Sächsischer Landtag
3. Wahlperiode

DRUCKSACHE 3/1749

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

8. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 2000

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 4. Juli 2000 Ausgegeben am: 4. Juli 2000

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
01067 Dresden
Telefon: 0351/4935401
Telefax: 0351/4935490

Postfach 12 09 05
01008 Dresden

Besucheranschrift: Devrientstraße 1
01067 Dresden

Vervielfältigung erwünscht.

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

Inhaltsverzeichnis

Abkürzungsverzeichnis

Vorschriften

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der *amtlichen, in Ausnahmefällen auch nichtamtlichen Abkürzung*, ersatzweise der *amtlichen Kurzbezeichnung* aufgeführt.
Die genaue Fundstelle und Angabe der letzten Änderung sind bei bekannteren Bundesgesetzen (die in den gängigen Gesetzessammlungen leicht zu finden sind) weggelassen worden.

AO	Abgabenordnung
ArbschG	Arbeitsschutzgesetz vom 7. August 1996 (BGBl. I S. 1246), zuletzt geändert durch Gesetz vom 16. Dezember 1997 (BGBl. I S. 2970)
ArbZG	Arbeitszeitgesetz vom 6. Juni 1994 (BGBl. I S. 1170)
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BGB	Bürgerliches Gesetzbuch
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) vom 7. Juli 1997 (BGBl. I S. 1650)
BSHG	Bundessozialhilfegesetz in der Fassung der Bekanntmachung vom 23. März 1994 (BGBl. I S. 646, ber. S. 2975), zuletzt geändert durch Art. 2 des Gesetzes vom 22. Dezember 1999 (BGBl. I S. 2671)
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 2 des Gesetzes vom 16. Juni 1998 (BGBl. I S. 1300)
BtMVV	Verordnung über das Verschreiben, die Abgabe und den Nachweis des Verbleibs von Betäubungsmitteln (Betäubungsmittel-Verschreibungsverordnung) vom 20. Januar 1998 (BGBl. I S. 74), zuletzt geändert durch Art. 23 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3853)
BVerfGG	Bundesverfassungsgerichtsgesetz

DRiG	Deutsches Richtergesetz in der Fassung der Bekanntmachung vom 19. April 1972 (BGBl. I S. 713), zuletzt geändert durch Gesetz vom 6. August 1998 (BGBl. I. S. 2026)
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
GWB	Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung der Neufassung vom 26. August 1998 (BGBl. I S. 2521), zuletzt geändert durch Art. 9 des Gesetzes vom 22. Dezember 1999 (BGBl. I S. 2626)
EStG	Einkommensteuergesetz
EU-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (Abl. EG L 281 vom 23. November 1995, S. 31)
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
FPStatG	Gesetz über die Statistik der öffentlichen Finanzen und des Personals im öffentlichen Dienst (Finanz- und Personalstatistikgesetz) in der Fassung der Bekanntmachung zur Neufassung vom 8. März 2000 (BGBl. I S. 206)
GemKVO	Verordnung des SMI über die Kassenführung der Gemeinden des Freistaates Sachsen (Gemeindekassenverordnung) vom 8. Januar 1991, geändert durch Art. 2 der Verordnung zur Änderung des kommunalen Haushalts- und Kassenrechts vom 3. Dezember 1996 (GVBl. S. 498)
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
GO	Geschäftsordnung des Landtages des Freistaates Sachsen in der jeweils geltenden Fassung
GVG	Gerichtsverfassungsgesetz
HGB	Handelsgesetzbuch
KindRG	Gesetz zur Reform des Kindschaftsrechts (Kindschaftsrechts-

	reformgesetz) vom 16. Dezember 1997 (BGBl. I S. 2942); Berichtigung des Gesetzes vom 29. April 1998 (BGBl. I S. 946)
KomPrO	Verordnung des SMI über das kommunale Prüfungswesen (Kommunalprüfungsordnung) vom 14. August 1995 (GVBl. S. 290), zuletzt geändert durch VO vom 13. Januar 1996 (GVBl. S. 65)
PStG	Personenstandsgesetz
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)
SächsBestG	Sächsisches Gesetz über das Friedhofs-, Leichen- und Bestattungswesen (Sächsisches Bestattungsgesetz) vom 8. Juli 1994 (GVBl. S. 1321), zuletzt geändert durch Art. 2 des Gesetzes vom 18. März 1999 (GVBl. S. 85)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 16. Juni 1994 (GVBl. S. 1153), zuletzt geändert durch das 2. Gesetz zur Änderung dienstrechtlicher Vorschriften vom 16. März 1999 (GVBl. S. 121)
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)
SächsGDG	Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen (Sächsisches Gesundheitsdienstgesetz) vom 11. Dezember 1991 (GVBl. S. 413)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 345)
SäHO	Vorläufige Haushaltsordnung des Freistaates Sachsen vom 19. Dezember 1990 (GVBl. S. 213), zuletzt geändert durch Art. 4 des Gesetzes vom 19. Oktober 1998 (GVBl. S. 505)
SächsJG	Sächsisches Justizgesetz (Entwurf)
SächsKAG	Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502), geändert durch Art. 3 des 1. Gesetzes zur Eurobedingten Änderung des sächsischen Landesrechts vom 19. Oktober 1998 (GVBl. S. 505)

SächsKHG	Gesetz zur Neuordnung des Krankenhauswesens (Sächsisches Krankenhausgesetz) vom 19. August 1993 (GVBl. S. 675), zuletzt geändert durch Art. 4 des Gesetzes zur Änderung verschiedener Vorschriften des sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398)
SäKitaG	Gesetz zur Förderung von Kindern in Tageseinrichtungen im Freistaat Sachsen (Gesetz über Kindertageseinrichtungen) in der Fassung vom 24. August 1996 (GVBl. S. 386)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577), zuletzt geändert durch Gesetz vom 20. Februar 1997 (GVBl. S. 105)
SächsMeldDÜVO	Dritte Verordnung des Sächsischen Staatsministeriums des Innern zur Durchführung des Sächsischen Meldegesetzes (Sächsische Meldedaten-Übermittlungsverordnung) vom 10. September 1997 (GVBl. S. 557)
SächsMG	Sächsisches Meldegesetz vom 21. April 1993 (GVBl. S. 353), in der Fassung der Bekanntmachung vom 11. April 1997 (GVBl. S. 377)
SächsPersVG	Sächsisches Personalvertretungsgesetz vom 21. Januar 1993 (GVBl. S. 29), zuletzt geändert durch Art. 3 des Gesetzes vom 29. Juni 1998 (GVBl. S. 271)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (GVBl. S. 466)
SächsRiG	Richtergesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. Februar 1997 (GVBl. S. 121), geändert durch Art. 2 des 2. Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 16. März 1999 (GVBl. S. 117)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453), zuletzt geändert durch Art. 2 des Gesetzes von 12. Februar 1999 (GVBl. S. 49)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVertrG	Gesetz zur Regelung der Vertretung des Freistaates Sachsen in gerichtlichen Verfahren vom 20. Februar 1997 (GVBl. S. 108)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (GVBl. S. 459)

SächsWG	Sächsisches Wassergesetz vom 21. Juli 1998 (GVBl. S. 393), geändert durch Art. 3 des Gesetzes zur Änderung verschiedener Vorschriften des sächsischen Landesrechts vom 25. Juni 1999 (GVBl. S. 398)
SchulG	Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (GVBl. S. 213), zuletzt geändert durch Gesetz vom 29. Juni 1998 (GVBl. S. 271)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes zur Reform der gesetzlichen Rentenversicherung vom 16. Dezember 1997 (BGBl. I S. 2998)
SGB V	Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 9 Nr. 2 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3853)
SGB VI	Sozialgesetzbuch - Gesetzliche Rentenversicherung - vom 18. Dezember 1989 (BGBl. I S. 2261, ber. BGBl. 1990 I S. 1337), zuletzt geändert durch Gesetz vom 24. März 1999 (BGBl. I S. 388)
SGB X	Sozialgesetzbuch - Verwaltungsverfahren - vom 18. August 1980 (BGBl. I S. 1469, ber. S. 2218), zuletzt geändert durch Art. 1 a des Gesetzes vom 6. August 1998 (BGBl. I S. 2022)
SigG	Signaturgesetz
SigV	Signaturverordnung vom 22. Oktober 1997 (BGBl. I S. 2498)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVÄG	Strafverfahrensänderungsgesetz (Entwurf)
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 das Sechste Gesetz zur Reform des Strafrechts vom 26. Januar 1998 (BGBl. I S. 164, 187)
StVG	Straßenverkehrsgesetz

TDDSG	Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG) vom 22. Juli 1997 (BGBl. I S. 1870)
TDSV	Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Telekommunikationsdienstunternehmen-Datenschutzverordnung) vom 12. Juli 1996 (BGBl. I S. 982)
TFG	Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz) vom 1. Juli 1998 (BGBl. I S. 1752)
TierSchG	Tierschutzgesetz in der Fassung der Bekanntmachung vom 25. Mai 1998 (BGBl. I S. 1105, ber. S. 1818)
TKG	Telekommunikationsgesetz vom 25. Juli 1996 (BGBl. I S. 1120)
VwGO	Verwaltungsgerichtsordnung
VwVOrgStA	Verwaltungsvorschrift des SMJus über die Organisation und den Dienstbetrieb der Staatsanwaltschaften (Organisationsstatut der Staatsanwaltschaften) vom 12. Januar 1998 (SächsJMBl. S. 18), zuletzt geändert durch 2. VwV des SMJus zur Änderung des Organisationsstatuts der Staatsanwaltschaften vom 2. Juli 1999 (SächsJMBl. S. 118)
VwVPersAktenB	Verwaltungsvorschriften des SMS über die Führung und Verwaltung von Personalakten der Beamten (Verwaltungsvorschrift Personalakten Beamte) vom 11. Dezember 1998 (SächsABl. vom 14. Januar 1999 S. 10)
VwVfG	Verwaltungsverfahrensgesetz
WoGG	Wohngeldgesetz in der Fassung der Bekanntmachung vom 1. Februar 1993 (BGBl. I S. 183), zuletzt geändert durch Art. 4 und Art. 5 zur Änderung des Wohngeldgesetzes und anderer Gesetze vom 22. Februar 1999 (BGBl. I S. 2671)
ZuschussVO	Verordnung der Sächsischen Staatsregierung über die Gewährung von Zuschüssen für Schulen in freier Trägerschaft vom 16. Dezember 1997 (GVBl. S. 682)

Sonstiges

ÄndVO	Änderungs-Verordnung
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.
AOK	Allgemeine Ortskrankenkasse
ARoV	Amt zur Regelung offener Vermögensfragen
AZR	Ausländerzentralregister
BAGE	Amtliche Sammlung der Entscheidungen des Bundesarbeitsgerichts
BAnz.	Bundesanzeiger
BayObLG	Bayerisches Oberstes Landesgericht
BayVBl.	Bayerische Verwaltungsblätter
BayVGH	Bayerischer Verwaltungsgerichtshof
BfA	Bundesanstalt für Artbeit
BfD	Der Bundesbeauftragte für den Datenschutz
BFH	Bundesfinanzhof
BND	Bundesnachrichtendienst
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BHW	Beamtenheimstättenwerk
BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse
BMF	Bundesministerium der Finanzen

BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BML	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BMWi	Bundesministerium für Wirtschaft und Technologie
BRD	Bundesrepublik Deutschland
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
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts
BVS	Bundesanstalt für vereinigungsbedingte Sonderaufgaben (bis 31. Dezember 1994: THA)
BZR	Bundeszentralregister
CD-ROM	Compact disc-read only memory
CR	Computer und Recht [Zeitschrift; früher auch „CuR“]
DSMeld	Datensatz für das Meldewesen
DVBl	Deutsches Verwaltungsblatt
DVO	Durchführungsverordnung
ed-	erkennungsdienstlich

EG	Europäische Gemeinschaft
EGN	Einzelgesprächsnachweis
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
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
GMBl.	Gemeinsames Ministerialblatt, hrsg. vom Bundesministerium des Innern
GVBl.	Sächsisches Gesetz- und Verordnungsblatt
HIV	human immunodeficieny virus (Aidserreger)
IKK	Innungskrankenkasse
INPOL	Polizeiliches Informationssystem des Bundes und der Länder
IM	Inoffizieller Mitarbeiter (des MfS/AfNS)
ISD	Internationaler Suchdienst Arolsen
ISDN	Integrated services digital network
JVA	Justizvollzugsanstalt
KANN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt in Flensburg
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
LPDK	Lehrpersonaldatenbank
LRA	Landratsamt
LUA	Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen
LÜVA	Lebensmittelüberwachungs- und Veterinäramt
LVA	Landesversicherungsanstalt
MDR	Mitteldeutscher Rundfunk
MedR	Medizinrecht (Zeitschrift)
MfS	Ministerium für Staatssicherheit
MPU-Stelle	Medizinisch-Psychologische Untersuchungsstelle
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
ÖbV	Öffentlich bestellter Vermessungsingenieur
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PersR	Zeitschrift Personalvertretungsrecht
PIN	Personal identification number (Persönliche Identifikationsnummer)

PKZ	Personenkennzahl
PersV	Die Personalvertretung (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RG	Reichsgericht
RGBl.	Reichsgesetzblatt
RP	Regierungspräsidium
RPA	Rechnungsprüfungsamt
SächsABl.	Sächsisches Amtsblatt
SächsJMBl.	Sächsisches Justizministerialblatt
SächsOVG	Sächsisches Oberverwaltungsgericht
SAKD	Sächsische Anstalt für Kommunale Datenverarbeitung
SLFS	Sächsisches Landesamt für Familie und Soziales
SächsVerfGH	Verfassungsgerichtshof des Freistaates Sachsen
SK	Sächsische Staatskanzlei
SLT	Sächsischer Landkreistag e. V.
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, Gesundheit, Jugend und Familie
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
StUFA	Staatliches Umweltfachamt
TB	Tätigkeitsbericht
TCP/IP	Transmission control protocol/Internet protocol
TdL	Tarifgemeinschaft deutscher Länder
THA	Treuhandanstalt
TK-Anlage	Telekommunikationsanlage
TÜ	Telefonüberwachung
TÜV	Technischer Überwachungsverein
VG	Verwaltungsgericht
VIZ	Zeitschrift für Vermögens- und Investitionsrecht
VO	Verordnung
VwV	Verwaltungsvorschift
VZR	Verkehrszentralregister
WWW	World wide web

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

Der vorliegende 8. Tätigkeitsbericht hat zwei Schwerpunkte: Zum einen haben wir datenschutzrechtliche Fehler im Bereich der Personaldatenverarbeitung und des Berichtswesens der Justizverwaltung zu kritisieren, zum anderen haben wir in mehreren - ich denke fundierten - Darstellungen die rechtliche Komplexität der Datenverarbeitung in der Sozialverwaltung an konkreten Beispielen beschrieben.

