andererseits muss der Empfänger eines patientenbezogenen Dokuments sicher sein können, genau dieses Dokument

von einem bestimmten Sender empfangen zu haben, und er darf nicht abstreiten können, genau das Dokument von einem bestimmten Sender empfangen zu haben. Die Nicht-Abstreitbarkeit ist eine Voraussetzung der Revisionsfähigkeit.

9. Nutzungsfestlegung

Medizinische Datenverarbeitungssysteme müssen es ermöglichen, für jedes patienten-bezogenes Dokument den Nutzerkreis sowie abgestufte Nutzungsrechte festzulegen und Nutzungsausschlüsse zu definieren.

IV. Formen der Datenhaltung

In diesem Kapitel werden Systeme zur einrichtungsübergreifenden Verarbeitung patientenbezogener Daten in Kategorien unterteilt, die in den folgenden Szenarien beschrieben werden. Die Kriterien für die Kategorisierung orientieren sich an den grundlegenden Formen der Datenhaltung. Es ist zu erwarten, dass jedes medizinische Datenverarbeitungssystem zur einrichtungsübergreifenden Kommunikation einer dieser Kategorien angehört oder sich als eine Kombination dieser darstellt. Damit wird es möglich Systeme einzuordnen und die zu den einzelnen Szenearien getroffenen Aussagen entsprechend auf das jeweils zu betrachtende System zu übertragen.

Szenario 1: Dezentrale Datenhaltung:
Bei der dezentralen Datenhaltung werden die Daten dort gespeichert, wo sie auch erzeugt wurden. Somit hat jede medizinische Einrichtung ihre eigene Datenhaltung. Die Datenhaltungssysteme der verschiedenen Einrichtungen können zwar über ein Netz miteinander kommunizieren, sind aber ansonsten als vollständig autonom anzusehen. Systemübergreifende einheitliche Dienste gibt es nicht.

Bei einer dezentralen Architektur muss für jeden Kommunikationsvorgang explizit eine Kommunikationsverbindung zwischen dem sendenden und dem empfangenden System aufgebaut werden. Die Initiierung der Kommunikation erfolgt durch den Sender. Dies erfordert, dass vor jeder Übermittlung von Dokumenten eines Patienten dem Sender (z. B. dem überweisenden Arzt) der Empfänger (z. B. der weiterbehandelnde Arzt) bekannt sein muss. Eine nicht-adressierte Kommunikation ist nicht möglich. Die Realisierung einer einrichtungsübergreifenden elektronischen Patientenakte ist daher nicht bzw. nur sehr eingeschränkt möglich (z. B. fallbezogen durch jeweiliges Mitsenden der bereits vorhandenen Dokumente).

Jede Einrichtung ist datenverarbeitende Stelle im Sinne der Datenschutzgesetze für ihre eigenen Daten. Datenübermittlungen an vor-, mit- und nachbehandelnde Ärzte sind nur aufgrund einer rechtlichen Legitimation (z. B. Einwilligung des Patienten im Einzelfall) zulässig. Spezielle rechtliche oder rechtspolitische Probleme bzgl. der ärztlichen Schweigepflicht entstehen bei der dezentralen Datenhaltung nicht.

Szenario 2: Zentrale Datenhaltung:
Bei der zentralen Datenhaltung werden Daten, deren Verarbeitung in der Verantwortung verschiedener medizinischer Einrichtungen liegt, (technisch) zentral zusammengeführt und in einem zentralen System gespeichert. Es gibt keine redundanten Datenbestände, d. h. bei den verschiedenen beteiligten Einrichtungen selbst werden keine Daten gespeichert.

Die Einrichtungen bleiben jeweils datenverarbeitende Stelle im Sinne der Datenschutzgesetze für ihre eigenen Datenbestände. Eine einrichtungsübergreifende zentrale Datenhaltung kann nur über die Vergabe einer Datenverarbeitung im Auftrag an einen externen Dritten realisiert werden. Die rechtlichen Voraussetzungen für eine Datenverarbeitung im Auftrag müssen erfüllt sein (s. Kapitel II). Auch wenn die rechtlichen Voraussetzungen erfüllt sind, bleibt es problematisch, dass der Beschlagnahmeschutz für die Patientendaten durch die Auftragsdatenverarbeitung aufgehoben ist und dass Dritte Kenntnis der medizinischen Daten erhalten. In jedem Fall muss die Möglichkeit der Kenntnisnahme personenbezogener medizinischer Daten durch den externen Dritten soweit wie möglich ausgeschlossen werden.

Im Übrigen ist die ärztliche Schweigepflicht gewahrt, wenn der Zugriffskontrollmechanismus des Zentralsystems gewährleistet, dass jede Einrichtung nur auf die eigenen Daten zugreifen kann.

Datenübermittlungen zwischen den angeschlossenen Einrichtungen werden technisch durch entsprechende Rechtevergaben realisiert. Will ein Mediziner der Einrichtung A ein Dokument X an einen Mediziner der Einrichtung B übermitteln, veranlasst er, dass dieser die Zugriffsrechte für dieses Dokument erhält.

Wie bei Szenario 1 muss eine rechtliche Legitimation für die Datenübermittlungen vorliegen. Der Patient kann einwilligen, dass seine Daten einem bestimmten Arzt übermittelt werden. Es ist auch möglich, dass der Patient darin einwilligt, dass ein Teil seiner Daten zum Abruf durch einen später von ihm bestimmten Arzt bereitgehalten werden. Die Voraussetzungen, unter denen ein Arzt auf die Daten zugreifen darf, müssen in der Einwilligungserklärung festgelegt sein. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Zugriff durch den jeweiligen Arzt vorliegen.

Mit diesem Modell ist die elektronische Patientenakte sowohl fallbezogen als auch umfassend realisierbar, soweit die einen Patienten behandelnden Einrichtungen bzw. Ärzte sich an der zentralen Datenhaltung beteiligen und die Einwilligung des Patienten vorliegt.

Unter rechtspolitischen Gesichtspunkten ist die zentrale Datenhaltung problematisch, weil eine zentrale Datensammlung über Patienten neue Missbrauchsmöglichkeiten eröffnet und neue Begehrlichkeiten nach weiteren zentralen Auswertungs- und Verwendungsmöglichkeiten der Patientendaten wecken kann.

Szenario 3: Verteilte Datenhaltung
Bei der verteilten Datenhaltung werden, wie im Falle der dezentralen Datenhaltung, die Daten auf den Systemen der Einrichtungen gespeichert, die sie auch erzeugt haben. Darüber hinaus gibt es aber systemübergreifende Dienste, die dafür sorgen, dass die einzelnen dezentralen Systeme zu einem Kommunikationsverbund zusammengeschlossen werden. Damit sind die dezentralen Systeme Subsysteme des durch den Verbund entstandenen Gesamtsystems. Den Nutzern eines verteilten Systems bleibt die physikalische Verteilung der Daten auf eine Vielzahl von Subsystemen verborgen (Verteilungstransparenz) und ihnen wird der Eindruck vermittelt, als arbeiten sie mit einem Zentralsystem. Ein verteiltes System benötigt Metainformationen über die bei den einzelnen Subsystemen gespeicherten Dokumente sowie einen systemweiten Zugriffskontrollmechanismus.

Die Einrichtungen bleiben jeweils datenverarbeitende Stelle im Sinne der Datenschutzgesetze für ihre eigenen Datenbestände. Datenübermittlungen zwischen den verschiedenen Einrichtungen, d. h. zwischen dezentralen Subsystemen, erfordern wie bei der zentralen Datenhaltung eine rechtliche Legitimation und eine entsprechende Rechtevergabe. Möchte ein Mediziner der Einrichtung A (Nutzer des Subsystems A) auf ein Dokument zugreifen, prüft der systemweite Zugriffskontrollmechanismus, ob er die entsprechenden Zugriffsrechte besitzt. Ist dies der Fall, ermittelt ein Systemdienst auf der Grundlage der Metainformationen den Lagerort des Dokumentes. Ist das Dokument bei Subsystem A gespeichert (also ein Dokument der Einrichtung A), erfolgt ein lokaler Datenzugriff. Ist das Dokument bei Subsystem B gespeichert (also ein Dokument der Einrichtung B), erfolgt ein entfernter Zugriff auf Subsystem B unter Nutzung von Kommunikationsmechanismen, ohne dass der Nutzer Kenntnis des Speicherortes haben muss.

Bei der verteilten Datenhaltung bleiben die verschiedenen Einrichtungen datenverarbeitende Stelle im Sinne der Datenschutzgesetze für ihre eigenen Daten. Grundsätzlich ist die ärztliche Schweigepflicht gewahrt, wenn jede Einrichtung nur auf ihre eigenen Daten zugreifen kann.

Der Patient kann einwilligen, dass seine Daten an einen bestimmten Arzt übermittelt werden. Es ist auch möglich, dass ein Teil seiner Daten für externe Zugriffe durch später von ihm bestimmte Ärzte unter den von ihm bestimmten Voraussetzungen bereitgehalten werden. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Datenzugriff durch den jeweiligen Arzt vorliegen. Der Aufbau einer einrichtungsübergreifenden („virtuellen“) elektronischen Patientenakte ist bei diesem Modell möglich.

Bei der verteilten Datenhaltung wird das o.a. rechtspolitische Problem der zentralen Datenhaltung gemildert, da selbst im „worst case“ nur die Daten zusammengeführt werden können, die für externe Zugriffe freigegeben wurden. Der Beschlagnahme-

schutz für die Patientendaten bleibt erhalten. Da die verteilte Datenhaltung keine Datenverarbeitung im Auftrag erforderlicht macht, ist das Problem der Kenntnisnahme von personenbezogenen medizinischen Patientendaten durch externe Dritte nicht gegeben.

Szenario 4: Dezentrale Datenhaltung mit zentraler Komponente
Bei dieser Datenhaltungsform findet eine dezentrale Datenhaltung bei den einzelnen medizinischen Einrichtungen statt. Außerdem können Dokumente der verschiedenen Einrichtungen an einer zentralen Stelle temporär (technisch) zusammengeführt werden.

Die verschiedenen Einrichtungen bleiben datenverarbeitende Stelle im Sinne der Datenschutz-gesetze für ihre eigenen Daten, auch bei der zentralen Speicherung eines Teildatenbestandes. Bei diesem Modell bildet die zentrale Speicherkomponente einen Puffer, der allen angeschlossenen Einrichtungen zum Up- und Download zur Verfügung steht. Dokumente werden vom Sender auf diesen zentralen Speicher übertragen (Upload) und können dann vom Empfänger von dort abgeholt (Download) werden.

Rechtlich handelt es sich beim Up- und dem zugehörigen Download um eine Datenübermittlung, die einer rechtlichen Legitimation (z. B. Einwilligung des Patienten) bedarf. Der Patient kann im Einzelfall einwilligen, dass seine Daten einem bestimmten Arzt über die zentrale Speicherkomponente übermittelt werden. Es ist auch möglich, dass der Patient darin einwilligt, dass ein Teil seiner Krankheitsdaten in den zentralen Datenbestand eingestellt wird und dort zum Abruf durch später von ihm bestimmte Ärzte bereitgehalten wird. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Abruf der Daten durch den jeweiligen Arzt vorliegen. Auf dem zentralen Speicher können Dokumente zur (fallbezogenen) elektronischen Patientenakte zusammengeführt werden, soweit der den Patienten behandelnde Arzt an die zentrale Speicherkomponente angeschlossen ist und eine Einwilligung des Patienten in die Bereitstellung der Daten für den Abruf durch andere Ärzte vorliegt.