Natürlich wird der Staatsminister der Justiz die Dinge ganz anders sehen. Er wird - das ist kein neues Argument - einwenden, drei Personal-Grundakten pro Richter und Staatsanwalt seien üblich, und die angeforderten Berichte über „öffentlichkeitswirksame“ Ermittlungsverfahren und über die Terminierungspraxis einzelner Richter beruhten auf hundertjähriger Tradition in Deutschland. Es sei auch nicht Aufgabe des Datenschutzbeauftragten, sich um die Unabhängigkeit der Justiz zu sorgen, die „selbstverständlich“ gewährleistet sei. Nur: Die behaupteten Traditionen bestehen - wenn so überhaupt - nur da und dort; sie sind für sich genommen auch kein Ersatz für die notwendige Rechtsgrundlage der Datenverarbeitung. Und die Unabhängigkeit der Justiz ist eine verfassungsrechtlich gebotene Schranke für die Datenverarbeitung, die der Justizminister als Teil der Exekutive strikt zu beachten hat. Unsere vielfältigen dienstlichen Kontakte mit Richtern und Staatsanwälten, die Eingriffe in ihre Unabhängigkeit durch Berichtspflichten bitter beklagen, machen uns Mut, den Finger in die Wunde zu legen. Denn die Datenverarbeitung ist ein feiner Indikator für eine grundlegende Fehlhaltung. Mitarbeiterdaten und konkrete Verfahrensinhalte sollten - schon wegen der vorbildlichen Funktion der Justizverwaltung im jungen Rechtsstaat - streng auf dem Boden der Rechtsordnung gehalten und nicht in politische Sphären gehoben werden. Dort gehören sie nicht hin.

Dagegen - so hoffe ich - teilt das SMS unsere Bemühungen um Klarheit in den manchmal hoffnungslos komplizierten Regelwerken der Datenverarbeitung im Sozialstaat, so z. B. bei der Frage, wie man eine datenschutzgerechte Qualitätssicherung bei der Behandlung von Zuckerkranken in ärztlicher Selbstverwaltung organisieren kann, ohne den dies finanzierenden Krankenkassen Patientendaten zugänglich zu machen.

Diesen Bericht verdanke ich - wie immer - dem Fleiß und dem Sachverstand meiner Mitarbeiter sowie der Betreuung und Versorgung durch die Bediensteten der Landtagsverwaltung. Herrn Landtagspräsident Erich Iltgen sowie dem Präsidium des Landtags danke ich besonders für die Entscheidung, meine Behörde in unmittelbarer Nähe des Landtags unterzubringen. Unsere vielfältigen täglichen Kontakte zur Verwaltung, zu den Fraktionen, den Ausschüssen und zu den einzelnen Abgeordneten sind dadurch gesichert.

1.1 Das Internet und die „Wissensgesellschaft“

Die Staatsregierung strebt an, grundsätzlich jedem Mitarbeiter und jedem interessierten Bürger einen Internet-Anschluss zu ermöglichen. Schulen fragen an, ob nicht

doch jedem Schüler eine E-Mail-Adresse zugeteilt werden solle. Die Kommunikation des Bürgers mit der Verwaltung soll in vielen Bereichen offen oder verschlüsselt über das Netz gehen. Regierungspräsidien denken über papierfreie, also netzgebundene Verwaltung nach.

Grundsätzlich stellt sich die Frage, ob die Verwaltung, die unter dem rechtsstaatlichen Gebot der Gesetzmäßigkeit steht, ihr personenbezogenes Wissen aus dem Internet schöpfen oder gar solche Informationen ins Internet stellen darf. Darf die Verwaltung intern oder extern über E-Mail im offenen Netz kommunizieren?

Jeder Politiker, der etwas auf sich hält, will uns in das gelobte Land der „Wissensgesellschaft“ führen. Dieser Begriff, der uns auch als „globale Wissensgesellschaft“ schmackhaft gemacht wird, gilt als das Markenzeichen programmatischer Aufrüstung für das begonnene Jahrtausend. Das „Informationszeitalter“ wird bemüht, jede Verwaltung will an der „globalen Vernetzung“ teilnehmen. Unsere Schulen sollen „ans Netz“. So wie sich die Schüler über die Fernsehserien austauschen, die gerade en vogue sind - so geht es den Internet-Begeisterten häufig darum mitzuteilen, dass man mitweiß. Das Wissensgut degradiert sich zum Mitwissertum, es geht geradezu um den olympischen Gedanken: Dabeiwissen ist alles.

In der Epoche der Multimedia-Maschinen und des Internets gilt bei vielen nur noch das Netz als tragfähige Kommunikationsbasis, es ist der gemeinsame Erfahrungsraum einer Massengesellschaft, die nicht mehr das persönliche Gespräch oder das öffentliche Ansehen von Meinungsführern, sondern die E-Mail (und die Mitwisser, den „Verteiler“ der E-Mail) braucht, um so etwas wie einen „breiten Konsens“ herbeizuführen. Wehe dem, der da nicht mitspielt, nicht mitmailt und nicht mitweiß!

Aber das Internet-Wissen ist Allgemeingut, es ist jedermann zugänglich. Wissensvorsprünge werden damit grundsätzlich unmöglich. Herrschaftswissen verliert im Netz seine Kraft - aber auch seine Bedrohlichkeit. Das Netz dezentralisiert und ebnet Hierarchien ein. So gesehen kann sogar das Internet die Demokratie sichern.

Mit dieser Art der Veröffentlichung von Wissen sind nicht nur Gefahren für die Authentizität und die Fälschungssicherheit verbunden; vor allem geht jede Vertraulichkeit verloren. Das Internet ist nicht mehr als ein großes, weltweites Lexikon. Es ist aber auch nicht weniger: Natürlich ist es faszinierend, das gesamte auf Datenträgern digitalisiert gespeicherte und zur freien Verfügung veröffentlichte Wissen der Welt abrufen zu können. In vielen Bereichen - denken wir an die Wissenschaften, an die Medizin in Theorie und Praxis, an Kunst und Kultur, aber auch an so profane Dinge wie Aktienkurse und Fahrpläne - grenzt es ans Wunderbare, sofort in den Stand neuester Erkenntnisse zu kommen. Die Digitalisierung verleiht uns Flügel - Wissen macht glücklich, behauptet Nicholas Negroponte („Total digital“, New York 1995).

Larmoyanz oder Kulturpessimismus sind nicht angezeigt, denn der Vorteil, den uns die Technik eröffnet, ist sicher groß. Aber dem stehen viele mit erheblichen Reserven gegenüber: Medientheoretiker und Kulturkritiker versichern uns, dass wir in einer

Zeit „progressiver Verblödung“ leben würden, denn in Wahrheit stehe die Kunst des Umgangs mit dem Nichtwissen im Vordergrund: Es gehe darum, zu wissen, was man nicht weiß. Wir sollten uns bemühen zu wissen, was wir nicht wissen können, und, was wir nicht wissen wollen: Denn Informationsüberflutung führe tendenziell zu totaler Unwissenheit. Wir informieren uns zu Tode, sagt Neil Postman („Die zweite Aufklärung“, Berlin 1999).

Es lohnt sich also, darüber nachzudenken, ob Wissen aus dem Internet tatsächlich eine wesentliche Erkenntnisquelle der Verwaltung ist, ob prägende Kommunikation tatsächlich per E-Mail erfolgen soll, ob ein „Kapitalismus des Wissens“, ein bloßes Massenwissen oder bloße Wissensmassen die moderne Massengesellschaft prägen sollen oder ob es gilt, dem gegenzusteuern und darüber nachzudenken, ob der Mensch mehr ist als nur ein Mitwisser, ein Wissensspeicher, eine „Festplatte auf zwei Beinen“.

Zu dieser - hochpolitischen und aktuellen - Diskussion möchte ich folgende einfachen und nüchternen Überlegungen beisteuern:

Zunächst: Beide Seiten haben viel für sich - sie bilden ja eigentlich auch keinen Gegensatz.

Kommunikation erschöpft sich nicht im Wissensaustausch, im „Chatten“, oder gar in der bloßen Abfrage des Internets. Wer sich um wirkliches Wissen bemüht, dem geht es letztlich um die Gabe der Unterscheidung der Geister. Das Ziel ist die Bildung geistiger Grundlagen, es geht weniger um Wissen als um Erkenntnis, besser: es geht um Erkenntnis durch Wissen. Wer nichts weiß, kann auch keine Idee von den Dingen, keine Zukunft entwickeln. Ungeformtes, unbeurteiltes Wissen ist etwas Unterschiedsloses, das keine Qualität besitzt, das insbesondere die Würde des Menschen weder erhält noch vermehrt. Deshalb muss man zwischen Wissen und Werten unterscheiden. Das, was das Internet bietet, muss an einer sittlichen Werteordnung - in unserer säkularisierten Gesellschaft sind dies das Grundgesetz und die Sächsische Verfassung - gemessen werden. Wissen, das nicht der Wahrheit und der Freiheit verpflichtet ist, degeneriert in die Beliebigkeit. Es eröffnet menschlichen Kategorien keine Zukunft.

Aber eine gute Gesellschaft, eine leistungsfähige Verwaltung, eine gerechte Regierung muss auch viel wissen. Nach der Verfassung muss dieses Wissen im Rechtsstaat aber auf gesetzliche Zweckbindung begrenzt und nach dem Grundsatz der Verhältnismäßigkeit auf das geeignete und erforderliche Maß beschränkt werden.

Es gibt weite Räume in der Kommunikation, die nicht dem Wissensaustausch dienen, in denen kein Wissen angehäuft und umgeschichtet wird. Ein Blick, ein Gesicht, eine Stimme, eine Haltung, ein Schweigen sagen mehr als viele E-Mails. Es wird auch künftig mehr und mehr der persönliche Austausch von Meinung und Überzeugung, von Haltung und gegenseitigem Respekt gefragt sein. Kommunikation ohne personale Elemente vermittelt allenfalls ein Wissensgerippe, eben Wissen ohne Fleisch und Blut. Wer auf die Anhäufung von Wissen setzt, wird sehr bald merken,

dass er an der Individualität, an den Impulsen, die den Einzelnen beflügeln und die die Wirklichkeit bilden, scheitert. Anders gesagt: Wirklichkeit ist mehr als Wissen.

Und Behörden, die alles von Mitarbeitern und Bürgern wissen wollen, scheitern sehr schnell an der datenschutzrechtlichen Maxime: Ist die Information, die da erhoben werden soll, wirklich geeignet und erforderlich, um einen konkreten Fall, der zur gesetzlichen Zuständigkeit gehört, mit den gesetzlichen Befugnissen und nach geltendem Recht zu entscheiden?

Seit altersher stehen die beiden Weisheiten diametral gegenüber: Sokrates sagt: „Ich weiß, dass ich nichts weiß“, während Fausts Wagner erstrebt: „Zwar weiß ich viel, doch möcht ich alles wissen!“ (Faust wird daraufhin übrigens ganz aktuell: „Wie nur dem Kopf nicht alle Hoffnung schwindet, der immerfort an schalem Zeuge klebt, mit gier’ger Hand nach Schätzen gräbt, und froh ist, wenn er Regenwürmer findet!“) Wer da weiter denkt, der wird zu einer „Kultur des Nichtwissens“ raten müssen. Damit sind wir beim Thema: Ist die Verwaltung als Teil dieser Gesellschaft wirklich darauf aus, Massenwissen anzuhäufen oder geht es nicht vielmehr darum, abzuschichten, genau zu prüfen, ob Informationen über Menschen geeignet und erforderlich sind, ob sie in zumutbarer Weise zu gesetzlichen Zwecken verarbeitet werden. Anders gesagt: Die Wissensbegrenzung des Staates ist das Problem. Der Datenschutz ist nichts anderes als die Lehre von der Wissensbegrenzung der Verwaltung, jedenfalls dann, wenn es um Wissen über einzelne Menschen geht. Mehr als früher ist zu beachten: Das natürliche Gefühl der Menschen für Datenschutz bremst die hochfliegenden Pläne von Wirtschaft und Verwaltung. Viele stehen ehrgeizigen und wohlfeilen Wünschen zur multimedialen Verwaltung mit kritischer Distanz gegenüber.

Ich erwarte von denen, die diese Gesellschaft politisch prägen, dass sie deutlicher als bisher vor den Gefahren ungebremster, undifferenzierter Wissensansammlungen warnen und dass Kultur, Bildung und Erziehung mehr als in letzter Zeit deutlich werden lassen, worum es geht: Wissensvermittlung ist das eine - sparsamer und haushälterischer Umgang mit Wissen das andere. Nur wenn zum Wissen eine Wertehierarchie hinzutritt, entgehen wir einem Materialismus/Kapitalismus des Wissens, der die Verwaltung zur massenkommunikativen Verzettelung führt und sie aufbläht. Oder: Konzentration auf das notwendige Wissen ist die Kunst jeder Behörde. Die Gesetzmäßigkeit prägt die Verwaltung, nicht die Allwissenheit.

Als Beispiel für eine Wertbindung sei der Umgang mit Daten in der Schule erwähnt: Die Sächsische Verfassung definiert in Art. 101 den Auftrag des staatlichen Bildungswesens wie folgt: „*Die Jugend ist zur Ehrfurcht vor allem Lebendigen, zur Nächstenliebe, zum Frieden und zur Erhaltung der Umwelt, zur Heimatliebe, zu sittlichem und politischem Verantwortungsbewußtsein, zu Gerechtigkeit und zur Achtung vor der Überzeugung des anderen, zu beruflichem Können, zu sozialem Handeln und zu freiheitlicher demokratischer Haltung zu erziehen*.“ Diesem Erziehungs- und Bildungsauftrag hat auch die Internet-Nutzung, hat jede Kommunikations-Ausbildung zu dienen. Es ist zwar dringend nötig, den Schülern das Handwerk des Umgangs mit PC, Netzen und Systemen, die theoretische und praktische Fertigkeit zur Nutzung der gängigen Hard- und Software beizubringen. Dies aber nicht als Ergebnis oder als

Bildungsziel, sondern als bloßes Werkzeug zur Wissenserschließung, als Krücke auf dem Weg zur wirklichen Bildung.

Über die Beherrschung der Zugangstechnik hinaus ist selbständiges Denken, ist Filtern, Abschichten, Ordnen von Wissen, sind eigenständige, ganz persönliche Gedanken gefragt: Kopieren oder Studieren? Wie kann man im Wissenswust des Internet die Spreu vom Weizen trennen? Wie kann man Wesentliches von Unwesentlichem, Wahres von Verfälschtem unterscheiden? Urteilsvermögen, Argumentationskunst, methodische Durchdringung, Definitionskraft vernünftiger Bildungsgegenstände und Ideale, sogar Illusionen und Träume müssen vermittelt werden. Das ist die neue und schwierige Aufgabe, die die künftige Gesellschaft intensiv beschäftigen sollte.

Autoritäten können nicht über das Internet erkannt und freiheitlich akzeptiert werden. Der Jahrmarkt, das Panoptikum der Allinteressantheiten lenkt ab, öffnet spontan neue Dimensionen der Vergnügung und erfüllt angeblich jeden Wissenswunsch. Das macht aber nicht glücklich, macht nicht klüger, macht auch die Verwaltung nicht sachgerechter und nicht rechtmäßiger.

So reduziert sich der Traum von der Wissensgesellschaft im rechtsstaatlichen Alltag auf die technische Möglichkeit, Fachwissen zu erschließen, Informationen gezielt abzurufen und damit zentralisierte Erkenntnisse zu dezentralisieren. Der damit verbundene gesamtgesellschaftliche Gewinn an allgemeinen Erkenntnissen ist zwar groß. Er ersetzt aber nicht die Initiative, die Risikofreude, das persönliche Engagement und das Urteilsvermögen des Einzelnen. Das gilt für die Verwaltung ebenso wie für Bildungseinrichtungen. Der Erziehungs- und Bildungsauftrag der Schulen hat sich ebenso wenig geändert wie die Verhältnismäßigkeitsbindung der Verwaltung. Das Netz der Netze ist für sie nicht mehr als ein - zurückhaltend zu nutzendes - Werkzeug, ein Hilfsmittel, um die gesetzlichen Aufträge zu erfüllen.

Ich bin zuversichtlich, dass ähnliche Überlegungen in der sächsischen Verwaltung entwickelt werden und das Internet mit der gebotenen Vorsicht - eben kritisch - genutzt wird.

Für die Zukunft rechne ich mit folgender Entwicklung:
Wenn - hoffentlich bald - Verschlüsselungstechnik und digitale Signatur eine bilaterale, eben nicht mehr nur öffentliche, sondern diskrete und geschützte Kommunikation ermöglichen, entsteht grundsätzlich eine neue Situation: Dann bietet das Netz eine individualisierte Transportfunktion neben der heutigen Veröffentlichungsfunktion. Das wird zu einer exponentiell steigenden individuellen Nutzung des Netzes führen, in der Herrschaftswissen in Entwicklung, Planung, Handel, Politik, Verwaltung und im wirklichen Privatbereich übermittelt wird. Unbeobachtete und vertrauliche Kommunikation wird zur weltweiten Zusammenarbeit gleichgesinnter und gleichberechtigter Partner und Organisationen einladen. Dies führt zu einer völlig neuen Dimension, nämlich zu ständig präsentem Herrschaftswissen. Und es führt zur Entwicklung und Abschottung tausender Netze im Netz, eben zur selektiven, persönlichen Kommunikation vieler Einzelner miteinander.

Es ist meine Aufgabe, diese Entwicklung zu beobachten und zu begleiten. Gern berate ich die sächsischen Behörden, die das Internet dann (aber bitte: erst dann) auch zur Bearbeitung einzelner Bürgeranliegen und individueller Verwaltungsvorgänge nutzen wollen.

1.2 Der Vollständigkeit halber ...

Dieser Tätigkeitsbericht, den ich dem Sächsischen Landtag vorzulegen habe, betrifft den Zeitraum vom 1. April 1999 bis zum 31. März 2000. Ich muss deshalb, allerdings nur so kurz wie möglich, auf den Schluss des datenschutzrechtlich herausragenden 3. Untersuchungsausschusses des Sächsischen Landtages eingehen: Mit Schreiben vom 1. Juli 1999 teilte Herr Staatsminister Meyer mir zum entscheidenden Streitpunkt endlich Folgendes mit:

„*Sehr geehrter Herr Dr. Giesen,*
in meiner Anhörung vor dem 3. Untersuchungsausschuss des Sächsischen Landtages ist mir bewusst geworden, dass mein an Sie gerichtetes Schreiben vom 10. August vergangenen Jahres eine falsche Datumsangabe enthält. Ich bedaure diese Tatsache zutiefst. Sie ist mir um so unverständlicher, als nur wenige Tage zuvor in einem Briefwechsel mit Herrn Gauck der Termin 09. Februar für die Akteneinsicht ausdrücklich bestätigt wurde.

Der Fehler kam zustande, da der für diese Angelegenheit in meinem Hause zuständige Bearbeiter seit Anfang August im Urlaub war und sein Vertreter den Sachverhalt offenbar nicht genau kannte.

Ich bitte Sie, diese Unkorrektheit zu entschuldigen. Den Briefwechsel mit Herrn Gauck füge ich bei.

Ich erlaube mir, eine Kopie dieses Schreibens dem 3. Untersuchungsausschuss im Sächsischen Landtag zukommen zu lassen.

Mit freundlichen Grüßen
Prof. Dr. Hans Joachim Meyer“

Ich konnte diese Entschuldigung aus mehreren sachlichen Gründen nicht akzeptieren, die ich dem Ausschuss am 3. August in einem Sonderbericht mitgeteilt habe, auf den ich hiermit verweise.

Dennoch ist die Angelegenheit aus meiner Sicht erledigt: Es war mir nicht möglich, die Petentin in ihrem Recht auf informationelle Selbstbestimmung zu schützen, weil der - in der Tat gravierende - Rechtsverstoß des SMWK bereits geschehen war, als ich von der Sache erfuhr. Ich habe keine rechtliche Möglichkeit, eine öffentliche Stelle zur Wiedergutmachung oder Rehabilitation zu zwingen. Soweit ich den Sächsischen Landtag bei der Ausübung seiner parlamentarischen Kontrolle unterstütze, wurde das,

was notwendig war, getan: Aufgrund meiner Kontrollen und Eingaben wurde ein Untersuchungsausschuss eingesetzt, der zwar ein gemeinsames Votum nicht abgegeben hat, aber seine Arbeit ordnungsgemäß - auch im Hinblick auf das Ende der Legislaturperiode - beendet hat. Es ist nicht meine Aufgabe, Konsequenzen zu fordern oder gar durchzusetzen. Es ist aber zu hoffen, dass sich ein Missbrauch von Stasi-Unterlagen in Sachsen auf höchster Ebene nicht wiederholen wird. Bedauerlich ist, dass Stasi-Unterlagen im SMWK nach wie vor von einem Vertrauten des Staatsministers außerhalb der zuständigen Verwaltungshierarchie verarbeitet werden.

1.3 Heimliche Dienstaufsicht

Ein leitender Mitarbeiter einer bedeutenden sächsischen Behörde, der dort eine eigenständige öffentliche Stelle leitet, bat mich um Beratung zu einer konkreten datenschutzrechtlichen Problematik, mit der seine Behörde sich auseinander zu setzen hat. Wegen der Bedeutung der mehrere Ressorts und kommunalen Stellen berührenden Thematik lud mein zuständiger Referatsleiter daraufhin zu einer gemeinsamen Besprechung ein, an der unter anderem neben dem leitenden Mitarbeiter auch ein Vertreter des über ihn dienstaufsichtsführenden Staatsministeriums teilnahm.

Nach einigen Monaten musste ich erfahren, dass gegen den leitenden Mitarbeiter dienstaufsichtliche Maßnahmen erwogen wurden, weil über sein Verhalten in der Besprechung durch den anwesenden Vertreter des dienstaufsichtsführenden Staatsministeriums Informationen notiert und seinem Vorgesetzten übermittelt worden waren.

Angesichts dieses Falles eines eklatanten datenschutzwidrigen Fehlverhaltens aufsichtsführender Stellen fordere ich an dieser Stelle die gesamte Verwaltung des Freistaates Sachsen auf, folgende Grundregeln zu beherzigen:

Die Beratung öffentlicher Stellen gehört zu den gesetzlichen Aufgaben des Sächsischen Datenschutzbeauftragten; deshalb ist jeder Leiter einer öffentlichen Stelle berechtigt - wenn nicht sogar dienstlich verpflichtet -, den Datenschutzbeauftragten auf datenschutzrechtliche Probleme aufmerksam zu machen und ihn um eine dienstliche Beratung zu bitten. Besteht sachlich ein derartiger Beratungsbedarf, so kann eine untergesetzliche Norm - wie immer sie auch aussehen mag - nicht reglementieren oder gar verhindern, dass leitende Mitarbeiter einer öffentliche Stelle sich an den Datenschutzbeauftragten wenden. Verwaltungsvorschriften, Dienstanweisungen etc. zur Einhaltung eines „Dienstweges“ dürfen im Ergebnis nicht dazu führen, dass die gesetzlichen Beratungsrechte und Beratungspflichten dahin modifiziert werden, dass letztendlich die Beratung nur gegenüber den Staatsministerien oder nur mit deren ausdrücklicher Billigung erfolgt. Damit würde das gesetzliche Beratungsgebot sachwidrig verengt, gefiltert oder ausgeschaltet.

Dieses Beratungsgebot korrespondiert mit meinem Kontrollrecht: Wenn es dem Sächsischen Datenschutzbeauftragten schon erlaubt ist, anlassfreie datenschutzrechtliche Kontrollen ohne Einhaltung irgendeines Dienstweges bei öffentlichen Stellen durchzuführen, so muss diesen erst recht gestattet sein, meinen Rat einzuholen, so dass unnötige Kontrollen vermieden oder so vorbereitet werden, dass sie beanstandungsfrei verlaufen.

Jede Datenverarbeitung, die von vornherein darauf abzielt, dass eine aufsichtsführende Stelle Informationen über das Verhalten von Mitarbeitern nachgeordneter Stellen notiert und deren Vorgesetzten übermittelt, verstößt gegen datenschutzrechtliche Grundregeln. Abgesehen davon, dass ein solches Verhalten unkollegial und einer offenen, fairen und produktiven Arbeitsatmosphäre abträglich ist, ist eine solche verdeckte Datenerhebung rechtlich zu beanstanden. Muss ein Bediensteter davon ausgehen, dass der an einer gemeinsamen Besprechung teilnehmende Entsandte der vorgesetzten Dienststelle die Absicht hat, hinter seinem Rücken Verhaltensdaten zu erheben, zu speichern und zu übermitteln, ist eine unbefangene und an der Sache orientierte Teilnahme an einer Besprechung nicht mehr möglich. Das Gesprächsklima ist dann insgesamt vergiftet. Damit wird letztlich nicht dem sachlichen Interesse des Dienstherrn an einer Problemklärung gedient, sondern nur noch eine sachlich unbegründete, dienstlich nicht veranlasste Neugier danach befriedigt, wie sich die eingesetzten Amtswalter verhalten und - meist - ob sie die Linie der Vorgesetzten halten. Auf diese Weise wird die Menschenwürde der Betroffenen verletzt. Die Datenverarbeitung dient in heimlicher Art und Weise der Verhaltens- und Leistungskontrolle; die Datenverarbeitung ist schließlich rechtswidrig, weil eine Rechtsvorschrift diese Art und Weise der Datenverarbeitung nicht zulässt.

Es mag ausnahmsweise vorkommen, dass sich unvorhergesehen während einer Besprechung ein dienstliches Fehlverhalten eines Mitarbeiters offenbart und sich für einen teilnehmenden Kollegen daraus die dienstliche Verpflichtung ergibt, dies zu dokumentieren und dem Vorgesetzten zu übermitteln. Die Überwachung darf jedoch nicht von vornherein beabsichtigt und (einziger) Zweck der Teilnahme sein. Überdies muss der betroffene Mitarbeiter in jedem Fall so früh wie möglich und völlig offen über die Datenspeicherung und -übermittlung informiert und damit über alle Absichten der Datenverarbeitung aufgeklärt werden.

Im eingangs geschilderten Fall hat das Staatsministerium meine Kritik an seinem Fehlverhalten im Ergebnis positiv aufgenommen und von der beabsichtigten Sanktionierung des (rechtmäßig handelnden) leitenden Mitarbeiters abgesehen.

2 Parlament

Siehe unten unter 9.4.1.

5 Inneres

5.1 Personalwesen

5.1.1 Nochmals zum Erfordernis einer Dienstvereinbarung beim Einsatz von Personalinformationssystemen

In 7/5.1.14 habe ich die Auffassung vertreten, dass der Abschluss einer Dienstvereinbarung beim Einsatz von Personalinformationssystemen aus verfassungsrechtlichen Gründen erforderlich sei. Dem haben das SMI und das SMWA entgegenhalten, *personalvertretungsrechtlich* bestehe keine Verpflichtung zum Abschluss einer Dienstvereinbarung; die Personalvertretung könne sie letztlich auch nicht erzwingen.