Die zentrale einrichtungsübergreifende Speicherung eines Teildatenbestandes aller Einrichtungen kann nur über die Vergabe einer Datenverarbeitung im Auftrag an einen externen Dritten realisiert werden. Die rechtlichen Voraussetzungen für eine Datenverarbeitung im Auftrag müssen erfüllt sein. Auch wenn die rechtlichen Voraussetzungen erfüllt sind, bleibt es problematisch, dass der Beschlagnahmeschutz für die Patientendaten durch die Auftragsdatenverarbeitung aufgehoben ist. Die Möglichkeiten einer Kenntnisnahme personenbezogener medizinischer Daten durch den externen Dritten müssen in jedem Fall soweit wie möglich ausgeschlossen werden.

Bei der dezentralen Datenhaltung mit zentraler Komponente entsteht das auch bei der zentralen Datenhaltung dargelegte rechtspolitische Problem: Es entsteht eine neue zentrale (Teil-)Datensammlung, die neue Möglichkeiten des Datenmissbrauchs

eröffnet und neue Begehrlichkeiten nach weiteren zentralen Datenauswertungen und –verwendungen wecken kann.

V. Spezielle Datensicherheitsmaßnahmen

Zur Realisierung der in Kapitel III definierten Sicherheitsziele sind für jedes medizinische Datenverarbeitungssystem auf der Grundlage einer Bedrohungs- und Risikoanalyse die individuell erforderlichen Sicherheitsmaßnahmen zu ermitteln. Naturgemäß ergibt sich eine Vielzahl zu treffender technischer und organisatorischer Sicherheitsmaßnahmen, die abhängig von den jeweiligen technischen Systemausprägungen und den unterschiedlichen Rahmenbedingungen von System zu System sehr unterschiedlich sein können. Aufgrund des hohen Schutzbedarfs der Daten, die von medizinischen Systemen verarbeitet werden, ergeben sich aber spezielle Sicherheitsmaßnahmen, die aus datenschutzrechtlicher Sicht als unabdingbar anzusehen sind. Diese Maßnahmen werden im Folgenden für die einzelnen Sicherheitsziele und Systemarchitekturen erläutert.

1. Sicherstellung der Vertraulichkeit

Der Vertraulichkeit kommt aufgrund der hohen Sensibilität medizinischer Daten und der Pflicht zur Wahrung des Arzt-Patienten-Geheimnisses eine große Bedeutung zu. Insofern muss bei jeder Phase der Datenverarbeitung sichergestellt werden, dass nur Befugte patientenbezogene Daten zur Kenntnis nehmen können. Eine hinreichende Gewährleistung der Vertraulichkeit mit den hohen Anforderungen des Gesundheitswesens kann nur durch Verschlüsselung der patientenbezogenen Daten mit starken kryptografischen Verfahren erreicht werden. Zum einen ist eine Verschlüsselung aller Daten zu fordern, die über ein Kommunikationsnetz übertragen werden und zwar unabhängig davon, ob es sich um ein lokales oder um ein öffentliches Netz handelt. Daneben sind alle bei den datenhaltenden Systemen gespeicherten Daten zu verschlüsseln. Nur so kann verhindert werden, dass Systemadministratoren, Wartungspersonal oder sonstige Dritte (z. B. durch Diebstahl) Kenntnis von Daten erhalten, die dem Arzt-Patienten-Geheimnis unterliegen.

(a) Verschlüsselung übertragener Daten:
Die Übertragung patientenbezogener Daten in dezentralen Systemen erfordert eine Verschlüsselung auf Anwendungsebene. Da die Systeme in dezentralen Architekturen autonom sind und sich somit aus der Sicht eines Systems die übrigen Systeme jeweils wie Black Boxes darstellen, kann nur die an Personen adressierte Verschlüsselung sicherstellen, dass nur Befugte die übermittelten Daten zur Kenntnis nehmen können.

In zentralen Systemen reicht eine Verschlüsselung auf Transportebene aus, da alle Nutzer dem Zugangs- und Zugriffskontrollmechanismus des Systems unterliegen.

In einem verteilten System reicht ebenso eine Verschlüsselung auf Transportebene aus, wenn es für den systemübergreifenden Datenaustausch einen einheitlichen, systemweiten Zugangs- und Zugriffskontrollmechanismus gibt.

Die dezentrale Architektur mit zentraler Komponente kann im Prinzip gehandhabt werden wie eine dezentrale Architektur, da die zentrale Komponente die Funktion eines „Postfaches" übernimmt, aus dem sich der Empfänger seine Nachricht abholt.

(b) Verschlüsselung gespeicherter Daten:
Die verschlüsselte Speicherung der Daten bei den datenhaltenden Systemen kann realisiert werden durch den Einsatz entsprechender Systemsoftware (z. B. Datenbanksysteme, die eine Datenverschlüsselung ermöglichen) oder durch entsprechende Zusatzsoftware (z. B. Tools zur Verschlüsselung von Plattenbereichen). Eine andere Möglichkeit zur Lösung dieses Problems besteht in der Verschlüsselung der patientenbezogenen Dokumente auf Anwendungsebene. Dabei bietet sich eine Hybridverschlüsselung an, wobei das Dokument selbst mit einem symmetrischen Schlüssel (Session Key) verschlüsselt wird und der symmetrische Schlüssel jeweils mehrfach nach einem asymmetrischen Verfahren mit den öffentlichen Schlüsseln der berechtigten Nutzern. Der für ein Dokument verantwortliche Mediziner legt dann (u. U. unter Mitwirkung des Patienten) bei der Aktivierung des Verschlüsselungsvorgangs die berechtigten Personen fest. Diese Vorgehensweise stellt sicher, dass nur berechtigte Nutzer in die Lage versetzt werden, ein Dokument zu entschlüsseln und realisiert damit gleichzeitig einen Zugriffskontrollmechanismus (bezogen auf Lesevorgänge). Das Verschlüsselungskonzept muss ein Verfahren vorsehen, dass eine Verfügbarmachung der Daten im Notfall gewährleistet.

2. Gewährleistung der Authentizität

Patientenbezogene Dokumente sind von ihrem Urheber bzw. von dem verantwortlichen Mediziner elektronisch zu signieren und u. U. mit einem Zeitstempel zu versehen. Nur durch die elektronische Signatur kann die Zurechenbarkeit von Dokumenten zum Urheber bzw. zum Verantwortlichen sichergestellt werden.

Die erforderlichen Mechanismen zur elektronischen Signatur von Dokumenten sind unabhängig von der gewählten Architektur der Datenhaltung.

3. Sicherstellung der Integrität

Mit dem elektronischen Signieren eines patientenbezogenen Dokumentes zur Sicherstellung der Authentizität wird gleichzeitig die Echtheit, Korrektheit und Vollständigkeit des Dokumenteninhalts bescheinigt, da der Signaturvorgang eine bewusste Hand-

lung vom Signierenden erfordert. Der Mediziner, der ein Dokument elektronisch signiert, also sozusagen elektronisch unterschreibt, bestätigt mit seiner Signatur nicht nur, dass er der Urheber bzw. der Verantwortliche ist, sondern gleichzeitig, dass das Dokument echt sowie inhaltlich korrekt und vollständig ist. Darüber hinaus sichert das der elektronischen Signatur zugrunde liegende kryptografische Verfahren die Erkennbarkeit einer nachträglichen Veränderung eines Dokuments. Die erfolgreiche Verifikation der Signatur eines Dokuments stellt damit gleichzeitig die Unversehrtheit des Dokumenteninhalts sicher.

4. Sicherstellung der Verfügbarkeit

Bei der Sicherstellung der Verfügbarkeit, teilen sich die verschiedenen Architekturansätze in zwei Lager:

(1) Sowohl im Falle der zentralen Datenhaltung als auch im Falle der dezentralen Datenhaltung mit zentraler Komponente ist eine hohe Verfügbarkeit realisierbar. Da bei der zentralen Datenhaltung ausschließlich die zentrale Datenverarbeitungsanlage Daten speichert und verarbeitet, sind die technischen Möglichkeiten gegeben für diese Anlage und damit für das gesamte System eine Hochverfügbarkeit zu gewährleisten. Die Situation bei der dezentralen Datenhaltung mit zentraler Komponente ist vergleichbar. Die für den einrichtungsübergreifenden Datenaustausch vorgesehenen Daten werden von der zentralen Komponente gespeichert, für die ebenso eine Hochverfügbarkeit realisierbar ist. Einschränkungen der Verfügbarkeit des Gesamtsystems können sich nur ergeben aus einer temporären Nichtverfügbarkeit von angeschlossenen dezentralen Systemen für einen notwendigen Upload oder Download.

(2) Bei der dezentralen und verteilten Datenhaltung hängt die Verfügbarkeit des Gesamtsystems von der Verfügbarkeit aller beteiligten (Sub-)Systeme ab. Bei der dezentralen Datenhaltung müssen die datenhaltenden Systeme als autonom angesehen werden, was einer systemweiten Verfügbarkeitsregelung entgegensteht. Insbesondere im niedergelassenen Bereich dürften sich die Verfügbarkeitszeiten der Systeme auf die Praxiszeiten beschränken, die zudem von Praxis zu Praxis noch unterschiedlich sein können. Insofern ist schon aus organisatorischen Gründen eine hohe Verfügbarkeit des Gesamtsystems nicht realisierbar. Bei der verteilten Datenhaltung müssen Kommunikationsprozesse - im Gegensatz zum dezentralen Fall - nicht explizit von den Nutzern eines Subsystems initiiert werden, sondern können durch systemweit verfügbare Kommunikationsmechanismen angestoßen werden. Insofern wird die Verfügbarkeit nicht notwendigerweise von beschränkten Praxiszeiten determiniert. Allerdings kann es zu technisch bedingten Ausfällen von Subsystemen kommen, die ohne Eingriffe vor Ort nicht behebbar sind. Solchen Schwierigkeiten kann man technisch dadurch begegnen, dass Datenreplikate an verschiedenen Speicherorten vorgehalten werden. Bei Nicht-

verfügbarkeit eines bestimmten Subsystems wird dann auf das entsprechende Replikat zurückgegriffen. Diese Vorgehensweise ist allerdings datenschutzrechtlich als sehr problematisch einzustufen, wenn die Replikate sich nicht im selben Herrschaftsbereich befinden, wie ihre Originale. Außerdem ergeben sich durch Replikate nicht zu unterschätzende Konsistenzprobleme. Letztlich ist auch im verteilten Fall die Verfügbarkeit abhängig von der Verfügbarkeit der beteiligten Subsysteme. Eine Hochverfügbarkeit dürfte nicht oder nur mit sehr hohen Aufwand realisierbar sein.