Selbst vor diesem Hintergrund sehe ich aus datenschutzrechtlicher Sicht in einer Dienstvereinbarung weiterhin die unverzichtbare Grundlage für die Verarbeitung von Beschäftigtendaten in einem automatisierten Personalinformationssystem. Dies legt das Gebot der Normenklarheit, also ein verfassungsrechtlicher Grundsatz, nahe, weil solche Verfahren tief in das Persönlichkeitsrecht eingreifen können. Datensätze verkürzen Sachverhalte, indem sie den Inhalt von Personalakten auf einzelne Daten reduzieren. Dadurch entstehen „schiefe Bilder“. Zudem verleiten Personalinformationssysteme bei organisatorischen, sozialen oder personellen Maßnahmen dazu, den Personalbestand „vorzufiltern“ und „Schema-F-Entscheidungen“ zu treffen. Nicht ohne Grund sieht das Sächsische Beamtengesetz in § 124 Abs. 4 vor, dass beamtenrechtliche Entscheidungen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden dürfen, „die unmittelbar durch automatisierte Verarbeitung personenbezogener Daten gewonnen werden“. Dazu gehören auch Vorfilter- oder Rasterentscheidungen, z. B. bei Beförderungen.

Nur Dienstvereinbarungen bieten die Gewähr, dass Bedienstete und ihre Vertreter mitentscheiden, welche (Personalakten-)Daten verarbeitet und zu welchen Zwecken sie ausgewertet werden. Das schafft nicht nur die verfassungsrechtlich gebotene Überschaubarkeit aus der Sicht der Betroffenen, sondern auch die erforderliche Transparenz für die Belegschaft und die Vorgesetzten sowie für die Kontrollorgane. Dienstvereinbarungen sind Rechtsnormen (eben nicht nur Verwaltungsvorschriften) die Eingriffe in die Selbstbestimmungsrechte der Bediensteten legitimieren.

Ich kann daher die Ausführungen in meinem 7. Tätigkeitsbericht nur unterstreichen.

5.1.2 Ausführungsbestimmungen der Bereitschaftspolizei Sachsen zur Erstellung von Beurteilungen

Meiner wiederholten Kritik an der Beurteilungsrichtlinie der Bereitschaftspolizei (vgl. 6/5.1.2 und 7/5.1.3), die sich insbesondere auf die *Verpflichtung* zum Anfertigen von schriftlichen Gedankenstützen und deren nicht sachgerechte Behandlung außerhalb der Personalakten bezog, folgte eine Erörterung im SMI mit dem Ergebnis, dass diese Notizen nicht mehr *vorgeschrieben* werden.

Nunmehr wird eindeutig geregelt, dass es den Vorgesetzten *freisteht*, im Vorfeld der Erstellung von Beurteilungen schriftliche Gedankenstützen zum eigenen persönlichen Gebrauch über Arbeitsergebnisse und Verhaltensweisen der zu Beurteilenden zu führen. Die Unterlagen sind (außerhalb der Personalakte) unter Verschluss zu halten und dürfen *niemandem* offenbart oder mitgeteilt werden. Auch die Vernichtung solcher Aufzeichnungen unmittelbar nach Bestandskraft der Beurteilung wird geregelt.

5.1.3 Paginierung von Personalakten

Das SMI hat mir den Entwurf einer Verwaltungsvorschrift mit ergänzenden Hinweisen zu der Verwaltungsvorschrift über die Führung und Verwaltung von Personalakten der Beamten vom 11. Dezember 1998 übersandt. Der Entwurf sah vor, dass die Seiten von Grund-, Teil- und Nebenakten in Zukunft nicht mehr nummeriert werden dürfen, „da ansonsten die Entnahme eines Bestandteils, z. B. einer belastenden Behauptung, aufgrund einer unterbrochenen Nummerierung der Akte sichtbar wird und damit ggf. Rückschlüsse auf den Inhalt möglich sein könnten".

Ich habe mich gegen eine solche Regelung ausgesprochen, weil erfahrungsgemäß die Gefahr besteht, dass Unterlagen unbemerkt entfernt werden, bevor ein Beschäftigter Einsicht in seine Personalakte erhält oder bevor Dritte ihre Aufsichts- oder Kontrollbefugnisse wahrnehmen (z. B. Rechnungshof, Rechnungsprüfungsämter, Datenschutzbeauftragter). Nur anhand von nummerierten Seiten lässt sich nachvollziehen, ob eine Personalakte vollständig ist.

Das Argument, eine unterbrochene Nummerierung eröffne Rückschlüsse über einen belastenden Inhalt, vermag ich nicht zu teilen. Rückschlüsse sind nicht möglich, allenfalls Spekulationen. Diesen kann aus meiner Sicht mit einer neutralen Notiz begegnet werden, beispielsweise mit dem Text: „Die Seiten mit den Nummern xx bis yy wurden heute mit Kenntnis von Herrn / Frau (*Name*) entnommen." Selbst wenn dies im Einzelfall Anlass zu einer Spekulation über den Inhalt der entfernten Seiten sein mag, so ist dies eher hinzunehmen als die latente Unsicherheit, ob die Personalakten vollständig sind oder gar der Vertrauensverlust der Mitarbeiter in eine rechtmäßige Personalaktenführung.
„Sprechende Lücken" können bei einer Entfernung belastenden, jedoch rechtswidrig zustandegekommenen oder zeitlich überholten Materials sehr wohl entstehen (siehe § 122 SächsBG). Sie belasten nicht den Betroffenen, vielmehr die Verwaltung, die so auch sichtbar dokumentiert, dass sie die Akten zu recht bereinigen musste. Der wirkliche Gang der Dinge hinterlässt eben Spuren.

Ich habe gebeten, die Paginierung (Durchnummerierung) verbindlich vorzuschreiben. Dem ist das SMI nicht gefolgt.
Das SMF legt demgegenüber großen Wert auf eine ordnungsgemäße Paginierung, wie meine Kontrolle gezeigt hat.

Ich erwarte, dass alle Personalakten sächsischer Behörden ordentlich durchnummeriert werden.

5.1.4 Führung von Nebenakten an Schulen

Mehrfach haben sich Lehrer an mich gewandt und die Rechtmäßigkeit der an den Schulen geführten Personalnebenakten in Frage gestellt. Ich habe ihnen Folgendes geantwortet:

§ 117 Abs. 2 Satz 3 SächsBG erlaubt die Führung von Nebenakten, wenn die personalverwaltende Behörde nicht zugleich die Beschäftigungsstelle ist. Das ist im Schulbereich der Fall: Die Beschäftigungsstelle eines Lehrers ist die Schule, personalverwaltende Stelle ist das Regionalschulamt.

Nebenakten dürfen nur solche Unterlagen enthalten, die für die rechtmäßige Aufgabenerfüllung erforderlich sind. Diese beamtenrechtliche Regelung hat sich aus der Rechtsprechung entwickelt und ist über § 31 Abs. 1 SächsDSG auch auf Angestellte anwendbar. Vor diesem rechtlichen Hintergrund habe ich die „Durchführungshinweise zur Personalaktenführung“ des Sächsischen Staatsministeriums für Kultus vom 5. Februar 1999 (Ministerialblatt des SMK S. 235) geprüft und keinen Widerspruch zu den genannten Vorschriften feststellen können; denn die in dieser Verwaltungsvorschrift aufgeführten Unterlagen wie z. B. Lehrbefähigung, Lehrberechtigung, Pflichtstunden, Teilzeit, Abordnung, Versetzung, Funktionsübertragungen, Fort- und Weiterbildung, Urlaub, Mutterschutz, Erkrankungen usw. sind für den sachgerechten Einsatz eines Lehrers sowie zur Durchführung des Arbeits- bzw. Dienstverhältnisses erforderlich. Die Führung von Nebenakten an den Schulen ist also rechtmäßig.

Großer Unmut entstand erneut, als einige Schulleiter von den Lehrern verlangten, sie mögen die in den Nebenakten fehlenden Unterlagen in Kopie beibringen. Ich habe das SMK gebeten, das Vorgehen der Schulleiter zu unterbinden und dafür Sorge zu tragen, dass die Unterlagen von den Regionalschulämtern zur Verfügung gestellt werden. Der Grund liegt in Folgendem:

Gemäß § 117 Abs. 2 Satz 3 SächsBG dürfen Nebenakten nur Unterlagen enthalten, die sich auch in der Grundakte oder Teilakte befinden. Diese beamtenrechtliche Regelung gilt nach der „Gemeinsamen 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“ in Verbindung mit der „Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern über die Führung und Verwaltung von Personalakten der Beamten“ auch für die Lehrer im Angestelltenverhältnis. Diese Regelung impliziert die Übermittlung von Personalunterlagen durch das Regionalschulamt an die Schule. Werden Nebenakten aufgrund von Unterlagen geführt, die der Betroffene beibringt, liegt darin ein beträchtliches Risiko. Denn wie soll ein Schulleiter feststellen, ob die von dem Lehrer beigebrachten Unterlagen vollständig und aktuell sind, ob die Kopien mit den Originalen übereinstimmen und die Unterlagen - wie von § 117 Abs. 2 Sächsisches Beamtengesetz vorgesehen - sich auch in den Grund- bzw. Teilakten befinden?

Das SMK hat reagiert. Die Schulleiter wurden über die Regionalschulämter in Rundschreiben und Besprechungen auf die korrekte Handhabung hingewiesen.

5.1.5 Einsichtnahme in Personalakten durch den Rechnungsprüfer

Immer wieder werde ich gefragt, ob Rechnungsprüfer ohne Einwilligung der Beschäftigten Einsicht in Personalakten nehmen dürfen.

§ 95 SäHO lautet:

„*(1) Unterlagen, die der Rechnungshof zur Erfüllung seiner Aufgaben für e r f o r d e r l i c h hält, sind ihm auf Verlangen innerhalb einer bestimmten Frist zu übersenden oder seinen Beauftragten vorzulegen.*

(2) Dem Rechnungshof und seinen Beauftragten sind die erbetenen Auskünfte zu erteilen."

§ 17 Abs. 2 KomPrO lautet:

„*Die Gemeinde hat den Prüfer bei seinen Aufgaben zu unterstützen. Der Prüfer kann alle Auskünfte und Unterlagen verlangen sowie eigene Erhebungen vornehmen, die zur Erfüllung seiner Aufgaben e r f o r d e r l i c h sind.*"

Sowohl für den staatlichen, wie für den kommunalen Bereich gilt demnach, dass die Prüfer *nicht erforderliche* Unterlagen nicht verlangen dürfen (siehe auch 4/5.1.10).

Die Entscheidung, was erforderlich ist und was nicht, obliegt ausschließlich dem Prüfer, der selbstverständlich dem Grundsatz der Gesetzmäßigkeit der Verwaltung (Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf) verpflichtet ist, und nicht der geprüften Stelle. Soweit sich also der Prüfungsauftrag auf personalrelevante Zusammenhänge (z. B. zur richtigen Eingruppierung) bezieht, darf den Prüfern eine Einsichtnahme in die Personalakten nicht verweigert werden. Dies ergibt sich nicht zuletzt aus der VwVPersAktenB vom 11. Dezember 1998 (SächsABl. 1999, S. 10), wo unter E II, Abs. 3 ausdrücklich und beispielhaft auf § 95 SäHO als Grundlage für die Einsichtnahme der Prüfer in Personalakten verwiesen wird.

5.1.6 Personaldatenverarbeitung - Erfassung von Beschäftigtendaten durch Bild- und Tonaufzeichnungen; Zugangskontrolle per Videoaufzeichnung

Bei einer datenschutzrechtlichen Kontrolle im Staatsschauspiel Dresden habe ich festgestellt, dass die Gebäudezugangsbereiche, die Proben und der Spielbetrieb mit Videokameras überwacht werden. Im Außenbereich wird teilweise der umliegende Verkehrsraum mit erfasst. Ein Hinweis auf die Videoüberwachung war in keinem Fall ersichtlich. Die Daten der Zugangskontrolle werden eine Woche gespeichert. Die Bilddaten der Bühnenüberwachung (z. B. Maschinenraum, Licht- und Tonregie) stehen für Techniküberwachung und Koordinierung des Spielbetriebes zur Verfügung und sind zusätzlich über Fernsehapparate (mit möglicher Videokassettenaufzeichnung) abrufbar. Die Beschäftigten können nicht erkennen (z. B. durch Lichtsignale), wann eine Beobachtung erfolgt.

Ich habe mich dazu wie folgt geäußert:
Mit der Videoüberwachung der Eingangsbereiche (z. B. Personaleingang) und des Bühnenbereiches werden Beschäftigtendaten erfasst, die als Leistungs- und Verhaltenskontrolle geeignet sind, ständigen Überwachungsdruck auf die Beschäftigten (ggf. auch auf Schauspieler) auszuüben, was unter Missachtung des Übermaßverbots in unverhältnismäßiger Weise in deren Persönlichkeitsrecht eingreift. Daher habe ich die Erforderlichkeit und die Zulässigkeit im Hinblick auf die Transparenz der Datenverarbeitung gemäß dem Volkszählungsurteil des BVerfG vom 15. Dezember 1983 (der Betroffene muss wissen, was, wann und wer, bei welcher Gelegenheit über ihn weiss) in Frage gestellt.
Nur wenn die Voraussetzungen, unter denen die Berechtigten Kontrollfunktionen (über Arbeitsabläufe von Proben und Vorstellungen) per Video durchführen dürfen in einer Dienstvereinbarung gemäß § 80 Abs. 3 Nr. 16 SächsPersVG geregelt werden, kann den Videobeobachtungen zugestimmt werden. Für die Betroffenen muss deutlich erkennbar sein, wann, wo und wozu die Beobachtung erfolgt. Sonst wäre die Videobeobachtung unzulässig.
Der Intendant hat aufgrund meiner datenschutzrechtlichen Bedenken den Abschluss einer Dienstvereinbarung auf den Weg gebracht, zu der ich mich insbesondere zu Löschungsfristen und dem Erfordernis gut sichtbarer Hinweisschilder äußern werde. Die Angelegenheit ist noch im Fluss.

5.1.7 Beamtenvereidigung

Der in 7/5.1.5 vom SMI unterbreitete und von mir akzeptierte Lösungsvorschlag wurde inzwischen im staatlichen Bereich offiziell wie folgt verwirklicht:

Muster siehe letzte Seite dieses Berichtes.

Sofern der Eid gemäß § 70 Abs. 2 SächsBG mit der Beteuerung „So wahr mir Gott helfe“ geleistet und/oder gemäß § 70 Abs. 3 SächsBG an Stelle der Worte „ich schwöre“ eine andere Beteuerungsformel gebraucht wird, ist dies nur *auf ausdrücklichen Wunsch* des Beamten auf der Niederschrift über die Vereidigung handschriftlich mit bestätigenden Unterschriften zu vermerken.

Die Wahlmöglichkeit des Beamten, den Diensteid mit oder ohne Beteuerung zu leisten oder eine andere Beteuerungsformel zu gebrauchen, wird dadurch nicht eingeschränkt.

Den nichtstaatlichen Dienstherren wurde empfohlen, entsprechend zu verfahren.

5.1.8 Aufzeichnungen über negative Erkenntnisse über die Amtsführung eines (ehemaligen) Verwaltungsleiters durch den Rektor einer Hochschule auf Geheiß des SMWK

Der ehemalige Verwaltungsleiter einer Hochschule informierte mich von Datenerhebungen des SMWK durch den Hochschulrektor, die Grundlage für eine Personalentscheidung sein sollten. Denn seine Stelle sollte entfallen. So musste der Hoch-

schulrektor auf Weisung des SMWK ab ca. Oktober 1998 bis weit ins Jahr 1999 hinein ausschließlich *negative* Erkenntnisse über den Betroffenen sammeln.

Im Zusammenhang mit der Entbindung des Petenten von seinen Aufgaben wurde eine Zusammenstellung dieser Erkenntnisse vom Fachreferat im SMWK tatsächlich angefordert und dem Personalreferat zur Verfügung gestellt.
Das SMWK hielt solche Vorgehensweise mit § 117 Abs. 4 SächsBG für vereinbar.

Entgegen der Auffassung des SMWK begegnen einer solchen Sicht- und Verfahrensweise grundsätzliche Bedenken:

§ 117 Abs. 4 SächsBG regelt ausschließlich, für welche *Zwecke* der Dienstherr die hierfür erforderlichen Daten erheben darf; ungeregelt bleibt, unter welchen *Voraussetzungen* und *bei wem/bei welchen Stellen* die Datenerhebung erfolgen darf. Das Urteil des Bundesverfassungsgerichts (Volkszählungsurteil) vom 15. Dezember 1983 (BVerfGE 65, S. 44 ff.) verlangt aber, dass Einschränkungen des Rechts auf informationelle Selbstbestimmung einer *normenklaren* und *verhältnismäßigen* gesetzlichen Grundlage bedürfen (siehe auch Art. 33 SächsVerf): 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. Informationelle Selbstbestimmung setzt aber voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich entsprechend dieser Entscheidung auch tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in welchen 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 wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der der Betroffene nicht mehr wissen kann, wer was wann und bei welcher Gelegenheit über ihn 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. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern schädigt auch das Gemeinwohl. Denn Selbstbestimmung ist eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt 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 i. V. m. Art. 1 Abs. 1 GG sowie von Art. 33 SächsVerf umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

All diese Grundsätze finden in § 117 Abs. 4 SächsBG (mit Ausnahme der Nennung der Zwecke, für die die Datenerhebung *erforderlich* sein soll) keinen Niederschlag, weil der Kreis der Stellen, bei denen Daten erhoben werden können, in keiner Weise konturiert wird: So kommen jegliche Stellen in Betracht, die personenbezogene Daten besitzen, private wie öffentliche. Aus diesem Grunde ist bei Datenerhebungen nach § 117 Abs. 4 SächsDSG ein Rückgriff auf § 11 SächsDSG, der den verfassungsrechtlichen Mindeststandard der Datenerhebung regelt, unerlässlich. Dort sind nämlich in Absatz 2 der vom Bundesverfassungsgericht vorgegebene Grundsatz, dass die Daten grundsätzlich beim Betroffenen selbst zu erheben sind, sowie sonstige Voraussetzungen für die Datenerhebung festgeschrieben. Nur ausnahmsweise dürfen abweichend von diesem Grundsatz personenbezogene Daten unter den abschließend in § 11 Abs. 4 SächsDSG aufgeführten Voraussetzungen bei Dritten erhoben werden.

Die Beauftragung des Hochschulrektors, negative Daten über den Verwaltungsleiter zu sammeln und diese Sammlung dem SMWK zur Verfügung zu stellen, ist aus keinem der in § 11 Abs. 4 SächsDSG aufgeführten Gründe gerechtfertigt gewesen. Die Datenerhebung des SMWK durch den Hochschulrektor war deshalb in dieser Form und mit diesem Inhalt unzulässig.

Unabhängig von vorstehenden Überlegungen war die Datenerhebung aber auch schon deshalb unzulässig, weil sie gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz verstößt. Die Maßnahme war nämlich aus mehreren Gründen weder geeignet noch angemessen und schon gar nicht erforderlich.

Zum einen wurde unter Missachtung des Übermaßverbots angeordnet, *ausschließlich negative Erkenntnisse* über den Verwaltungsleiter, und zwar über einen geraumen Zeitraum, zu sammeln, *positive hingegen nicht*. Dass dies zu einer subjektiven Einschätzung des Betroffenen führte (ohne dass die Grundsätze des § 119 SächsBG beachtet wurden), liegt auf der Hand.

Zum anderen hätte spätestens mit In-Kraft-Treten des Sächsischen Hochschulgesetzes am 1. Juli 1999, als nämlich Verwaltungsleiterstellen kraft Gesetzes obsolet wurden, auf weitere Datenerhebungen mangels Erforderlichkeit verzichtet werden müssen. Der datenschutzrechtliche Grundsatz der Erforderlichkeit bedeutet nämlich, dass die öffentliche Stelle ohne die Daten im konkreten Einzelfall ihre Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Es reicht deshalb nicht aus, wenn die Daten zur Aufgabenerfüllung der erhebenden Stelle nur „dienlich“ oder z. B. als Hintergrundinformation oder zur „Abrundung des Bildes“ nützlich sind (vgl. im Übrigen Simitis/Dammann/ Geiger/Mallmann/Walz, § 13 BDSG, Rdnr. 23). Genau hierzu erfolgte aber die Datensammlung, obwohl sich im SMWK bereits eine Meinung über Eignung und fachliche Leistung des Betroffenen verfestigt hatte.

Ich habe das SMWK daher aufgefordert, das auf unzulässige Weise zustande gekommene Geheft mit den negativen Eindrücken über den Betroffenen unverzüglich zu vernichten. Dem ist das SMWK sofort nachgekommen.

5.1.9 Verfahren bei Gehaltspfändungen im Landesamt für Finanzen

In 7/5.1.6 habe ich darüber berichtet, dass die Bezügestelle des LfF die personalverwaltenden Stellen über jeden Gehaltspfändungs- und Überweisungsbeschluss unterrichtet. Da solche Mitteilungen nur in seltenen Fällen dienstrechtlich relevant sind und - so hat meine Recherche ergeben - meistens bloß abgeheftet werden, drängt sich die Frage auf, ob tatsächlich jede (kleine) Pfändung mitgeteilt werden muss. Gegenüber SMF und SMI habe ich meine Sichtweise wie folgt konkretisiert:

1. *Erforderlichkeit der Mitteilung von der Bezügestelle an die personalverwaltende Stelle*
   Diese Mitteilung ist nur erforderlich, wenn seitens der Personalverwaltung daraus Konsequenzen gezogen werden und diese aktenkundig gemacht werden. Mögliche Konsequenzen sind: Hilfsangebote (z. B. Vorschussgewährung), Umsetzung des Betroffenen aus einem „korruptionsanfälligen“ oder „sicherheitsempfindlichen“ Bereich und bei der Personalplanung keine Besetzung einer solchen Stelle mit einem verschuldeten Mitarbeiter. Vor diesem Hintergrund dürften deshalb nur „größere“ Beträge oder nachhaltige Verschuldung interessant sein.

2. *Wann sollen Mitteilungen erfolgen?*
   - Wenn der Pfändungsbetrag (einschließlich Kosten) das Monatsbrutto übersteigt (entweder als Einzelpfändung oder in der Addition mehrerer Pfändungen).
   - Wenn der Betroffene in einem besonders sicherheitsempfindlichen Bereich tätig ist; denn die Sicherheitsüberprüfung, die auch die wirtschaftlichen Verhältnisse betrachtet, gibt nur den Status zu einem bestimmten Zeitpunkt wieder. Insoweit habe ich gegen turnusmäßige Anfragen der personalverwaltenden Stellen beim LfF keine Bedenken.

3. *Rechtsgrundlage für die Mitteilungen*
   Auch wenn die Ermächtigungsgrundlage in § 1 Abs. 1 Nr. 2 SächsVertrG nach meiner Auffassung nicht zu den Verfahrensregelungen in § 12 Abs. 2 VertretungsVO ermächtigt, so ergibt sich dennoch die Zulässigkeit aus §§ 31 Abs. 1 SächsDSG, 117 Abs. 1 und 2 SächsBG. Von meiner in 7/5.1.6 vertretenen Auffassung nehme ich insoweit Abstand.

Die konstruktiven Gespräche dauern an; ich rechne mit einer einvernehmlichen Regelung, die überflüssige Datenübermittlungen vermeidet.

5.1.10 Teilnehmereinschätzungen im Rahmen von Fortbildungsveranstaltungen

In ihrer Stellungnahme zu 7/5.1.13 führt die Staatsregierung aus:

„Das Sächsische Staatsministerium der Finanzen hält einen völligen Verzicht auf eine Erfolgskontrolle aufgrund der Bedeutung der Fortbildung für die Steigerung von Qualität und Quantität der Arbeitsabläufe im Geschäftsbereich für nicht vertretbar. Insoweit hat es sich innerhalb seiner ihm zustehenden Organisationsbefugnis für die

im Tätigkeitsbericht dargestellte Form der Teilnehmereinschätzung entschieden und hält an seiner Einschätzung fest, dass eine generelle schriftliche Leistungsabforderung im Rahmen der Fortbildungsveranstaltungen für die Beschäftigten der Steuerverwaltung nicht in Betracht kommt. Dies entspricht auch den Intentionen des Hauptpersonalrats im Geschäftsbereich des Sächsischen Staatsministerium der Finanzen und der Deutschen Steuergewerkschaft.

Eine größtmögliche Objektivität bei der Einschätzung der Teilnehmer durch Dozenten wird u. a. erreicht durch:

- *den Einsatz qualifizierter Dozenten*

- *die Bewertung durch einen Dozenten nur dann, wenn dieser ausreichend Gelegenheit hatte, sich über den Einsatz jedes einzelnen Teilnehmers und die Qualität seiner Beiträge ein Urteil zu bilden. Dies ist bei mindestens einwöchigen Fortbildungsmaßnahmen, die ausschließlich durch einen Dozenten durchgeführt werden, erfahrungsgemäß gegeben.*

- *Herstellung eines einheitlichen Beurteilungsmaßstabes, gewährleistet durch regelmäßige Dozentenbesprechungen.*

Ferner verfügen die Dozenten über verschiedene Methoden (Gruppenarbeit, gezielte Befragung der Teilnehmer, kurzes Lösen von Beispielen), um sich einen Eindruck über die Lehrgangsteilnehmer zu verschaffen."

Unerwähnt bleibt, dass sich das SMF *„im Rahmen seiner ihm zustehenden Organisationsbefugnis" d*azu entschlossen hat, den Beschäftigten seines Zuständigkeitsbereichs eine differenzierte Teilnahmebescheinigung auszustellen, die wie folgt aussieht:

- hat *mit Erfolg* teilgenommen,
- hat teilgenommen.

Hiergegen habe ich eingewandt, dass eine Aufnahme solcher Fortbildungsnachweise in die Personalakten der Betroffenen zwangsläufig eine Ungleichbehandlung gegenüber den Bediensteten der anderen Ressorts und sonstiger Behörden (z. B. außersächsische Dienstherren, Kommunen), die solche Differenzierungen nicht kennen, nach sich zieht. Die bisher allgemein übliche Teilnahmebescheinigung „hat teilgenommen" stellt sich aus Sicht des SMF als nicht hinreichend qualifiziert, mithin als „abwertend" dar, was sich bei Bewerbungen/Versetzungen nachteilig auswirken kann.

Im Übrigen muss für die Fortbildungsnachweise „hat teilgenommen" und „hat mit Erfolg teilgenommen" die Justizgarantie (Art. 19 Abs. 4 GG) gelten.
Ferner habe ich darauf hingewiesen, dass die vom SMF wiederholt zitierte „Organisationsbefugnis", die die von mir kritisierte Verfahrensweise rechtfertige, ihre gesetzlichen Grenzen z. B. in §§ 117 ff. SächsBG, § 31 SächsDSG findet (Art. 20 Abs. 3 GG, Art. 3 Abs. 3, 33 SächsVerf).

Hierauf steht eine Stellungnahme des SMF noch aus.

5.1.11 Kontrolle der Verarbeitung von Beschäftigtendaten bei einer Kriminalpolizeiinspektion

Anlässlich einer datenschutzrechtlichen Kontrolle bei einer Kriminalpolizeiinspektion wurden auf dem hauseigenen System im Sachbereich Innerer Dienst eine Reihe von Dateien mit Beschäftigtendaten gefunden, die der KPI-Leiter für seinen Bedarf angelegt hatte, ohne dass meine Beteiligung gemäß § 31 Abs. 7 SächsDSG erfolgt ist. Im Einzelnen handelte es sich um eine

1. Anwesenheitsliste „Einsatzplan“, aus der Abwesenheitsgründe wie Urlaub, Krankheit, Lehrgang, dienstfrei ersichtlich sind,

2. Überstundendatei, in der die Daten aus der manuellen Zeiterfassung übernommen werden,

3. Abwesenheitsdatei (wer ist in welcher Angelegenheit mit welchem Dienstwagen und welcher Funknummer wohin unterwegs und wann kommt er voraussichtlich zurück),

4. Diensthabendendatei einschließlich Einsatzgruppen zum Zwecke der Alarmierung,

5. Urlaubsdatei.

Meinen Feststellungen zufolge fehlte bei den Dateien (lfd. Nr. 2 und 3), die geeignet sind, die Leistung und das Verhalten der Bediensteten zu kontrollieren, auch die nach § 80 Abs. 3 Nr. 16 SächsPersVG erforderliche Mitbestimmung des Personalrats.