5. Gewährleistung der Revisionsfähigkeit

Grundvoraussetzung für die Gewährleistung der Revisionsfähigkeit ist das elektronische Signieren der patientenbezogenen Dokumente, weil hiermit die Verantwortlichkeit bzw. Urheberschaft anerkannt wird. Da der Inhalt ein signierten Dokuments nachträglich nicht mehr verändert werden kann, ohne die Signatur zu verletzen, können inhaltliche Änderungen nur in Form von Ergänzungen einem Dokument angefügt werden. Wird das Ursprungsdokument plus Ergänzungen wiederum digital signiert, kann die Historie eines Dokuments manipulationssicher festgehalten werden.

Die von der Dokumentensignatur nicht erfassbaren Verarbeitungsschritte des Übermitteln eines Dokuments und des Lesen eines Dokuments sind mittels einer manipulationssicheren Protokollierung einer Revision zugänglich zu machen. Das vollständige Löschen eines Dokuments muss aus Gründen der Dokumentationspflicht in jedem Fall vom Zugriffskontrollmechanismus unterbunden werden.

Eine Protokollierung ist bei zentralen Systemen naturgemäß recht einfach und umfassend zu realisieren, da hierbei die Datenverarbeitung von nur einem System vorgenommen wird, welches damit auch die Kontrolle über alle Verarbeitungsphasen eines Dokuments hat und außerdem die einzelnen Verarbeitungsschritte den Personen zuordnen kann, die sie verursacht haben.

Hingegen durchläuft ein Dokument im Zuge seiner Verarbeitung bei einem dezentralen System u. U. mehrere lokale Systeme. Da es in einem dezentralen System keine zentrale Kontrollinstanz über die Verarbeitungsschritte der Einzelsysteme gibt, ist eine zentrale Protokollierung nicht möglich. Hier bleibt nur die Protokollierung durch die lokalen Systeme.

Die Protokollierung von Lesevorgängen ist problemlos möglich. Die Protokollierung von Übermittlungsvorgängen erfordert allerdings die Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangs von Dokumenten. Für die Revision der Gesamtheit aller Verarbeitungsschritte eines Dokuments ist allerdings das Zusammenführen der relevanten Protokolldaten aller lokaler Systeme erforderlich, die das Dokument durchlaufen hat.

Bei verteilten Systemen können systemweit zur Verfügung stehende Dienste zur Protokollierung von Verarbeitungsschritten genutzt werden, die systemübergreifende Wirkung haben (also im Wesentlichen Datenübermittlungen). Alle anderen Aktivitäten, die nicht von systemweiten Diensten abhängen, können wie in dezentralen Systemen nur von den beteiligten lokalen Subsystemen protokolliert werden.

Die dezentrale Datenhaltung mit zentraler Komponente erlaubt eine Protokollierung aller Aktivitäten, die sich auf die zentrale Komponente beziehen, wie die zentrale Datenhaltung. Alle Aktivitäten, die sich auf die lokalen Systeme beschränken, müssen von diesen protokolliert werden. Die Protokollierung von Datenübermittlungen zwischen den lokalen Systemen und der zentralen Komponente erfordert wiederum die Mechanismen zur Gewährleistung der Nicht-Abstreitbarkeit des Sendens und Empfangs von Dokumenten.

6. Gewährleistung der Validität

Die Sicherstellung der Validität ist prinzipiell unabhängig von der Architektur der beteiligten Systeme. Sie ist aber in hohem Maße abhängig von einer Standardisierung der für die Validität relevanten Systemkomponenten (Hard- und Softwarekomponenten). Insofern ist anzunehmen, dass eine valide Datenverarbeitung umso schwieriger herstellbar ist, je heterogener die zu betrachtende Systemlandschaft ist.

7. Gewährleistung der Rechtssicherheit

Die Voraussetzung für die Rechtsicherheit ist die Revisionsfähigkeit und damit auch das elektronische Signieren eines jeden patientenbezogenen Dokuments. Damit eine elektronische Signatur rechtsverbindlich einer verantwortlichen Person zugeordnet werden kann, bedarf es der qualifizierten Signatur. Erst die qualifizierte Signatur gewährleistet eine rechtswirksame Überprüfbarkeit der Zuordnung einer Signatur zu der Person, die die Signatur erzeugt hat.

8. Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen

Die Nichtabstreitbarkeit des Sendens und Empfangs spielt primär eine Rolle in Architekturen mit dezentraler Ausrichtung, da aufgrund der Autonomie der lokalen Systeme eine Datenübermittlung explizit von einem Systemnutzer angestoßen werden muss und es keine systemübergreifenden Kontrollmechanismen gibt, die einen Übermittlungsvorgang technisch überwachen und im Fehlerfall entsprechende Maßnahmen einleiten.

Die Nicht-Abstreitbarkeit in einem dezentralen System ist nur über ein Quittungsverfahren unter Verwendung elektronischer Signaturen zu realisieren. Der Sender eines Dokuments versieht dieses zunächst mit einer elektronischen Signatur und sendet es an den Empfänger. Der Empfänger verifiziert die Signatur, um festzustellen, ob das Dokument von dem angegeben Sender stammt. Dann muss der Empfänger dem Sender bestätigen, dass er ein Dokument mit bestimmten Inhalt von ihm bekommen hat. Diese Empfangsbestätigung kann realisiert werden, indem von dem empfangenen Dokument der Hashwert gebildet wird und dieser zusammen mit einem das Dokument identifizierenden Merkmal (und evtl. mit der Eingangszeit) vom Empfänger elektronisch signiert an den Sender gesendet wird. Der Sender verifiziert die Signatur der Quittung, bildet seinerseits den Hashwert des von ihm gesendeten Dokuments und vergleicht diesen mit dem in der Quittung zugesandten Hashwert. Stimmen beide Werte überein, kann der Sender sicher sein, dass genau der von ihm spezifizierte Empfänger (aufgrund der Signaturverifikation) auch genau das von ihm gesendete Dokument (aufgrund des Vergleichs der Hashwerte) erhalten hat. Schlägt die Signaturverifikation oder der Hashwertvergleich fehl, muss sich der Sender mit dem Empfänger in Verbindung setzen. Erhält der Empfänger keine Reklamation durch den Sender, dann kann er seinerseits sicher sein, dass das empfangene Dokument genau von dem vermuteten Sender kommt, mit genau dem vom Sender gesendeten Inhalt. Erhält bei diesem Quittungsverfahren der Sender nach einer gewissen Zeit keine Quittung für seine gesendete Nachricht, so ist entweder die Nachricht oder die Quittung nicht zugestellt worden. Für diesen Fall ist eine adäquate Handlungsweise zu vereinbaren (z. B. erneutes Senden der Nachricht nach einer Wartefrist oder Kontaktieren des Empfängers).

Solch ein Quittungsverfahren ist natürlich softwaretechnisch entsprechend so zu unterstützen, dass es so weit wie möglich automatisiert abläuft. Ein Standard-Email-System ist nicht in der Lage, die Forderung der Nicht-Abstreitbarkeit zu erfüllen.
Bei einem dezentralen System mit zentraler Komponente ist ein solches Quittungsverfahren in modifizierter Form ebenfalls realisierbar. Hier erhält der Sender einer Nachricht eine Quittung von der zentralen Komponente und der Empfänger sendet seine Quittung an die zentrale Komponente. Die Nicht-Abstreitbarkeit ist dann über die Informationskette Sender, Protokolldaten der zentralen Komponente, Empfänger herstellbar.

Die Signatur von Dokumenten zur Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen ist nicht zu verwechseln mit der Signatur von Dokumenten zur Gewährleistung der Authentizität. Im ersten Fall dient die Signatur der Zuordnung eines Dokuments zu seinem Sender, im zweiten Fall der Zuordnung eines Dokuments zu seinem Urheber. Da der Sender eines Dokuments aber nicht notwendigerweise auch der Urheber ist, muss jedes Dokument bei einer Übermittlung vom Sender elektronisch signiert werden.

Bei zentralen und verteilten Architekturen ist die Nicht-Abstreitbarkeit auf der Grundlage der entsprechenden Protokollinformationen realisierbar.

9. Gewährleistung der Nutzungsfestlegung

Da im zentralen Fall der Zugriffskontrollmechanismus eine systemweite Kontrolle ausüben kann, ist eine Nutzungsfestlegung prinzipiell umfassend zu realisieren. Es kommt nur darauf an welche Differenzierung das Berechtigungskonzept bzw. die Zugriffskontrolle des jeweiligen Systems zulässt. Aufwendig könnte die Umsetzung eines Nutzungsausschlusses sein (z. B. leseberechtigt sind alle Mediziner der Abteilung A (Rolle) mit Ausnahme von Herrn Dr. X der Abteilung A).

Existiert in einem System mit verteilter Datenhaltung ein systemweites Berechtigungskonzept und ein systemweiter Zugriffskontrollmechanismus sind Nutzungsrechte, die systemübergreifende Bedeutung haben, wie bei einem Zentralsystem definierbar.

Bei dezentralen Systemen sind Nutzungsrechte mittels des Zugriffskontrollmechanismus jeweils für die lokalen Systeme definierbar. Wird ein Dokument von einem lokalen System an ein anderes übermittelt, müssen die u. U. bestehenden Nutzungsrechte bzw. Nutzungsausschlüsse mit dem Dokument übermittelt werden. Der Empfänger des Dokuments muss dann für deren Einhaltung sorgen.

Dezentrale Systeme mit zentraler Komponente können Zugriffskontrollmechanismen für die zentrale Komponente wie im zentralen Fall realisieren. Dokumente, die sich im Speicherbereich der Subsysteme befinden oder in deren Speicherbereich gelangen, entziehen sich dem zentralen Zugriffskontrollmechanismus und sind wie im dezentralen Fall zu behandeln.

VI. Beispiele für Ansätze/Projekte zur Kommunikation im Gesundheitswesen

1. Patientenbegleitende Dokumentation (PaDok)

PaDok wurde vom Fraunhofer-Institut für Biomedizinische Technik als technische Lösung zur Erfüllung eines großen Teils der alltäglichen Kommunikation von Leistungserbringern im Gesundheitswesen entwickelt. Technisch realisiert sind zur Zeit der elektronische Arztbrief, die elektronische Überweisung, die elektronische Einweisung, die elektronische Quartalsabrechnung, das elektronische Rezept und die elektronische Fall-Akte. Von seiner Architektur unterstützt PaDok eine dezentrale Datenhaltung mit zentraler Komponente. Die zentrale Komponente wird von einem PaDok-Server gebildet, der als Nachrichtenpuffer dient. Der Absender einer Nach-

richt versieht eine elektronische Information mit einer Empfänger-Kennung und schickt sie an den PaDok-Server, der an einer zentralen Stelle im regionalen Netzwerk steht. Der Empfänger der Nachricht kann sich dann die Nachricht vom PaDok-Server abholen. Insofern gleicht das Grundprinzip von PaDok dem der E-Mail. Alle PaDok-Nachrichten werden elektronisch signiert und mittels eines asymmetrischen Verfahrens verschlüsselt. Damit ist die Vertraulichkeit, Integrität und Authentizität von PaDok-Nachrichten sichergestellt.

Im Gegensatz zu einem Standard-Mailingsystem erlaubt PaDok die nicht-adressierte Kommunikation. Wird beispielsweise ein Patient von seinem Hausarzt zwecks einer internistischen Weiterbehandlung überwiesen, steht u. U. zum Zeitpunkt der Überweisung der Internist als Person noch nicht fest, da der Patient die freie Arztwahl hat. Das Problem besteht nun darin, dass zum Verschlüsseln der zu übermittelnden Dokumente mittels eines asymmetrischen Verfahrens der öffentliche Schlüssel des Empfängers erforderlich ist, also zum Zeitpunkt der Verschlüsselung der konkrete Empfänger feststehen muss. PaDok löst dieses Problem, indem es die Dokumente des Absenders (hier der Hausarzt), die an den Empfänger (hier der noch nicht feststehende Internist) übermittelt werden sollen, mit einer Vorgangskennung versieht. Diese Vorgangskennung besteht aus zwei Teilen. Der eine Teil dient der Identifikation der Dokumente und der andere Teil wird als Schlüssel (Vorgangsschlüssel) verwendet. Vereinfacht ausgedrückt werden nun die Dokumente durch ein zweistufiges Verschlüsselungsverfahren verschlüsselt. Dazu ist der Vorgangsschlüssel und der öffentliche Schlüssel des PaDok-Servers erforderlich. Die verschlüsselten Dokument werden an den PaDok-Server versandt und der Patient erhält die Vorgangskennung, entweder in ausgedruckter Form oder auf einer Chipkarte. Findet sich der Patient schließlich bei einem weiterbehandelnden Internisten seines Vertrauens ein, so übergibt er ihm die Vorgangskennung. Der identifizierende Teil der Vorgangskennung dient nun der Selektion der Dokumente auf dem PaDok-Server. Der PaDok-Server entschlüsselt die selektierten Dokumente mit dem geheimen Server-Schlüssel und verschlüsselt sie anschließend mit dem öffentlichen Schlüssel des anfordernden Internisten. Die Verschlüsselung, die mit dem Vorgangsschlüssel erfolgte, bleibt bei diesem Umschlüsselungsvorgang erhalten, so dass die Dokumente auf dem Server zu keinem Zeitpunkt lesbar sind. Die umgeschlüsselten Dokumente werden dann an den Internisten geschickt. Dieser benötigt zur Entschlüsselung seinen geheimen Schlüssel und den in der Vorgangskennung enthaltenen Vorgangsschlüssel. Mit diesem Verfahren ermöglicht PaDok eine nicht-adressierte Kommunikation unter Wahrung einer adressierten Vertraulichkeit. Der Patient wird dadurch in die Lage versetzt, den Adressaten seiner Dokumente (hier der weiterbehandelnde Internist) selbst zu bestimmen, ohne dass er diesen dem Absender der Dokumente (hier der überweisende Hausarzt) mitteilen muss. Außerdem ist sichergestellt, dass nur der vom Patienten bestimmte Absender die Dokumente lesen kann.

Der Mechanismus der nicht-adressierten Kommunikation ermöglicht es außerdem,

patientenbezogene Fallakten anzulegen. Hierzu können die für einen Fall relevanten Dokumente von der an der Behandlung des Patienten beteiligten Ärzten in einer temporären Akte auf dem PaDok-Server hinterlegt werden. Der Patient selbst hat auf der Grundlage des oben beschrieben Verfahrens zu jedem Zeitpunkt seiner Behandlung die Entscheidung darüber, welcher behandelnde Arzt Dokumente seiner Fallakte einsehen kann.

2. Die „Elektronische Patientenakte" (EPA)

Der Begriff „Elektronische Patientenakte" wird in unterschiedlichen Ausprägungen verwendet. Zum einen wird unter einer Elektronischen Patientenakte eine Sammlung medizinischer Informationen zu einem Patienten innerhalb einer Institution auf digitalen Datenträgern verstanden. Dies kann die Krankenakte über einen Patienten in einem Krankenhaus sein, aber auch die ärztliche Dokumentation in einer Praxis. Daneben wird der Begriff zunehmend auch werbewirksam von kommerziellen Anbietern benutzt. Sie bieten an, medizinische Daten über eine Person über das Internet zur Verarbeitung oder/und zum Abruf durch einen Arzt, Krankenhaus etc. bereitzuhalten. Im Rahmen der Diskussion der Reform im Gesundheitswesen wird allerdings der Begriff in einer anderer Bedeutung verwendet. Unter einer „elektronischen Patientenakte" ist dabei die jederzeit verfügbare, institutionsübergreifende und unter Kontrolle des Patienten und (eines) Arztes befindliche Kopie aller relevanten Daten der Krankengeschichte zu sehen. Auf der Basis dieser Definition wurden von verschiedenen Gruppen beispielsweise „Junge Mediziner in der SPD", Konzepte entwickelt, die einerseits die Vorteile der informationstechnischen Verarbeitung medizinischer Daten nutzen und anderseits durch den Einsatz von datenschutzfreundlichen Techniken den Datenschutz und die Datensicherheit für diese Informationen sichern will.

Die Grundkonzeptionen aller EPA-Modelle geht dabei von einer Kombination einer Chipkarte mit Schlüsselfunktion und einem gesicherten Zugang zu pseudonymisierten Daten aus. In den vorgestellten Projekten sollen folgende technische Maßnahmen den Datenschutz sicherstellen:

- Nur mit einer Chipkarte und der Einwilligung des Patienten ist ein Zugang zu seiner EPA technisch überhaupt möglich.
- Die Einwilligung kann auf einzelne Ärzte oder Krankenhäuser beschränkt werden.
- Ein Widerruf ist jederzeit möglich, auch die Löschung aller Daten ist auf Wunsch des Patienten vorgesehen.

Die Modelle variieren dahin gehend, dass der Ort der Speicherung der Daten, beispielsweise auf der Chipkarte des Patienten oder auf zentralen und dezentralen, regionalen Servern und der Umfang der medizinischen Daten (Arztbrief, Rezept, Röntgenaufnahmen etc.) verschieden ist.

Der Zugang zu den medizinischen Daten steht allerdings immer unter der Prämisse, dass keine Daten ohne Karte des Patienten aus dem System gelangen können und damit von Unbefugten, also auch Ärzten, gelesen werden können, d. h., der Patient kontrolliert den Zugang zu seinen Daten. Eingeschränkt wird dieser Zugang des Patienten in manchen Modellen dadurch, dass für den Zugang auch ein Arzt benötigt wird. Die Speicherung der medizinischen Daten erfolgt in der Regel in pseudonymisierter Form.

Technisch wird der Zugang zu den medizinischen Daten mit Hilfe von Verschlüsselungsverfahren sichergestellt. Ein Modell geht dabei von folgendem Verfahren aus:

Die medizinischen Daten werden auf einem regionalen Server, beispielsweise in einem Krankenhaus verschlüsselt gespeichert. Zur Pseudonymisierung der Daten erzeugt die Software auf der Chipkarte des Versicherten einen Code, der den Zugang zu Daten ermöglicht, d. h. (selbst) der Rechner des Arztes kennt nicht das Pseudonym des Patienten. Mit Hilfe des Codes, also weder mit dem Namen des Patienten, noch seinem Pseudonym, werden Daten von einem (regionalen) Server angefordert oder geschrieben. Zur Absicherung des Abrufes und/oder der Verarbeitung von Daten muss zunächst die Authentifizierung des Arztes mit Hilfe eine Health Care Professional Card erfolgen, sowohl beim (regionalen) Server wie gegenüber der Patientenchipkarte. Die Einwilligung des Patienten zu der Verarbeitung bzw. zum Abruf der Daten wird über die Vorlage bzw. Benutzung der Patientenchipkarte realisiert. Damit sichergestellt wird, dass ein Widerruf der Verarbeitung der Daten möglich ist, wird zudem auf der Karte des Patienten ein Code generiert, der den Arzt zur Datenabfrage /Datenverarbeitung berechtigt („upload code“). Mit Hilfe dieses UPLOAD-Code kann ein Arzt allerdings nur eine befristete Zeit beispielsweise 3 Monate auf die Daten des Patienten zugreifen, danach erlischt dieses Recht, der UPLOAD-Code wird ungültig. Die Übertragung der Daten zum bzw. vom Server wird zudem über Session-Keys verschlüsselt. Geht der Patienten im Rahmen einer Behandlung zu einem anderen Arzt, kann dieser bei Vorlage der Patientenchipkarte und bei Freigabe der Daten durch den einstellenden Arzt befristet auf die Daten zugreifen.

Die der EPA zugrunde liegen Modelle sehen in allen Fällen einerseits die Verarbeitung von medizinischen Daten zu besseren und wirtschaftlicheren Versorgung des Patienten vor, anderseits soll durch die Pseudonymisierung der Daten anderen Bedarfsträgern (Gesundheitsministerium, Krankenkassen, Forschung und Wissenschaft) die Möglichkeit gegeben werden, statistische Auswertung auf den Daten durchführen zu können. Aus Gründen des Datenschutzes kann auch eine Pseudonymisierung der Arztdaten in diesen Datensätzen vorgesehen werden. Modellversuche mit einer (größeren) Anzahl von Patienten und Ärzten bzw. medizinischen Institutionen stehen noch aus.

14.7 Möglichkeiten und Risiken von USB-Schnittstellen

USB steht für Universal Serial Bus und ist ein Industriestandard, um periphere Geräte an einen PC oder ein Notebook anzuschließen. Die derzeit aktuelle Spezifikation USB 2.0 hat im Gegensatz zum älteren Standart USB 1.0 eine höhere Datenübertragungsrate. Die Windows-Betriebssysteme 98, ME, 2000, XP und Linux unterstützen die USB-Schnittstelle. Für alle Computer mit Windows NT 4.0 müssen die USB-Treiber nachinstalliert werden. Jeder neue PC ist mit zwei bis vier USB-Ports für den Anschluss von Peripheriegeräten ausgestattet. Ältere Rechner lassen sich mit PCI-Karten mit integrierten USB-Schnittstellen nachrüsten. An diese Schnittstellen können alle USB-Geräte wie Tastaturen, Mäuse, Drucker, Kameras, Modems, Festplatten, Smart-Cards, Joysticks, Scanner, USB-Sticks und auch USB-Hubs (Verteiler), an denen mehrere USB-Geräte gleichzeitig eingesteckt werden können, angeschlossen werden.