Neben diesen (bislang) rechtswidrig betriebenen Dateien mit Beschäftigtendaten wurde auch eine personenbezogen geführte Asservatendatei festgestellt, bei der die nach § 50 SächsPolG vorgeschriebene Errichtungsanordnung einschließlich meiner Beteiligung fehlt.

Da nicht auszuschließen ist, dass auch in den übrigen Polizeidienststellen solche „selbstgestrickten“ Dateien existieren, ohne dass diese Verfahren nach § 31 Abs. 7 SächsDSG, § 80 Abs. 3 Nr. 16 SächsPersVG, § 50 SächsPolG behandelt wurden, habe ich das SMI gebeten, die Polizeidienststellen im Rahmen der Dienstaufsicht zu sensibilisieren und ggf. zu kontrollieren (Verhinderung von „Wildwuchs“).

5.1.12 Aufbewahrung und Löschung von Unterlagen über erfolglose Bewerbungen

Nach § 31 Abs. 4 SächsDSG sind Daten, die vor Beginn eines Dienst- oder Arbeitsverhältnisses erhoben wurden, unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt.

Für die praktische Umsetzung dieser Vorschrift vertrete ich Folgendes:

1. Aufzubewahrende Bewerbungsunterlagen sind: Bewerbungsschreiben, Eingangsbestätigung, ggf. Zwischenbescheid, Einladung des Bewerbers und der Teilnehmer am Auswahlverfahren, Bewerberspiegel, Aufzeichnungen zu den Vorstellungsgesprächen, Absageschreiben, ggf. Schriftverkehr mit dem Bewerber. Alle übrigen Bewerbungsunterlagen, die beispielsweise als Anlagen dem eigentlichen Bewerbungsschreiben beigefügt waren (Lebenslauf, Lichtbild, Zeugnisse, Urkunden, Befähigungsnachweise usw.), werden mit der Absage an den Bewerber zurückgesandt.

   Wie lange aber die zurückbehaltenen Unterlagen aufzubewahren sind, ist fraglich. Der Bemessung der Frist liegt auch die Überlegung zugrunde, dass auf die Unterlagen und Aufzeichnungen in einem möglichen Gerichtsverfahren als Beweismittel zurückgegriffen werden muss und bei der Auswahl von Beamten der ablehnende Bescheid die Qualität eines Verwaltungsaktes hat: Denn aus Art. 33 Abs. 2 i. V. m. Art. 19 Abs. 4 GG folgt, dass das Recht auf Zugang zu öffentlichen Ämtern nach gerechter Bewertung von Eignung, Befähigung und fachlicher Leistung einklagbar sein muss. Deshalb muss der Dienstherr unterlegene Beamtenbewerber vor der Ernennung eines Mitbewerbers vom Ausgang des Verfahrens so rechtzeitig unterrichten, dass ein effektiver Rechtsschutz gewährt ist. Für Angestellte und Arbeiter besteht ähnlicher arbeitsrechtlicher Konkurrentenschutz. Diese Mitteilung an den unterlegenen Mitbewerber ist nach herrschender Auffassung in Bezug auf Beamtendienstposten (= öffentliches Recht) ein Verwaltungsakt, der normalerweise mit Rechtsmittelbelehrung zu versehen ist. Dann beträgt die Klagefrist einen Monat.

   Häufig aber enthalten die Ablehnungsbescheide keine Rechtsbehelfsbelehrung, so dass die Rechtsbehelfsfrist gemäß § 58 Abs. 2 VwGO ein Jahr beträgt. Fristbeginn ist der Tag des Bescheidzugangs. Dieser ist nur bei Zustellung mit Postzustellungsurkunde genau zu bestimmen. Da jedoch diese Zustellungsform bei der Ablehnung einer Bewerbung unüblich ist, erscheint ein Zeitpuffer von einem Monat als angemessen. So hat es die Verwaltung selbst in der Hand zu entscheiden, ob die Auswahlentscheidung nach Ablauf einer Frist von einem Monat oder erst nach 13 Monaten bestandskräftig wird. Aus datenschutzrechtlicher Sicht muss eine Rechtsbehelfsbelehrung beigefügt und mit Postzustellungsurkunde zugestellt werden, damit die Unterlagen möglichst schnell vernichtet werden können. Das spart im Übrigen viel Verwaltungsaufwand.

2. Sofern Bewerberdaten in der Personalverwaltung auch automatisiert erfasst werden, sind sie ebenfalls nach 13 Monaten zu löschen.

3. Erfolglose, hausinterne Bewerbungen haben wie externe Bewerbungen Sachaktenqualität; denn sie stehen in keinem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis (§ 117 Abs. 1 SächsBG, analog bei Arbeitern und Angestellten). Sie sind ebenfalls 13 Monate aufzubewahren.

5.2 Personalvertretung

Aufbewahrung und Löschung von Unterlagen über Personalmaßnahmen beim Personalrat

Die personalverwaltenden Stellen beteiligen den Personalrat meist in Form eines Schreibens, aus dem sich der Sachverhalt und die beabsichtigte Maßnahme ergeben. Die erforderlichen Unterlagen werden üblicherweise in Kopie beigefügt. In 5/5.2.2 und 6/5.2 habe ich darauf hingewiesen, dass es unzulässig ist, wenn beim Personalrat die zur Verfügung gestellten Unterlagen und der darüber hinaus anfallende Schriftwechsel zu einer über den Bediensteten geführten Akte genommen und mit vorangegangenen Personalmaßnahmen zusammengeführt werden. Auf diese Weise würden Personal-Nebenakten im Sinne von § 117 Abs. 2 SächsBG entstehen, die den beruflichen Werdegang nachzeichnen und beim Personalrat fehl am Platze sind.

Auf meine diesbezüglichen, im Geschäftsbereich des SMK getroffenen Feststellungen hat das Ministerium reagiert und die Personalräte schriftlich auf die korrekte datenschutzrechtliche Handhabung hingewiesen. Bei der Kontrolle eines Hauptpersonalrats im Geschäftsbereich eines anderen Ministeriums bin ich wieder auf solche „Nebenakten“ gestoßen. Dies nehme ich zum Anlass, nochmals die Grundsätze zur Aufbewahrung und Löschung aufzuzeigen.

Nebenakten dürfen unter den in § 117 Abs. 2 SächsBG genannten Voraussetzungen nur von der personalverwaltenden Stelle geführt werden. Die Personalvertretung gehört nicht dazu. Deshalb hat sie Unterlagen über eine bestandskräftig abgeschlossene oder anderweitig endgültig erledigte Maßnahme nach einer angemessenen Frist zu vernichten, spätestens jedoch, wenn der Personalmaßnahme eine neue folgt (§ 19 Abs. 2 SächsDSG). Die ggf. in einem EDV-System noch gespeicherten Schreiben sind gleichzeitig zu löschen. Da sich die Unterlagen ohnehin in der Personalakte des Bediensteten befinden, kann die Personalstelle sie bei Bedarf (erneut) zur Verfügung stellen.

Vor einer Vernichtung sind die Unterlagen gemäß § 5 SächsArchivG dem zuständigen Archiv zur Übernahme anzubieten (vgl. auch § 19 Abs. 3 SächsDSG).

Die beschriebene Handhabung hat zudem den Vorteil, dass der Aktenbestand „automatisch“ um die Akten ausgeschiedener Mitarbeiter bereinigt wird; denn die Personalvertretung erhält nur im Fall der Kündigung oder Versetzung Kenntnis vom Ausscheiden, nicht aber - zumindest nicht offiziell - vom Ausscheiden durch Tod oder aus Altersgründen. Da für ausgeschiedene Beschäftigte keine Personalmaßnahmen mehr in Betracht kommen können, ist die gesamte Akte i. S. v. § 19 Abs. 2 SächsDSG zur Aufgabenerfüllung nicht mehr erforderlich. Eine Aufbewahrung über das Beschäftigungsende hinaus wäre beim Personalrat unzulässig.

5.3 Einwohnermeldewesen

5.3.1 Automatisierter Datenabruf der Polizeibehörden aus dem Melderegister (§ 11 SächsMeldDÜVO)

Im Frühjahr 2000 verstärkten sich im SMI die Aktivitäten, den Polizeibehörden Online-Zugriffe auf sächsische Melderegister gemäß § 11 Abs. 3 SächsMeldDÜVO zu gestatten.

Ich habe vorsorglich vorgeschlagen, aus datenschutzrechtlicher Sicht wie folgt zu verfahren:

1. In jeder Polizeidirektion wird ein rund um die Uhr mit Fachkräften besetzter Bildschirm installiert, von dem aus auf alle Melderegister (soweit technisch möglich) im jeweiligen Zuständigkeitsbereich zugegriffen werden darf. Nachgeordnete Polizeidienststellen rufen bei Bedarf in der Polizeidirektion an, um sich die für ihre Aufgabenerfüllung erforderlichen Meldedaten mitteilen zu lassen (Vorteil: Filterfunktion bei der Polizeidirektion).

2. Da dem eindeutigen Wortlaut des § 11 Abs. 1 SächsMeldDÜVO zufolge nur die zur Aufgabenerfüllung *erforderlichen* Daten abgerufen werden dürfen, ist der jeweilige Datenumfang durch entsprechende Masken je nach Erforderlichkeit zu staffeln (z. B. Maske 1 = nur Namen, Anschrift und Geburtsdatum), bis hin zum Höchstumfang des durch § 11 Abs. 1 SächsMeldDÜVO vorgegebenen Rahmens.

3. Abweichend von § 4 Abs. 3 SächsMeldDÜVO ist ausnahmslos jeder Datenabruf zur Kontrolle der Rechtmäßigkeit der Anfragen bei der Polizeidirektion zu protokollieren (wer hat wann über wen für welche Polizeidienststelle welche Daten abgerufen?). Eine Protokollierung bei der jeweiligen Meldebehörde bzw. im Rechenzentrum des Datenlieferanten ist unzulässig, weil so die Meldebehörde von polizeilichen Aktivitäten in Bezug auf die Betroffenen informiert würde.

4. § 4 SächsMeldDÜVO ist zu beachten (sonstige personelle, technische und organisatorische Voraussetzungen).

Unter den o. a. Voraussetzungen ist es nicht erforderlich, anderen Polizeidienststellen als den Polizeidirektionen Online-Zugriffe auf sächsische Melderegister zu gestatten. Es würden nur die *erforderlichen* personellen, technischen und organisatorischen Maßnahmen getroffen (§ 4 Abs. 1 SächsMeldDÜVO). Der Grundsatz der Verhältnismäßigkeit bliebe gewahrt, Kosten würden gespart.

Ich habe gebeten, mich an der weiteren Entwicklung zu beteiligen.

5.3.2 Veröffentlichung von Jubiläumsdaten in gemeindlichen Mitteilungsblättern

Nach § 33 Abs. 2 SächsMG darf die Gemeinde Namen, Doktorgrad, Anschriften, Tag und Art des Jubiläums von Alters- und Ehejubilaren veröffentlichen. Altersjubilare

sind Einwohner, die den 70. oder einen späteren Geburtstag begehen; Ehejubilare sind Einwohner, die die goldene Hochzeit oder ein späteres Ehejubiläum begehen. Der Veröffentlichung kann gemäß § 33 Abs. 4 SächsMG widersprochen werden. Hierauf hat die Meldebehörde mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.
Durch eine Eingabe erfuhr ich, dass eine Gemeinde entgegen o. a. Bestimmungen bereits die Daten der über 59jährigen im Gemeindeblatt veröffentlicht. Nachdem ich auf die Unzulässigkeit der Veröffentlichung der Daten vor Vollendung des 70. Lebensjahres hingewiesen habe, hat die Gemeinde die künftige Beachtung des § 33 SächsMG zugesichert.

Eine Veröffentlichung der Daten von Einwohnern, die noch nicht 70 Jahre alt sind, wäre allenfalls mit deren Einwilligung akzeptabel; sie gehört auch nicht zum traditionellen Aufgabenkreis der Gemeinde. Manche(r) findet es eben gar nicht so lustig, wenn sein /ihr „jugendliches Alters“ schon im „Seniorenverzeichnis“ steht.

5.3.3 Folgen von Personenverwechslungen bei Melderegisterauskünften

In 6/5.3.3 habe ich bereits auf die unangenehmen Folgen, die mit auf Personenverwechslung beruhenden Melderegisterauskünften verbunden sind, hingewiesen und Maßnahmen zur Schadensbegrenzung angeregt. Dennoch erreichte mich wieder ein Beschwerdebrief eines Betroffenen.

Der Eingabe des Petenten zufolge hätte die Meldebehörde verschiedenen Behörden und Firmen Auskünfte aus dem Melderegister mit der Folge erteilt, dass er mit kriminellen Machenschaften in Verbindung gebracht und auf Betreiben eines Finanzamtes sogar mit einem Gerichtsvollzieher konfrontiert wurde. Augenscheinlich war der Mann das Opfer einer Personenverwechslung bei Melderegisterauskünften.

Ich habe die Meldebehörde unter Beifügung von 6/5.3.3 gebeten, unverzüglich Maßnahmen zur Schadensbegrenzung zu ergreifen. Insbesondere sollte sich die Meldebehörde auch mit dem Petenten in Verbindung setzen, um ihn auf die Möglichkeit der Beantragung einer Auskunftssperre hinzuweisen, die m. E. aus Billigkeitsgründen kostenfrei sein sollte.

5.3.4 Die Einwohnermeldeauskunft der Zukunft

Ein Privatunternehmen stellte mir ein Projekt vor, mit dem sogenannte einfache Melderegisterauskünfte via Telefon abgewickelt werden sollen.
Die Firma stellt dem Einwohnermeldeamt einen Dienst zur Verfügung, der sich so spezifiziert, dass der Telefonanschluss, den das Einwohnermeldeamt ihr mitteilt, in folgenden Programmablauf eingebunden wird:

- Der Auskunftssuchende wählt die von der Firma publizierte Servicerufnummer 0190-0 ... Nach einer kurzen Begrüßung wird er aufgefordert, die PLZ der gesuchten Person mittels Telefontastatur einzugeben.