Die USB-Schnittstelle hat mehrere Vorteile:

- Durch „Hot-Plug & Play“ werden USB-Geräte bei laufendem Betriebssystem nach dem Einstecken erkannt und ihre Treiber automatisch installiert. Die Geräte sind sofort betriebsbereit, ohne dass der PC neu gestartet werden muss. Sie können während des PC-Betriebs angeschlossen und entfernt werden.
- An einen USB-Hub können weitere USB-Geräte (i. a. 5 bis 10 Geräte) angeschlossen werden.
- Die Datenübertragungsrate ist gegenüber der älteren seriellen bzw. parallelen Schnittstelle höher (bei USB 2.0 ist auch der Festplattenanschluss praktikabel).
- Externe USB-Speichergeräte wie „Memory Sticks“, „Memory Cards“ oder Finger-Sticks lassen sich mit einer Speicherkapazität von bis zu zwei GB anschließen. Sie können mit Passwörtern oder per Fingerabdruck vor unbefugter Benutzung geschützt werden. Der Finger-Sensor ist dabei im Stick integriert.
- Eine USB-Smart-Card oder ein e-Token benötigt gegenüber einem herkömmlichen Smart-Card-Systeme kein zusätzliches Lesegerät. Der Krypto-Chip ist im USB-Gerät integriert und kann mit Passwort oder PIN gesichert werden. Eine USB-Smart-Card kann sicher authentifizieren, signieren und verschlüsseln.
- Mit einem USB-Stick kann unter bestimmten Voraussetzungen ein Notfall-System gebootet werden (Alternative zur Notfall-Diskette oder CD).
- Stecker und Buchse sind für alle USB-Geräte gleich.
- Das Kabel ist dünn, flexibel und preiswert. Von den vier Adern dienen zwei zur Datenübertragung und zwei zur Stromversorgung von USB-Geräten mit niedrigem Stromverbrauch. Diese Peripheriegeräte benötigen deshalb keine separate Stromversorgung.
- Mit USB-Link-Kabeln können zwei oder mehrere PCs verbunden (vernetzt) werden.

Den vielen Vorteilen und Einsatzmöglichkeiten der neuen Schnittstelle stehen jedoch bei unautorisiertem Gebrauch erhebliche Datenschutzrisiken gegenüber. In sensiblen Bereichen kann bisher beim PC der Zugriff auf Laufwerke (Diskette oder CD) aus Gründen des Datenschutzes und der Datensicherheit gesperrt werden. Für die USB-Schnittstelle ist dies aber nur eingeschränkt möglich, weil zukünftig auch die Eingabegeräte (Tastatur, Maus) und Ausgabegeräte (Drucker) nur mit USB-Anschluss angeboten werden. Damit können wie oben geschildert auch Speichermedien wie Memory Stick, USB-Sticks oder USBdisk mit einer hohen Speicherkapazität bis zu 2 GB angeschlossen werden. Eine Abschottung von personenbezogenen Daten in einem geschützten Bereich wird dadurch ausgehebelt. Außerdem besteht die Gefahr, dass durch den unkontrollierten Datenaustausch auch externe Programme aufgespielt und Viren u. ä. importiert werden. Die datenverarbeitende Stelle muss diese Risiken kennen und versuchen, mit technischen und organisatorischen Maßnahmen die Missbrauchsmöglichkeiten einzuschränken. So kann der Beschäftigte Dateien nur dann kopieren, ändern oder einspielen, wenn er entsprechende Zugriffsrechte auf seinem Computer oder die Ressourcen im Netz besitzt. Deshalb ist es unbedingt notwendig, die Zugriffsrechte, die zur Erledigung der Aufgabe erforderlich sind, immer restriktiv zu vergeben.

Mit technischen Maßnahmen lässt sich der unbefugte Zugriff auf die USB-Schnittstelle zwar aufwändig sperren, allerdings kann der Beschäftigte dann auch nicht mehr auf Geräte mit USB-Anschluss zugreifen. Die einfachste Möglichkeit ist die Deaktivierung des USB-Ports im BIOS oder im Gerätemanager. Dies verhindert allerdings nicht immer den Zugriff auf USB-Geräte. Ein anschließender Test ist daher unbedingt erforderlich. Eine weitere Reglungsmöglichkeit für den Zugriff ist das Deaktivieren bzw. Aktivieren von USB-Ports in der „Registry“ (bei Windows-Systemen). In der „c´t 8/2003“ ist darüber hinaus ein VB-Skript für die USB-Schnittstelle abgedruckt, mit dessen Hilfe ein Administrator festlegen kann, welcher Benutzer ein USB-Gerät anschließen darf. In diesem Artikel wird auch auf ein kommerzielles Produkt *SecureNT* verwiesen. Außerdem soll man mit dem Security-Tool *Device Lock* USB-Sticks benutzerbezogen verwaltet können. Die Verwendung von Hardware-Schutzmaßnahmen (analog Diskettenschloss) ist noch nicht bekannt.

Ein Missbrauch der USB-Schnittstelle kann demnach vermieden werden durch:

- organisatorische Regelungen, die das unautorisierte Anschließen von USB-Geräten untersagen und bei Zuwiderhandlung Sanktionen androhen, verbunden mit regelmäßigen Kontrollen,
- restriktive Vergabe von Zugriffsrechten,
- USB-Ports im BIOS, Gerätemanger oder Registry sperren, deaktivieren oder das angesprochene Skript einsetzen, solange noch Ein- und Ausgabegeräte ohne USB genutzt werden können. Sollte dies bald nicht mehr möglich sein, wird diese Lösung problematisch.

15 Vortrags- und Schulungstätigkeit

In diesem Jahr nicht belegt.

16 Materialien

16.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.1.1 Entschließung zwischen der 63. und 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Geplanter Identifikationszwang in der Telekommunikation

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift „Schließen von Regelungslücken“ stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig - teilweise nach jedem Telefonat - wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.

- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.

- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.

- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.

- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.

- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.

Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

16.1.2 Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002 in Trier zur Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

16.1.3 Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002 in Trier zur systematischen verdachtslosen Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Ab-

rechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen - allerdings unter weitgehendem Ausschluss der Öffentlichkeit - diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebensowenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

16.1.4 Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002 in Trier zur datenschutzgerechten Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

16.1.5 Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in Dresden: Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.
Sie sehen dabei folgende essentielle Punkte:

- Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

- Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.
- Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.
- Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
- Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).

- Technischer Datenschutz

  Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

- Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

  Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein

Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

- Förderung von datenschutzgerechter Technik

  Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind. Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird. Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

- Anonyme Internetnutzung

  Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von e-mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht. Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-

Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

- Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

  Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten: Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken. Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden. Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

  Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung - für geboten.

  Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung - als grundrechtssicherndes Verfahrenselement ergreifen muss.

- Stärkung des Schutzes von Gesundheitsdaten

  Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weiter-

gegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

- Datenschutz und Gentechnik

  Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen - dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

- Datenschutz im Steuerrecht

Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und –speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

- Arbeitnehmerdatenschutz

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

  Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.
  Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

◆ Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

  Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

  Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

◆ Stellung des Bundesdatenschutzbeauftragten

  Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

◆ Verbesserung der Informationsrechte

  Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

16.1.6 Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in Dresden zu TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz „Trusted Computing Platform Alliance“ (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,

- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet und E-mail-Verkehr durch Softwarerestriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

16.1.7 Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in Dresden zur Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Absatz 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

16.1.8 Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in Dresden: Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt

ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.
So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)“ entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen. [1]

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt. [2]

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und –Produkte vertrauenswürdig und daten-

---

1 Die Schutzprofile mit dem Titel „BISS – Benutzerbestimmbare Informationsflusskontrolle“ haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.
2 Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

schutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

16.1.9 Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in Dresden: Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u.a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1.
Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2.
Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grds. selbst zu entscheiden,
- ob sie überhaupt verwendet wird,
- welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
- welche Daten zu löschen sind und wann das zu geschehen hat,
- ob sie im Einzelfall vorgelegt wird und
- welche Daten im Einzelfall ausgelesen werden sollen.

Sicherzustellen ist weiterhin
- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass" (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen" vom 3. Mai 2002, wonach „der Patient Herr seiner Daten" sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3.
Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski", „raucht", „trinkt zwei Biere pro Tag"), diese überwachen und so zur „Gesundheitspolizei" werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4.
Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

16.1.10 Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in Dresden zur Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kenn-

zeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10 Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

16.1.11 Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003 in Dresden zur elektronischen Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28.1.2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen„ eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unter-

zeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.

- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen.
  Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.

Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,

- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,

- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,
- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,
- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,
- e-Government- und e-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,
- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,
- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

16.1.12 Entschließung zwischen der 65. und 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz v. 28.3.2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher - die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PINs und PUKs – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmä-

ßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12.3.2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines „vertragslosen" Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwcken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

16.1.13 Entschließung zwischen der 65. und 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sogen. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr - wie vom geltenden Recht gefordert - in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,

- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nichtcodieren-den Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z. B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem

sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

16.1.14 Entschließung zwischen der 65. und 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuordnung der Rundfunkfinanzierung

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die die GEZ künftig auch online zugreifen.

- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.

- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

16.2 Sonstiges

16.2.1 Urteil des Bundesgerichtshofs vom 9. Dezember 2002 in der Strafsache gegen Dr. Thomas Giesen wegen Verletzung des Dienstgeheimnisses

5 StR 276/02

BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

vom 9. Dezember 2002
in der Strafsache
gegen

Dr. Thomas G i e s e n aus Dresden,
geboren am 22. Dezember 1946 in Kapellen-Stolzenfels,

wegen Verletzung des Dienstgeheimnisses

Der 5. Strafsenat des Bundesgerichtshofs hat in der Sitzung vom 9. Dezember 2002, an der teilgenommen haben:

Vorsitzende Richterin Harms,

Richter Häger,
Richter Dr. Raum,
Richter Dr. Brause,
Richter Schaal

als beisitzende Richter,

Oberstaatsanwalt beim Bundesgerichtshof Schaper

als Vertreter der Bundesanwaltschaft,

Rechtsanwalt Prof. Dr. Dahs,
Rechtsanwalt Heinemann,
Rechtsanwalt Priv.-Doz. Dr. Lesch

als Verteidiger,

Justizangestellte Thiel,
Justizangestellte Reimann

als Urkundsbeamtinnen der Geschäftsstelle,

für Recht erkannt:

Die Revision der Staatsanwaltschaft gegen das Urteil des Landgerichts Dresden vom 7. November 2001 wird verworfen.

Die Kosten des Rechtsmittels und die dem Angeklagten dadurch entstandenen notwendigen Auslagen werden der Staatskasse auferlegt.

– Von Rechts wegen –

Gründe

Das Landgericht hat den Angeklagten von dem Vorwurf freigesprochen, im August 2000 als Sächsischer Datenschutzbeauftragter in drei Fällen Dienstgeheimnisse verletzt zu haben. Die hiergegen gerichtete Revision der Staatsanwaltschaft, die mit der Sachrüge die Beweiswürdigung und die rechtliche Würdigung angreift, bleibt ohne Erfolg.

I.