- Das Programm erkennt das zu dieser PLZ gehörige Einwohnermeldeamt und verbindet den Anrufer zu der vom Einwohnermeldeamt angegebenen Telefonnummer.

- Sollten zu dieser Uhrzeit keine Auskünfte gegeben werden, gibt das System dem Anrufer einen Hinweis „Dieses Einwohnermeldeamt können Sie nur in der Zeit von ... bis ... erreichen - bitte versuchen Sie es in dem angegebenen Zeitraum noch einmal."

- Der zuständige Mitarbeiter nimmt das Gespräch, nachdem er einen Hinweis über eine zu erteilende Einwohnermeldeauskunft bekommen hat, entgegen und erst jetzt kommen für den Anrufer Gebühren auf.

- Die Einwohnermeldeauskunft wird dem Auskunftsuchenden erteilt. Die Gebühren hierzu werden beim Informierten mittels Telefonabrechnung eingezogen.

- Sollte es sich um eine komplizierte Auskunft handeln, bei der erhöhte Gebühren anfallen, weil z. B. im Archiv gesucht werden muss, dann besteht die Möglichkeit, dass der Mitarbeiter dem Auskunftsuchenden dieses mitteilt und ihn bittet in z. B. einer Viertelstunde noch einmal anzurufen. In dieser Zeit kann der Mitarbeiter die gewünschte Auskunft ermitteln; der Anrufer zahlt durch den erneuten Anruf doppelte Gebühren.

  Der Zentralrechner der Firma stellt nur die Verbindung her. Die einzige Datei, die im System der Firma entsteht, ist die Anzahl der eingegangenen Anrufe zu den jeweiligen Einwohnermeldeämtern, zwecks Gebührenabrechnung, zum Monatsschluss. Eine Aufzeichnung des jeweiligen Telefonates ist ausgeschlossen.

Das Angebot ist eine innovative und vernünftige Variante zum herkömmlichen manuellen Auskunftsverfahren. Die weitere Entwicklung behalte ich im Auge.

5.4 Personenstandswesen

Datenerhebung durch den Standesbeamten bei vermuteter „Scheinehe"

Im Rahmen seiner Dissertation fragte ein Doktorand nach den datenschutzrechtlichen Möglichkeiten zur Erlangung von Anhaltspunkten, die dem Standesbeamten die Feststellung ermöglichen, dass es sich bei der bevorstehenden Eheschließung um eine „Scheinehe" handelt.

Bisher habe ich mich lediglich in 5/5.4.3 mit dem Thema „Scheinehen" unter Berücksichtigung der seinerzeitigen Rechtsgrundlagen befasst. Das inzwischen novellierte Personenstandsrecht veranlasste mich, die Problematik mit dem SMI zu erörtern.

Nach den personenstandsrechtlichen Vorschriften kann der Standesbeamte - sofern konkrete Anhaltspunkte dafür bestehen, dass die zu schließende Ehe nach § 1314 Abs. 2 BGB aufhebbar wäre - die Verlobten in dem hierzu erforderlichen Umfang einzeln oder gemeinsam befragen und ihnen ggf. die Beibringung geeigneter Nachweise aufgeben.

Aus datenschutzrechtlicher Sicht gehen diese Bestimmungen als leges speciales dem Sächsischen Datenschutzgesetz vor (§ 2 Abs. 4 SächsDSG), so dass m. E. wegen des abschließenden Charakters kein Raum mehr für eigene Nachforschungen des Standesbeamten (nach §§ 11 Abs. 4, 13 SächsDSG) z. B. bei der Ausländerbehörde *im Vorfeld oder neben* der vorgesehenen Befragung der Verlobten bleibt, um die „konkreten Anhaltspunkte“ erst einmal zu ermitteln. Keinesfalls darf ein Standesbeamter von Anhaltspunkten für eine Scheinehe nur deshalb ausgehen, weil ein Ausländer eine Deutsche heiratet.

Insbesondere hat mich interessiert, ob und ggf. nach welchen Bestimmungen der Standesbeamte aus Sicht des SMI befugt ist, z. B. bei der Ausländerbehörde (durch Befragung, durch Einsichtnahme in die Ausländerakte) nach „konkreten Anhaltspunkten“ zu suchen.

Das SMI teilte u. a. mit, dass es nach § 5 Abs. 4 PStG nicht Aufgabe des Standesbeamten sei, im Rahmen der Prüfung der Ehefähigkeit nach konkreten Anhaltspunkten für einen Aufhebungsgrund - z. B. durch Einsichtnahme in die Ausländerakte - zu „suchen“, denn der Standesbeamte hätte „kein beliebiges Nachforschungsrecht“. *Nur dann*, wenn aufgrund der routinemäßigen Prüfung der Ehefähigkeit *konkrete* Anhaltspunkte dafür erkennbar seien, dass die zu schließende Ehe aufhebbar wäre (z. B. weil eine wirkliche eheliche Lebensgemeinschaft nicht beabsichtigt ist und deshalb die Ehe als bloße Scheinehe eingegangen werden soll), sei der Standesbeamte berechtigt und verpflichtet, weitere Ermittlungen gemäß § 5 Abs. 4 PStG, z. B. auch durch Beteiligung der Ausländerbehörde, vorzunehmen. Ausführungsbestimmungen zu § 5 Abs. 4 PStG gäbe es im Freistaat Sachsen derzeit noch nicht. Wann, in welchem Umfang und in welcher Weise der Standesbeamte die Ausländerbehörde beteiligen soll, oder ob dem Standesbeamten weitere, nicht in § 5 Abs. 4 PStG genannte Beweismittel zur Verfügung stehen, bedarf noch der abschließenden Klärung. Ich bleibe „am Ball“.

5.5 Kommunale Selbstverwaltung

5.5.1 Datenschutzrechtliche Einordnung der Leipziger Versorgungs- und Verkehrsgesellschaft mbH und ihrer Tochterunternehmen

In einem konstruktiven Gespräch hat mir der Geschäftsführer die Aufgaben und Strukturen der Leipziger Versorgungs- und Verkehrsgesellschaft mbH ausführlich dargelegt.

Insbesondere hat er mir erläutert, dass seitens der Verwaltung und des Stadtrates Leipzig keinerlei bestimmender Einfluss auf die Tarifpolitik, die Personalentscheidungen und die Organisation der beteiligten Unternehmungen ausgeübt wird; deren Verhalten am Markt wird nicht unter verwaltungsrechtlichen oder kommunalpolitischen Aspekten gesteuert, sondern ganz real von marktwirtschaftlichen Überlegungen geprägt und bestimmt.

Unter diesen Bedingungen wird der öffentliche Versorgungsauftrag, wie er sich aus § 2 SächsGemO ergeben könnte, allenfalls theoretisch wahrgenommen; die tatsächliche Entwicklung in den letzten Jahren hat - jedenfalls in der Stadt Leipzig - dazu geführt, dass eine direkte Aufgabenerfüllung durch die Verwaltung der Gemeinde auf den Wirtschaftsgebieten, die die zu ihrem Verbund gehörenden Unternehmungen erfüllen, nicht stattfindet.

Deshalb lassen sich sowohl die Holding als auch die ihr zugehörenden Unternehmen nicht als öffentliche Stelle im Sinne des § 2 Abs. 2 SächsDSG definieren. Die dort stattfindende Verarbeitung personenbezogener Daten ist daher nicht durch das Sächsische Datenschutzgesetz, sondern durch das Bundesdatenschutzgesetz geregelt.

Es kann im vorliegenden Zusammenhang dahingestellt bleiben, ob in anderen Kreisen und kreisfreien Städten des Freistaates Sachsen wegen der dort vorhandenen andersartigen Strukturen auch eine andere rechtliche Einordnung der einschlägigen Unternehmen angezeigt ist. Mit anderen Worten: Die mir im Einzelnen dargelegten richtungweisenden und zukunftsorientierten Besonderheiten der Aufgaben und Strukturen der in Frage stehenden Unternehmen und insbesondere die Tatsache, dass diese keine Aufgabe der öffentlichen Verwaltung wahrnehmen, führen zu dem von mir dargestellten Ergebnis; Parallelen mit anderen Gebietskörperschaften sind nicht zwingend zu ziehen.

5.5.2 Veröffentlichung von Vereinsdaten im gemeindlichen Mitteilungsblatt

Eine Gemeinde fragte, ob sie außer Vereinsnamen und Sitz auch Namen und Adressen der örtlichen Vereinsvorstände im Mitteilungsblatt veröffentlichen dürfe.
Ich habe darauf hingewiesen, dass nach § 64 BGB i. V. m. § 3 Nr. 3 Vereinsregisterverordnung vom 10. Februar 1999 (BGBl. I S. 147) in das Vereins*register* u.a. auch die Namen und Anschriften des Vereinsvorstandes einzutragen sind. Gemäß § 66 Abs. 1 BGB i. V. m. § 14 Vereinsregisterverordnung ist die Eintragung unverzüglich zu veröffentlichen, allerdings *ohne* die personenbezogenen Vorstandsdaten.

Daraus folgt, dass die Gemeinde ihrerseits zwar Vereinsnamen und -anschriften der in der Kommune tätigen und deshalb für ihren umfassenden Aufgabenkreis bedeutsamen (§ 2 Abs. 1 SächsGemO) Vereine veröffentlichen darf, zumal ein unmittelbarer Personenbezug fehlt. Sollte jedoch auch die Veröffentlichung von Namen und Anschriften der Vereinsvorstände erwogen werden, so darf dies – nicht zuletzt aus Gründen des Gemeindefriedens (Konfliktvermeidung), besonders aber aus Gründen der informationellen Selbstbestimmung – nur mit deren Einverständnis erfolgen.

5.5.3 Einholung von SCHUFA-Auskünften über einen Vorhabenträger durch den Bürgermeister

Ein Bürgermeister versuchte ohne Kenntnis eines in Aussicht genommenen Vorhabenträgers dessen Bonität mittels SCHUFA-Auskunft zu überprüfen. Ich musste ihm mitteilen, dass nach § 11 Abs. 2 SächsDSG eine Datenerhebung grundsätzlich *bei den Betroffenen selbst* mit deren Kenntnis zu erfolgen hat. Nur unter den besonderen

Voraussetzungen des § 11 Abs. 4 SächsDSG ist eine Datenerhebung bei Dritten (hier SCHUFA) ausnahmsweise zulässig. Denn auch für die am Markt teilnehmende - also z. B. fiskalisch tätige - Verwaltung gelten die Regeln des öffentlichen Datenschutzrechts.

Der Bürgermeister hatte in seiner Stellungnahme nicht dargetan, ob und weshalb er sich die finanziellen Verhältnisse des Vorhabenträgers, z. B. durch Vorlage von Bilanzen, Kontoauszügen, Vermögensnachweisen, Bankbürgschaften u. ä. auf freiwilliger Basis, nicht hat vorlegen lassen. Eine solche Vorgehensweise hätte § 11 Abs. 2 SächsDSG entsprochen.

Auch hatte er nicht erläutert, welche der acht alternativen Voraussetzungen des § 11 Abs. 4 SächsDSG ihn bewogen hatte, ohne Kenntnis des Betroffenen eine SCHUFA-Auskunft zu beantragen. Ein Blick ins Gesetz hätte genügt, ihm klarzumachen, dass ihn § 11 Abs. 4 SächsDSG nicht ermächtigt, vom Grundsatz, die Daten zunächst beim Betroffenen selbst zu erheben, abzuweichen, es sei denn eine der dort genannten Voraussetzungen wäre erfüllt (was ich mir nur schwerlich vorzustellen vermag).

Vor diesem Hintergrund hielt ich sein Auskunftsersuchen an die SCHUFA für rechtswidrig und forderte ihn auf, bei künftigen Datenerhebungen die datenschutzrechtlichen Bestimmungen zu beachten. Nur unter dieser Voraussetzung habe ich von einer förmlichen Beanstandung (§ 26 SächsDSG) abgesehen.

5.5.4 Bewertungsausschuss in kommunalen Vertretungskörperschaften

Im Zuge der Konstituierung der kommunalen Vertretungskörperschaften in Sachsen werden in vielen Fällen so genannte Bewertungsausschüsse gebildet, die stellvertretend für die Vertretungskörperschaft zum einen die Abgeordneten, zum anderen Mitarbeiter der Kommune überprüfen sollen. Die damit einhergehende Diskussion wird teils unsicher (Was ist erlaubt, wie sollen wir es machen?), teils hochemotional (Ist das überhaupt noch sinnvoll?) geführt. Im Folgenden geht es um den ersten Teil dieser Diskussion, denn wenn sich kommunale Vertretungen entschließen, einen solchen Ausschuss zu bilden, haben die Beteiligten und vor allem die Betroffenen einen Anspruch darauf, dass die Ausschusstätigkeit zugleich gesetzeskonform und sensibel geschieht. Das für den Kreistag Gesagte gilt analog auch für Gemeinde- und Stadträte.

Die Überprüfung der Kreisräte hat einen rechtlichen Ansatzpunk im Stasi-Unterlagengesetz. Dort ist eine Überprüfung von Angehörigen kommunaler Vertretungskörperschaften gesetzlich ermöglicht (§ 21 Abs. 1 Nr. 6 b StUG). Das reicht als Rechtsgrundlage aus. Der Landkreis sollte darüber hinaus jedoch als kommunale Körperschaft sich dafür eine gesicherte Verfahrensordnung geben. Dies kann eine eigene Satzung, ggf. auf Grundlage der Hauptsatzung, aber auch ein einfacher Beschluss des Kreistages sein, für seine Mitglieder einen Bewertungsausschuss einzurichten. Die Satzung hat den Vorteil, dauerhaft, also auch für künftige Kreistagsmitglieder zu gelten.

Anders ist es bei Bediensteten. Sie können nach Maßgabe der bestehenden Rechtsvorschriften überprüft werden (§ 21 Abs. 1 Nr. 6 d StUG). Für den Landkreis ist § 57 Abs. 1 Landkreisordnung die maßgebliche Rechtsvorschrift. Danach sind „geeignete Bedienstete einzustellen“. Aus Art. 119 SächsVerf ergibt sich, dass zur Eignungsprüfung auch die Stasi-Überprüfung gehört. § 49 Abs. 4 der SächsLKrO legt fest, dass der Landrat oberste Dienstbehörde der Bediensteten ist. Er überprüft in dieser Eigenschaft die Bediensteten der Landkreisverwaltung.