Das Landgericht hat folgende Feststellungen getroffen:

Der Angeklagte ist seit 1992 Datenschutzbeauftragter des Freistaats Sachsen. In dieser Eigenschaft wurde er vom damaligen Oberbürgermeister der Stadt Görlitz, Lechner, zwischen 1998 und 2000 mehrfach von dem Verdacht unterrichtet, das Sächsische Staatsministerium der Justiz könne in einem Ermittlungsverfahren gegen den Beigeordneten für Finanzen der Stadt

Görlitz und stellvertretenden Kreisvorsitzenden der CDU, Neumer, in unlauterer Weise auf die Staatsanwaltschaft eingewirkt haben. Das Verfahren gegen Neumer war auf Grund einer Strafanzeige des ebenfalls der CDU angehörenden Oberbürgermeisters Lechner eingeleitet worden. Im Rahmen der datenschutzrechtlichen Anrufung überprüfte der Angeklagte im Juli 2000 die Akten des Ministeriums zum „Fall Neumer". Dabei stellte er fest, daß sich der Görlitzer Landtagsabgeordnete und dortige Kreisvorsitzende der CDU, Bandmann, am 19. August 1997 telefonisch an den Justizminister Heitmann gewandt und den Wunsch nach einer raschen Klärung der Vorwürfe – auch im Hinblick auf einen am 20. September 1997 stattfindenden Kreisparteitag der CDU – zum Ausdruck gebracht hatte. Der Justizminister hatte daraufhin die Strafrechtsabteilung seines Hauses mit der Vorlage eines Berichts über dieses Verfahren beauftragt, der ihm möglichst noch vor einer am 28. August 1997 in Görlitz stattfindenden Klausur der Landtagsfraktion der CDU zugeleitet werden sollte; zugleich hatte er darum gebeten, auf eine „beschleunigte Behandlung" des Ermittlungsverfahrens hinzuwirken. Der für strafrechtliche Einzelsachen zuständige Referatsleiter hatte in der Folgezeit den Leitenden Oberstaatsanwalt in Görlitz telefonisch vom Anliegen des Justizministers unterrichtet. Nach Eingang des Berichtes der Staatsanwaltschaft Görlitz hatte er am 26. August 1997 über den Gegenstand des Ermittlungsverfahrens gegen Neumer und den damaligen Sachstand einen umfangreichen Vermerk verfaßt, in dem darauf hingewiesen wurde, er hätte den Leitenden Oberstaatsanwalt gebeten, „für eine rasche und sensible Behandlung der Sache Sorge zu tragen". Dieser Vermerk war auf dem Dienstweg dem Minister vorgelegt worden. Dieser hatte am 27. August 1997 die Vorlage zur Kenntnis genommen; er hatte den Landtagsabgeordneten Bandmann am folgenden Tag unterrichtet und am 30. August 1997 die Strafrechtsabteilung gebeten, ihn weiter „auf dem Laufenden zu halten".

Diese aus den Akten ersichtlichen Vorgänge bewertete der Angeklagte als erhebliche Verstöße gegen die Bestimmungen des Datenschutzgesetzes. Nachdem er die Führung des Justizministeriums unverzüglich vor-

ab informiert hatte, kündigte er mit Schreiben vom 18. Juli 2000 eine datenschutzrechtliche Beanstandung an und gab dem Ministerium Gelegenheit zur Stellungnahme bis 24. Juli 2000. Mit Schreiben vom 25. Juli 2000 wies der Leiter der Strafrechtsabteilung die Vorwürfe des Datenschutzbeauftragten zurück; die von diesem beanstandete Vorgehensweise sei rechtmäßig gewesen. Der Angeklagte wandte sich daraufhin an den Chef der Sächsischen Staatskanzlei mit der Bitte, den Justizminister zu bewegen, Berichtsanforderungen der beanstandeten Art sowie die Informierung Dritter zu unterlassen und die in Verwaltungsvorschriften festgelegten Berichtspflichten der Staatsanwaltschaft zu ändern.

Nachdem am 16. August 2000 ein Journalist der BILD-Zeitung einem Mitarbeiter des Angeklagten einen Entwurf eines Zeitungsartikels über das Verhalten des Justizministers im Hinblick auf das Ermittlungsverfahren gegen Neumer zur Kenntnis gebracht, vor einer beabsichtigten Veröffentlichung aber noch einige Tage Stillschweigen zugesagt hatte, wandte sich der Angeklagte am 21. August 2000 erneut an den Chef der Staatskanzlei und kündigte an, wegen des Drucks der Presse am Folgetag um 18.00 Uhr nach Eingang einer von ihm erwarteten Stellungnahme des Justizministers eine Pressekonferenz abzuhalten. Am Morgen des 22. August 2000 erschien indes bereits in großer Aufmachung der zuvor angekündigte bebilderte Bericht in der BILD-Zeitung, in dem unter anderem das Anliegen des Landtagsabgeordneten Bandmann und dessen Unterrichtung durch den Justizminister – letzteres ohne Einzelheiten, aber auf dem Hintergrund politischer Verbindungen – geschildert wurde; ferner wurden Neumer als Beschuldigter sowie Lechner als Anzeigeerstatter benannt. In der auf 18.00 Uhr einberufenen Pressekonferenz verlas der Angeklagte daraufhin vor den anwesenden Pressevertretern die vom Justizminister stammenden Verfügungen (Fall 1 der Anklage). Am nächsten Tag übersandte er dem Justizministerium gegen 9.00 Uhr eine datenschutzrechtliche Beanstandung, in der er die Gesetzesverstöße nochmals im Einzelnen darstellte, die Verfügungen des Justizministers zitierte und eine abstrakte Darstellung des Berichts des Leiten-

den Oberstaatsanwalts in Görlitz vom 25. August 1997 beifügte. Gegen 10.00 Uhr übermittelte er das gesamte Beanstandungsschreiben an den Petenten Lechner (Fall 2 der Anklage), eine Stunde später berief er eine weitere Pressekonferenz ein. In diesem Rahmen verlas er die gesamte datenschutzrechtliche Beanstandung im Wortlaut und legte für die Journalisten Kopien zur Mitnahme aus (Fall 3 der Anklage).

Das Landgericht hat die im August 1997 aktenkundig gewordenen verwaltungsinternen Vorgänge im Sächsischen Staatsministerium der Justiz, die in diesem Zusammenhang erfolgte Unterrichtung Dritter über den Sachstand des damaligen Ermittlungsverfahrens sowie die datenschutzrechtliche Beanstandung des Datenschutzbeauftragten gegenüber dem Justizministerium vom 23. August 2000 jeweils als Dienstgeheimnisse gemäß § 353b Abs. 1 StGB angesehen. Der Angeklagte habe aber bei Offenbarung dieser Geheimnisse keine wichtigen öffentlichen Interessen im Sinne dieser Vorschrift gefährdet; zudem habe er nicht unbefugt gehandelt, sondern sei aus verfassungsrechtlichen Gründen wegen Notstands gerechtfertigt.

II.

Die gegen das freisprechende Urteil gerichtete Revision der Staatsanwaltschaft ist unbegründet.

1. Ohne Erfolg rügt die Beschwerdeführerin, die Beweiswürdigung sei unvollständig und genüge nicht den Anforderungen des § 267 Abs. 5 StPO. Dem Urteil ist zu entnehmen, daß der Angeklagte den Sachverhalt so geschildert hat, wie er im Urteil festgestellt worden ist. Seine Angaben werden bestätigt durch die in der Hauptverhandlung verlesenen Schriftstücke und die Aussagen der vom Landgericht benannten Zeugen, die als Beteiligte die Darstellung des Angeklagten „objektiviert" haben. Mehr ist bei einem Freispruch aus rechtlichen Gründen nicht geboten.

2. Der Freispruch hält auch im übrigen sachlichrechtlicher Nachprüfung stand.

a) Mit der Verlesung der vom Justizminister stammenden Verfügungen am 22. August 2000 (Fall 1 der Anklage) hat der Angeklagte nicht gegen § 353b StGB verstoßen.

Gemäß § 353b Abs. 1 Nr. 1 StGB macht sich strafbar, wer ein Geheimnis, das ihm als Amtsträger anvertraut worden oder sonst bekannt geworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet.

aa) Geheimnisse im Sinne dieser Vorschrift sind Tatsachen, die nur einem begrenzten Personenkreis bekannt und zudem geheimhaltungsbedürftig sind. Darunter fallen auch personenbezogene Umstände, die vertraulich zu behandeln sind. Sie müssen dem betreffenden Amtsträger im inneren Zusammenhang mit seiner Diensttätigkeit bekanntgeworden sein (vgl. BGHSt 46, 339, 340 f.; 10, 108 f.; BGH NStZ 2000, 596, 598; Hoyer in SK-StGB 41. Lfg. § 353b Rdn. 6). In diesem Sinne kann auch rechtswidriges Handeln Dritter im Einzelfall eine geheimhaltungsbedürftige Tatsache darstellen (vgl. BGHSt 20, 342, 354 ff.; Hoyer in SK aaO Rdn. 5).

Das als normatives Element des Geheimnisbegriffs erforderliche Geheimhaltungsbedürfnis (vgl. BGHSt 46, 339, 341) ergibt sich vorliegend aus § 23 Abs. 6 Satz 1 des hier maßgeblichen Sächsischen Datenschutzgesetzes (SächsDSG). Nach dieser Vorschrift unterfallen die dem Angeklagten als Sächsischem Datenschutzbeauftragten bei seiner Tätigkeit bekanntgewordenen personenbezogenen Daten der Pflicht zur Verschwiegenheit. Von ihr miterfaßt werden auch personenbezogene Daten der vom Datenschutzbeauftragten kontrollierten Amtswalter, weil insoweit das dienstliche Grundverhältnis betroffen ist, in dem der öffentliche Bedienstete seinem Dienstherrn als Grundrechtsträger gegenübertritt (vgl. Globig, DÖD 1991, 217, 218, 220).

Ausgenommen sind nach Satz 2 dieser Bestimmung Mitteilungen im dienstlichen Verkehr oder allgemein zugängliche Daten. Solche sind – wie offenkundige Tatsachen im Sinne von § 61 Abs. 1 Satz 2 BBG, § 39 Abs. 1 Satz 2 BRRG, § 23 Abs. 5 Satz 2 BDSG (vgl. BGH, Urt. vom 8. Oktober 2002 – 1 StR 150/02 S. 7; zur Veröffentlichung in BGHSt bestimmt) – insbesondere dann anzunehmen, wenn von ihnen verständige und erfahrene Menschen ohne weiteres Kenntnis haben und sie keiner weiteren Überprüfung oder Bestätigung bedürfen (vgl. BGH aaO S. 6, BGH NStZ 2000, 596, 597 m. w. N.; Träger in LK 10. Aufl. § 353b Rdn. 7; Tröndle/Fischer, StGB 51. Aufl. § 353b Rdn. 7, § 93 Rdn. 9).

Entsprechendes ergibt sich aus § 78 Abs. 1 Satz 2 SächsBG, wonach die Verschwiegenheitspflicht entfällt, wenn die fraglichen Tatsachen offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Diese für weisungsunterworfene Landesbeamte getroffene Regelung kann als allgemeiner Grundsatz auf den nach § 23 Abs. 4 Satz 1 SächsDSG unabhängigen, weisungsfreien und nur dem Gesetz unterworfenen Sächsischen Datenschutzbeauftragten, der Beamter auf Zeit ist, angewandt werden. Bedeutungslosigkeit kann allerdings nicht angenommen werden, wenn eine Angelegenheit unter irgendeinem Gesichtspunkt aus irgendeinem Grund jetzt oder auch später Bedeutung gewinnen (vgl. BGHSt 46, 339, 341 m. w. N.), insbesondere ihre Offenbarung auf ein laufendes oder zukünftiges Verfahren Einfluß haben kann (Zängl in GKÖD Bd. I BR Lfg. 5/99 § 61 Rdn. 45).

bb) Auf dieser rechtlichen Grundlage ergibt sich für die dem Angeklagten zur Last gelegten Handlungen, daß er durchaus Geheimnisse im Sinne von § 353b Abs. 1 StGB offenbarte, indem er als Sächsischer Datenschutzbeauftragter anläßlich der ersten Pressekonferenz am Abend des 22. August 2000 die innerdienstlichen Vermerke und Verfügungen des Sächsischen Justizministers vom 19. und 30. August 1997 zu den Vorgängen im Fall Neumer verlas und damit einem größeren Personenkreis bekanntmach-

te, der von diesen Vorgängen bis zu diesem Zeitpunkt in dieser konkreten Form noch keine Kenntnis hatte.

Den Charakter als Geheimnis verloren diese Aktenbestandteile auch nicht ohne weiteres allein dadurch, daß der Angeklagte im Rahmen seiner datenschutzrechtlichen Überprüfung Verstöße des Justizministers gegen das Sächsische Datenschutzgesetz festgestellt hatte. Zwar hatte der Justizminister vor dem Hintergrund seiner parteipolitischen Motivation offensichtlich nicht in Ausübung des ihm nach § 146 GVG zustehenden externen Weisungsrechts gegenüber der Staatsanwaltschaft (vgl. Schoreit in KK 4. Aufl. § 146 GVG Rdn. 2; Kleinknecht/Meyer-Goßner, StPO 45. Aufl. GVG § 146 Rdn. 1) gehandelt. Die Anforderung des Berichts über die Strafrechtsabteilung beim Leitenden Oberstaatsanwalt in Görlitz hinsichtlich der Einzelheiten des Verfahrens gegen Neumer stellt das Erheben personenbezogener Daten im Sinne von § 3 Abs. 2 Nr. 1 SächsDSG dar; eine zweckbestimmte Auswertung dieser Daten oder auch nur eine zielgerichtete Kenntnisnahme von ihnen ist eine Nutzung nach § 3 Abs. 2 Satz 2 Nr. 6 SächsDSG (OVG Bautzen NJW 1999, 2832, 2835) und die Unterrichtung Dritter ein Übermitteln im Sinne von § 3 Abs. 2 Nr. 4 lit. a SächsDSG. Diese Datenverarbeitungen waren nach § 4 Abs. 1 SächsDSG unzulässig. Weder das Sächsische Datenschutzgesetz noch andere Rechtsvorschriften lassen ein solches Vorgehen zu. Auch eine Einwilligung der Betroffenen ist nicht ersichtlich. Die Verschwiegenheitspflicht schützt nicht nur die Betroffenen, sondern auch die zu kontrollierenden öffentlichen Stellen und deren Mitarbeiter (Gola/Schomerus, BDSG 7. Aufl. § 23 Rdn. 10; vgl. auch Dammann in Simitis/Dammann/Geiger/Mallmann/ Walz, BDSG 4. Aufl. § 23 Rdn. 25). Der vorliegende Fall nötigt den Senat nicht, näher zu bestimmen, unter welchen Voraussetzungen die Offenbarung rechtswidrigen Verhaltens die Verschwiegenheitspflicht verletzen kann.

cc) Gleichermaßen kann dahingestellt bleiben, ob der Angeklagte deshalb von der Verschwiegenheitspflicht entsprechend § 61 Abs. 4 BBG

befreit oder befugt war, die aktenkundigen verwaltungsinternen Vorgänge zu offenbaren, weil er zum Erhalt der freiheitlich-demokratischen Grundordnung handelte (vgl. BVerfGE 28, 191, 202 ff.; BGHSt 20, 342, 365, 367 f.; Träger in LK 10. Aufl. § 353b Rdn. 35; Plog/Wiedener/Lemhöfer, BBG/BeamtenVG § 61 Rdn. 7; Battis, BBG 2. Aufl. § 61 Rdn. 4 f.). Zugleich kann offenbleiben, ob damit – wie der Tatrichter meint – der Angeklagte im Sinne von § 34 StGB gerechtfertigt war. Die vom Landgericht getroffenen Feststellungen tragen diesen Schluß nicht ohne weiteres.

dd) Das Landgericht hat aber im Ergebnis zutreffend eine Gefährdung wichtiger öffentlicher Interessen im Sinne von § 353b Abs. 1 StGB verneint (vgl. BGHSt 46, 339, 343).

Eine konkrete unmittelbare Gefährdung öffentlicher Interessen ist nicht ersichtlich. Auch die Revision stellt nicht in Abrede, daß die Offenbarung der fast drei Jahre zurückliegenden Verstöße des Justizministers gegen das Datenschutzrecht wichtige öffentliche Interessen nicht gefährden konnte. Eine Gefährdung wichtiger öffentlicher Interessen käme allenfalls mittelbar in Betracht, falls durch das Offenbaren der Verfügungen des Justizministers das Vertrauen der Öffentlichkeit in die Integrität des Datenschutzbeauftragten beeinträchtigt wäre. Eine solche mittelbare Gefährdung kann nach der Rechtsprechung des Bundesgerichtshofs ausnahmsweise genügen (vgl. BGH NStZ 2000, 596, 598; vgl. auch Träger in LK 10. Aufl. § 353b Rdn. 26 m. w. N.; Tröndle/Fischer, StGB 51. Aufl. § 353b Rdn. 13a; ablehnend Lenckner/Perron in Schönke/Schröder, StGB 26. Aufl. § 353b Rdn. 9; Hoyer in SK-StGB 41. Lfg. § 353b Rdn. 8; Kuhlen in NK-StGB § 353b Rdn. 22 ff.; Perron JZ 2002, 50, 51 f.; Behm StV 2002, 29, 32 f.). Dazu bedarf es einer Gesamtabwägung im Einzelfall, um dem Merkmal der Gefährdung wichtiger öffentlicher Interessen seinen eigenständigen Bedeutungsgehalt zu erhalten. Dabei müssen Inhalt und Umfang der geheimhaltungsbedürftigen Daten, deren in Aussicht genommene Verwendung und die Person des Amtsträgers Berücksichtigung finden (BGH aaO).

Auf der Grundlage dieser Rechtsprechung, an der der Senat festhält, hat das Landgericht im Ergebnis rechtsfehlerfrei eine Gefährdung öffentlicher Interessen durch den Angeklagten verneint. Ein Amtsträger, der wie der Angeklagte zur Kontrolle der Gesetzestreue eines anderen Amtsträgers berufen ist, kann wichtige öffentliche Interessen nicht durch die Offenbarung eines Gesetzesverstoßes gefährden, wenn er die Öffentlichkeit – wie ersichtlich hier – auch als Verbündeten gewinnen will, um auf ein gesetzmäßiges Verhalten hinzuwirken. Damit verfolgte der Angeklagte selbst ein wichtiges öffentliches Interesse, was einen Verlust des Vertrauens hinsichtlich der Integrität des Datenschutzbeauftragten in der Öffentlichkeit ausschließt. Entgegen der Auffassung der Revision kann ein Verlust des Vertrauens in die Integrität des Justizministeriums keine wichtigen öffentlichen Interessen begründen. Die offenbarten Verfügungen des Justizministers waren offensichtlich rechtmäßig in den Besitz des Angeklagten gelangt. Damit wurden sie Bestandteil eines Verwaltungsvorgangs der vom Angeklagten geleiteten Behörde (vgl. Dammann in Simitis/Dammann/Geiger/Mallmann/Walz, BDSG 4. Aufl. § 23 Rdn. 25) und bildeten ausschließlich deren Geheimnis. Dessen Offenbarung könnte dann auch nur einen Verlust des Vertrauens hinsichtlich der Integrität dieser Behörde bewirken. Die Anerkennung einer weiteren Mittelbarkeit – hier bezogen auf das Justizministerium als Ursprungsbehörde – würde auch die Grenzen dessen, was im Gesetzgebungsverfahren als von der Rechtsprechung ausreichend klar umrissen bezeichnet wurde (vgl. BayObLG NStZ-RR 1999, 299, 300; Träger in LK 10. Aufl. § 353b StGB Rdn. 26), überschreiten und dem Erfordernis der Tatbestandsbestimmtheit zuwiderlaufen (vgl. Tröndle/Fischer, StGB 51. Aufl. § 353b Rdn. 13a).

b) Dieselben Grundsätze gelten auch hinsichtlich des Verlesens der datenschutzrechtlichen Beanstandung am 23. August 2000 (Fall 3 der Anklage). Auch insoweit war die Verschwiegenheitspflicht des Angeklagten aus § 23 Abs. 6 Satz 1 SächsDSG nicht schon wegen Bedeutungslosigkeit entfallen. Jedenfalls war insoweit die Offenbarung dieser Geheimnisse aber aus

den oben dargelegten Gründen nicht geeignet, wichtige öffentliche Interessen zu gefährden.

c) Hinsichtlich der Übersendung der datenschutzrechtlichen Beanstandung an Lechner (Fall 2 der Anklage) bestand für den Angeklagten insoweit schon keine Verschwiegenheitspflicht mehr, weil die ihren spezifischen Zweck erfüllende Unterrichtung zu den Mitteilungen im dienstlichen Verkehr im Sinne von § 23 Abs. 6 Satz 2 SächsDSG zu rechnen ist (vgl. Dammann in Simitis/Dammann/Geiger/Mallmann/Walz, BDSG 4. Aufl. § 23 Rdn. 26). Nach Abschluß des Kontrollverfahrens mit der datenschutzrechtlichen Beanstandung erlangte Lechner, der den Angeklagten entsprechend § 22 SächsDSG angerufen hatte, – wie ein Petent – einen Anspruch auf Bescheidung seiner Eingabe (vgl. BayVGH NJW 1989, 2643; Dammann aaO § 21 Rdn. 18). Zwar ist eine ins einzelne gehende Begründung nicht vorgeschrieben (Dammann aaO). Stellt der Datenschutzbeauftragte aber eine Rechtsverletzung fest, muß er angeben, welches Recht er durch welchen Vorgang verletzt sieht (Dammann aaO). Erfolgt eine datenschutzrechtliche Beanstandung, ist der Anrufende auch davon zu unterrichten (Dammann aaO). Diese aus dem Wesen des Anrufungsrechts entwickelten – allgemein praktizierten – Maßstäbe haben durch die die Informationsrechte des Bürgers betonende Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl EG Nr. L 281/31 vom 23. November 1995) und deren Umsetzung im Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001 (BGBl I 904) eine neue Qualität gefunden. Die in Art. 28 III. dritter Spiegelstrich der Richtlinie vorgesehene Anzeigebefugnis des Datenschutzbeauftragten wurde um die ausdrückliche Befugnis in § 23 Abs. 5 Satz 7 BDSG ergänzt, den Betroffenen über den Datenschutzverstoß zu informieren (vgl. BT Drucks. 14/4329, S. 1, 41). Der Angeklagte hat sich bei der Unterrichtung Lechners an diese Erfordernisse gehalten und die Grenzen seiner Befugnis nicht überschritten. Zwar war die Wiedergabe der

Verfügungen des Justizministers im Wortlaut nicht geboten. Dies führte aber nicht zu einer Offenbarung weiterer Tatsachen, weil nichts mitgeteilt wurde, was nicht inhaltsgleich mit eigenen Worten hätte umschrieben werden können.

Harms Häger Raum

Brause Schaal

Ausgefertigt

Reimann
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

16.2.2 Auszug aus dem Volkszählungsurteil

ENTSCHEIDUNGEN
DES
BUNDESVERFASSUNGSGERICHTS

Herausgegeben
von den
Mitgliedern des Bundesverfassungsgerichts

65. Band

1984

J. C. B. MOHR (PAUL SIEBECK) TÜBINGEN

in Verbindung mit § 5 Nr. 1 des Volkszählungsgesetzes vom 14. April 1969 (BGBl. I S. 292) vorgesehen. Bei dieser Sachlage war der Bund befugt, die Erhebung der Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft gesetzlich anzuordnen.

2. Durch die Vorschriften des Volkszählungsgesetzes 1983 wird auch nicht gegen das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) verstoßen.

Dieses Grundrecht ist nicht – wie einige Beschwerdeführer meinen – deshalb verletzt, weil sie nach § 3 Abs. 2 in Verbindung mit § 5 Abs. 1 Nr. 3 VZG 1983 gezwungen sind, ihre privaten Wohnverhältnisse offenzulegen. Wohnung im Sinne des Art. 13 GG ist allein die räumliche Privatsphäre (BVerfGE 32, 54 [72]). Das Grundrecht normiert für die öffentliche Gewalt ein grundsätzliches Verbot des Eindringens in die Wohnung oder des Verweilens darin gegen den Willen des Wohnungsinhabers. Dazu gehören etwa der Einbau von Abhörgeräten und ihre Benutzung in der Wohnung, nicht aber Erhebungen und die Einholung von Auskünften, die ohne Eindringen oder Verweilen in der Wohnung vorgenommen werden können. Sie werden von Art. 13 GG nicht erfaßt. Die nach § 4 Abs. 2 in Verbindung mit § 5 Abs. 1 Nr. 3 VZG 1983 vorgeschriebene Auskunftspflicht über wohnungsstatistische Fragen ist mit einem zwangsweisen Eindringen oder Verweilen in der Wohnung der Auskunftspflichtigen nicht verbunden.

3. Die Verpflichtung zur Auskunft zu bestimmten, in den §§ 2 bis 4 VZG 1983 im einzelnen aufgeführten Sachverhalten verstößt auch nicht gegen das Grundrecht auf Meinungsäußerungsfreiheit (Art. 5 Abs. 1 Satz 1 GG).

Der Auffassung, die durch Art. 5 Abs. 1 GG gewährleistete Freiheit, seine Meinung nicht zu äußern (negative Meinungsäußerungsfreiheit), schütze auch gegenüber der Ermittlung, Speicherung und Weitergabe von Tatsachen, so daß der grundrechtliche Schutz vor Informationseingriffen ausschließlich durch Art. 5 Abs. 1 Satz 1 GG gewährleistet werde, kann nicht gefolgt wer-

den. Ein solcher Schutz würde von vornherein bei Informationseingriffen durch Datenerhebungen versagen, die bei Dritten oder durch heimliche Beobachtungen (Observationen) vorgenommen werden. An einer Meinungsäußerung fehlt es aber auch, wenn der Betroffene selbst Angaben zu einer statistischen Erhebung macht.

Konstitutiv für die Bestimmung dessen, was als Äußerung einer „Meinung" vom Schutz des Grundrechts umfaßt wird, ist das Element der Stellungnahme, des Dafürhaltens, des Meinens im Rahmen einer geistigen Auseinandersetzung; auf den Wert, die Richtigkeit, die Vernünftigkeit der Äußerung kommt es nicht an. Die Mitteilung einer Tatsache ist im strengen Sinne keine Äußerung einer „Meinung", weil ihr jenes Element fehlt. Durch das Grundrecht der Meinungsäußerungsfreiheit geschützt ist sie nur, soweit sie Voraussetzung der Bildung von Meinungen ist, welche Art. 5 Abs. 1 GG in seiner Gesamtheit gewährleistet (BVerfGE 61, 1 [8 f.]). Demgegenüber sind Angaben im Rahmen statistischer Erhebungen wie denen des Volkszählungsgesetzes 1983 reine Tatsachenmitteilungen, die mit Meinungsbildung nichts zu tun haben.

II.

Prüfungsmaßstab ist in erster Linie das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht.

1. a) Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient – neben speziellen Freiheitsverbürgungen – das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann (vgl. BVerfGE 54, 148 [153]). Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschließend. Es umfaßt – wie bereits in der

Entscheidung BVerfGE 54, 148 [155] unter Fortführung früherer Entscheidungen (BVerfGE 27, 1 [6] – Mikrozensus; 27, 344 [350 f.] – Scheidungsakten; 32, 373 [379] – Arztkartei; 35, 202 [220] – Lebach; 44, 353 [372 f.] – Suchtkrankenberatungsstelle) angedeutet worden ist – auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (vgl. ferner BVerfGE 56, 37 [41 ff.] – Selbstbezichtigung; 63, 131 [142 f.] – Gegendarstellung).

Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsicht- und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.

Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung

tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

b) Dieses Recht auf „informationelle Selbstbestimmung" ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über

„seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden (BVerfGE 4, 7 [15]; 8, 274 [329]; 27, 1 [7]; 27, 344 [351 f.]; 33, 303 [334]; 50, 290 [353]; 56, 37 [49]). Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.

Diese Beschränkungen bedürfen nach Art. 2 Abs. 1 GG – wie in § 6 Abs. 1 des Bundesstatistikgesetzes auch zutreffend anerkannt worden ist – einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfGE 45, 400 [420] m. w. N.). Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Dieser mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerläßlich ist (BVerfGE 19, 342 [348]; st. Rspr.). Angesichts der bereits dargelegten Gefährdungen durch die Nutzung der automatischen Datenverarbeitung hat der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken (vgl. BVerfGE 53, 30 [65]; 63, 131 [143]).

2. Die Verfassungsbeschwerden geben keinen Anlaß zur erschöpfenden Erörterung des Rechts auf informationelle Selbst-

bestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses" Datum mehr.

Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten. Dabei ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymisierter Form erhoben und verarbeitet werden (dazu unter a), und solchen, die für statistische Zwecke bestimmt sind (dazu unter b).

a) Schon bislang ist anerkannt, daß die zwangsweise Erhebung personenbezogener Daten nicht unbeschränkt statthaft ist, namentlich dann, wenn solche Daten für den Verwaltungsvollzug (etwa bei der Besteuerung oder der Gewährung von Sozialleistungen) verwendet werden sollen. Insoweit hat der Gesetzgeber bereits verschiedenartige Maßnahmen zum Schutz der Betroffenen vorgesehen, die in die verfassungsrechtlich gebotene Richtung weisen (vgl. beispielsweise die Regelungen in den Datenschutzgesetzen des Bundes und der Länder; §§ 30, 31 der Abgabenordnung – AO –; § 35 des Ersten Buches des Sozialgesetzbuches – SGB I – in Verbindung mit §§ 67 bis 86 SGB X). Wieweit das

Recht auf informationelle Selbstbestimmung und im Zusammenhang damit der Grundsatz der Verhältnismäßigkeit sowie die Pflicht zu verfahrensrechtlichen Vorkehrungen den Gesetzgeber zu diesen Regelungen von Verfassungs wegen zwingen, hängt von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie der Gefahr ihres Mißbrauchs ab (vgl. BVerfGE 49, 89 [142]; 53, 30 [61]). Ein überwiegendes Allgemeininteresse wird regelmäßig überhaupt nur an Daten mit Sozialbezug bestehen unter Ausschluß unzumutbarer intimer Angaben und von Selbstbezichtigungen. Nach dem bisherigen Erkenntnis- und Erfahrungsstand erscheinen vor allem folgende Maßnahmen bedeutsam:

Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.

Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich.

Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.

b) Die Erhebung und Verarbeitung von Daten für statistische Zwecke weisen Besonderheiten auf, die bei der verfassungsrechtlichen Beurteilung nicht außer acht bleiben können.

aa) Die Statistik hat erhebliche Bedeutung für eine staatliche Politik, die den Prinzipien und Richtlinien des Grundgesetzes verpflichtet ist. Wenn die ökonomische und soziale Entwicklung nicht als unabänderliches Schicksal hingenommen, sondern als permanente Aufgabe verstanden werden soll, bedarf es einer umfassenden, kontinuierlichen sowie laufend aktualisierten Information über die wirtschaftlichen, ökologischen und sozialen Zusammenhänge. Erst die Kenntnis der relevanten Daten und die Möglichkeit, die durch sie vermittelten Informationen mit Hilfe der Chancen, die eine automatische Datenverarbeitung bietet, für die Statistik zu nutzen, schafft die für eine am Sozialstaatsprinzip orientierte staatliche Politik unentbehrliche Handlungsgrundlage (vgl. BVerfGE 27, 1 [9]).

Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Es gehört zum Wesen der Statistik, daß die Daten nach ihrer statistischen Aufbereitung für die verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden sollen; demgemäß besteht auch ein Bedürfnis nach Vorratsspeicherung. Das Gebot einer konkreten Zweckumschreibung und das strikte Verbot der Sammlung personenbezogener Daten auf Vorrat kann nur für Datenerhebungen zu nichtstatistischen Zwecken gelten, nicht jedoch bei einer Volkszählung, die eine gesicherte Datenbasis für weitere statistische Untersuchungen ebenso wie für den politischen Planungsprozeß durch eine verläßliche Feststellung der Zahl und der Sozialstruktur der Bevölkerung vermitteln soll. Die Volkszählung muß Mehrzweckerhebung und -verarbeitung, also Datensammlung und -speicherung auf Vorrat sein, wenn der Staat den Entwicklungen der industriellen Gesellschaft nicht unvorbereitet begegnen soll. Auch wären Weitergabe- und Verwertungsverbote für statistisch aufbereitete Daten zweckwidrig.

16.2.3 Muster einer datenschutzgerechten Einwilligung bei Geburtsanzeigen (11/10.1)

Einwilligung zur Weitergabe personenbezogener Daten

Mir ist bekannt, dass personenbezogene Daten durch den Standesbeamten nur an solche Stellen weitergegeben werden dürfen, die in den für ihn geltenden Vorschriften genannt sind. Ich bin aber damit einverstanden, dass

- ☑ die Vor- und Familiennamen des Kindes und der Eltern/eines Elternteiles (nicht zutreffendes bitte streichen)
- ☑ Namen und Anschrift

weitergegeben werden

- ☑ der regionalen Tagespresse
- ☐ den ortsansässigen Banken und Sparkassen
- ☑ Versicherungen
- ☐ Babyausstattern
- ☑ .....(Raum für eigene Wünsche)

Mir ist bekannt, dass die Daten nach der Veröffentlichung auch für Werbezwecke, Meinungsforschung usw. verwendet werden und in Dateien von Firmen, Institutionen o. ä. gespeichert werden.

Mir ist bekannt, dass wir die Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen können.

Ich gebe hiermit meine ausdrückliche Einwilligung im Sinne des § 4 Bundesdatenschutzgesetz (BDSG) in der jetzt gültigen Fassung sowie der entsprechenden landesrechtlichen Bestimmung.

(Unterschrift der Mutter) (Unterschrift des Vaters)