Der Kreistag bestimmt für sich selbst in der Hauptsatzung, in welchem Umfang er bei Personalmaßnahmen mitwirkt oder inwieweit er diese vollständig auf den Landrat überträgt. Im Zuge dieser Mitwirkung erhält er Einblick in die Personalakte und damit auch in das Ergebnis der Überprüfung. Aber er initiiert weder die Überprüfung der Bediensteten noch wirkt er bei ihr mit, da er nicht oberste Dienstbehörde der Kreisverwaltungsbediensteten ist. Für eine generelle Mitwirkung des Bewertungsausschusses - auch beratender Art - ist also kein Raum. Höchstens für die Bediensteten, bei denen er sich z. B. nach der Hauptsatzung eine Mitwirkung für Personalmaßnahmen vorbehält, könnte im Zuge dieser Mitwirkung die Einsicht in den Personalakteinteil „Stasi-Überprüfung“ durch den Bewertungsausschuss erfolgen.

Die Alternativen wären also:
- Verzicht auf Mitarbeiterbewertung durch den Kreistag oder
- Aufführung der Aufgabe „Einsichtnahme in die Stasi-Überprüfungsakte bei einer Mitwirkung in Personalangelegenheiten“ mit Verweis und Begrenzung auf den Personenkreis in der Hauptsatzung, für den sich der Kreistag eine Mitwirkung vorbehält.

Der Vorteil der zweiten Variante wäre, dass bei einer Mitwirkung in Personalangelegenheiten nicht alle Kreisräte den ihnen ansonsten zustehenden Einblick in diesen Teil der Akten bekämen.

Bei einer Regelung der Einsichtnahme von Kreisräten in ihr eigenes Überprüfungsergebnis innerhalb der Geschäftsordnung des Bewertungsausschusses sind die entsprechenden Regelungen des Stasi-Unterlagengesetzes, insbesondere § 16, zu beachten, die keine Einsichtnahme eines Täters in die Teile seiner Täterakte vorsehen, die Opferdaten enthalten.

Ich weise auch noch einmal darauf hin, dass Mitglieder des Berwertungsausschusses einem strengen Schweigegebot über die ihnen zur Kenntnis gelangten Daten unterliegen. Da liegt manches im Argen.

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Statistikgeheimnis für kommunale Wirtschaftsunternehmen?

Das Statistikgeheimnis ist älter als das im Zusammenhang mit der Einführung der elektronischen Datenverarbeitung in die Verwaltung entdeckte Datenschutzrecht. Das Statistikgeheimnis schützt seit alters her denjenigen, dessen Daten für Zwecke der amtlichen Statistik verarbeitet werden, vor allem vor einer Bekanntgabe durch die Statistikbehörde nach außen. In Grenzbereichen geht das Statistikgeheimnis über das auf der Anerkennung eines aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG herzuleitenden Grundrechtes auf informationelle Selbstbestimmung (Art. 33 SächsVerf) beruhende allgemeine Datenschutzrecht hinaus: Es schützt Verstorbene (eine zeitliche Grenze dürfte in praktischen Ergebnis nur durch das Archivrecht gesetzt sein!), und es schützt auch juristische Personen. (Am Rande: Das Statistikrecht geht hier nicht nur weiter als die [in Art. 33 SächsVerf festgeschriebene] herschende Meinung zum Grundrecht auf informationelle Selbstbestimmung [vgl. Simitis-Dammann Rdnr. 17 zu § 3 BDSG] und die entsprechenden gesetzlichen Regelungen [etwa § 3 Abs. 1 SächsDSG, § 3 Abs. 1 BDSG] mit ihrer ausdrücklichen Beschränkung auf natürliche Personen, nein, das Statistikrecht *ist* hier weiter.)
Die Grenzen dieses Schutzes, den das gesetzliche Statistikgeheimnis juristischen Personen gewährt, zeigen, dass es auch beim Statistikgeheimnis um ein Grundrecht geht. Denn die Grenzen des Statistikgeheimnisses sind, eben gerade wie beim Anwendungsbereich der Grundrechte, dort erreicht, wo hinter der juristischen Person der Staat selbst – richtiger gesagt die öffentliche Gewalt – steht.

Auf diese Rechtslage war eine „Wohnungsgesellschaft“ hinzuweisen, die in der Rechtsform der GmbH betrieben wird und deren Geschäftsanteile ausschließlich von einer kreisangehörigen sächsischen Kleinstadt und zwei kleineren Nachbargemeinden gehalten werden.
Die GmbH hatte sich an mich gewandt, weil sie vom Kommunalamt des Landkreises aufgefordert worden war, zum ihrem laut Mitteilungen des StaLA bestehenden, hohen und weiter steigenden Schuldenstand Stellung zu nehmen.

Auskunftspflichtig war die Wohnungsgesellschaft gegenüber dem StaLA, wie übrigens auch Bund und Länder, nach § 5 Nr. 1 des *Gesetzes über die Statistiken der öffentlichen Finanzen und des Personals im öffentlichen Dienst* (Finanz- und Personalstatistikgesetz - FPStatG - in der Fassung der Bekanntmachung vom 22. März 2000, BGBl. I S. 206) zur *Statistik über die Schulden und Bürgschaften;* hinzu kam die nach § 3 Abs. 7 desselben Gesetzes bestehende Berichtspflicht zur *Statistik über die Jahresabschlüsse.* Unter die Auskunftspflichtigen fiel die Wohnungsgesellschaft deswegen, weil bei ihr die Voraussetzungen des § 2 Abs. 1 Nr. 10, Abs. 3 Satz 1 FPStatG erfüllt sind: Staatliche und kommunale Fonds, Einrichtungen und wirtschaftliche Unternehmen sind auskunftspflichtig, vorausgesetzt, dass Bund, Länder, Gemeinden oder Zweckverbände unmittelbar oder mittelbar mehr als 50 vom Hundert des Nennkapitals oder des Stimmrechtes innehaben. Für solche - auskunftspflichtigen - sogenannten Erhebungseinheiten erlaubt § 15 FPStatG die *Veröffentlichung der Ergebnisse auf der Ebene der Erhebungseinheit,* also die Veröffentlichung

der Merkmalsausprägung (hier zum Beispiel *Schulden in Höhe von 51,5 Millionen DM*) mit Nennung des Namens der juristischen Person. Dies ist eine Ausnahme vom allgemeinen Statistikgeheimnis gemäß § 16 Abs. 1 Satz 1 BStatG. Ihr Sinn ist klar: Sogar die Öffentlichkeit, nicht nur die Aufsichtsbehörde, soll wissen, wieviel Schulden zum Beispiel der Bund oder eine Stadt oder eben deren Gesellschaften oder Betriebe haben. Datenschutz gibt es insoweit nicht, denn es gibt insoweit keinen Grundrechtsschutz (und auch kein in der freiheitlichen Demokratie legitimes Staatsgeheimnis). Ziel der Finanzstatistik ist es gerade, eine umfassende und lückenlose Darstellung der öffentlichen Finanzen zu gewährleisten. Ein zuverlässiges Gesamtbild der Finanzen aller öffentlichen Haushalte muss aber gerade auch diejenigen Einrichtungen erfassen, die durch die Ausgliederung von Aufgabenfeldern aus den Haushalten der Gebietskörperschaften entstehen.

5.7.2 Daten-Direktlieferung im Rahmen des § 19 Abs. 5 SächsStatG; Datennutzungserlaubnis als implizite Datenerhebungserlaubnis

Bei dem unten in Abschnitt 13.1 im Einzelnen dargestellten Adressmittlungsverfahren sollte das StaLA mithelfen: Es sollte den Familiengerichten die Arbeit dadurch erleichtern, dass es die Aktenzeichen derjenigen Scheidungsverfahren, für welche ein Forschungsvorhaben mit Adressmittlung stattfinden sollte, aus den im Rahmen der *Justizgeschäftsstatistik für Familiensachen* vorhandenen Unterlagen heraussuchte. Konkret sollte dies dadurch geschehen, dass aus den von den Gerichten ausgefüllten und dem StaLA überlassenen sog. Zählkarten entnommen werden sollte, in welchen Fällen die vom Forschungsinstitut aufgestellten Kriterien für den Umfang des zu befragenden Personenkreises erfüllt waren.
Es leuchtete ein, dass auf diese Weise die Aktenzeichen der einschlägigen Verfahren mit erheblich weniger Aufwand - und namentlich auch erheblich weniger geistiger Aufnahme personenbezogener Daten - würden gefunden werden können als im Wege einer Durchsicht der Akten selbst. (Vorausgesetzt war, dass die Gerichte selbst keine Durchschriften der von ihnen ausgefüllten Zählkarten haben.)

Die betreffenden Daten auf den Zählkarten sind nicht frei von Personenbezug, sondern einer über das Aktenzeichen bestimmbaren natürlichen Person zuzuordnen, also personenbezogen im Sinne von § 3 Abs. 1 i. V. m. Abs. 2 Nr. 4 SächsDSG. Diese Daten - „Einzelangaben“ im Sinne des Statistikrechtes - sollten dann durch das StaLA zu einem anderen Zweck als zur Durchführung einer gesetzlich angeordneten oder erlaubten (§ 7 Abs. 1, Abs. 2 SächsStatG) Statistik verarbeitet werden.

Als Erlaubnis des betreffenden Datenverarbeitungsvorganges kam am ehesten § 19 Abs. 5 SächsStatG in Betracht (die gleichbedeutende Vorschrift des § 16 Abs. 6 BStatG konnte hier vernachlässigt werden). Es handelt sich um die Erlaubnis, Einzelangaben an Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung zu übermitteln, sofern die Bediensteten des Empfängers der im öffentlichen Dienst üblichen strafbewehrten Verschwiegenheitspflicht unterliegen und die Angaben in einem Maße faktisch anonymisiert sind, dass sie nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft identifizierbaren Personen zugeordnet werden können. Die Übermittlung an Gerichte wird von der Vorschrift nun aber eigentlich nicht erfasst, weil Gerichte ja keine Einrichtung mit der Aufgabe

unabhängiger wissenschaftlicher Forschungen sind. Die Vorschrift hätte es im vorliegenden Fall jedoch erlaubt, die Aktenzeichen - um mehr ging es ja nicht - an das Forschungsinstitut zu übermitteln, welches diese dann dem jeweiligen Familiengericht hätte übermitteln dürfen. Und das Gericht hätte die Aktenzeichen auch erheben dürfen, weil es sie auch erlaubterweise gemäß § 12 Abs. 2 Nr. 4 SächsDSG (dazu wiederum unten unter 13.1) aus den ihm vorliegenden Unterlagen hätte heraussuchen dürfen.
Wenn dem so war, dann musste § 19 Abs. 5 SächsStatG auch als Erlaubnis verstanden werden dürfen, stattdessen eine *Daten-Direktlieferung* vorzunehmen, also den Umweg über das Forschungsinstitut einzusparen. Denn diese Datenübermittlung im Wege der Direktlieferung stellte einen geringeren Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar als die von der Vorschrift unmittelbar erlaubte Datenübermittlung über die Zwischenstation des Forschungsinstitutes.

Ob man ersatzweise in solchen Fällen auch argumentieren dürfte, dass im Falle der Statistik im Verwaltungsvollzug - die Justizgeschäftsstatistik für Familiensachen ist eine solche - die Datenrücklieferung an die öffentliche Stelle, in deren Geschäftsgang die Daten angefallen sind, ohnehin erlaubt sein müsste, sofern diese Stelle die Daten erheben dürfte, konnte dahinstehen.
SMJus und StaLA hatten gegen diese Begründung für eine Erlaubtheit der arbeitssparenden Hilfestellung seitens des StaLA erwartungsgemäß keine Einwände.

5.7.3 Statistik des SMS zur sog. „Jugendzahnpflege“ in Kindertageseinrichtungen: Sekundärstatistik mit Doppelfehler

Das Gesundheitsamt der Stadt Dresden untersuchte, wie sich auf eine Eingabe hin herausstellte, in Gestalt des sog. Jugendzahnärztlichen Dienstes in den Dresdner Kindertagesstätten die Gebisse der Kinder. Die Untersuchung mündete in eine „Mitteilung an die Eltern“, in der - je nachdem - empfohlen wurde, zahnärztliche Kontrolle, Beratung oder auch Behandlung in Anspruch zu nehmen, verbunden etwa mit der Angabe, dass dies wegen Karies oder beim Kieferorthopäden geschehen solle.

Bei der Untersuchung wurden aber mehr Daten erhoben, als erforderlich waren, um durch Ankreuzen in dem vorgedruckten Empfehlungs-Katalog die jeweils angemessene Empfehlung aussprechen zu können. Diese zusätzlichen Daten dienten der Durchführung einer Statistik. Mittels eines Formulares wurden folgende Daten erhoben: Landkreis/Kreisfreie Stadt, Ort, Name und Anschrift der „Kindereinrichtung“, Gruppe und Gruppengröße, Schuljahr, erhebender Zahnarzt, Namen und Vornamen der einzelnen Kinder sowie deren Geschlecht, Geburtsmonat und -jahr und eine Vielzahl ins einzelne gehender Feststellungen zum Gebisszustand, wie z. B. „unterer Frontzahnvorbiss“, „vereinzelte Zahnbeläge“ oder „Anzahl der gefüllten Zähne des Milch-Gebisses“.
Das SMS erhielt vom Gesundheitsamt die ausgefüllten Vordrucke, wobei die Namen der Kinder geschwärzt wurden.

Die Untersuchung war eine Erhebung personenbezogener Daten; die Nutzung der Erkenntnisse für die einzelne Empfehlung wie auch die Nutzung für die Statistik waren Weiterverarbeitungen dieser Daten.

Eine Einwilligung der Sorgeberechtigten in die Untersuchung hatte man nicht eingeholt, weder im Hinblick auf die Erarbeitung der Empfehlung noch im Hinblick auf die Durchführung der Statistik.

Insoweit die Datenerhebung und -nutzung über das hinausging, was für die *Empfehlung* nötig war (dazu unten Abschnitt 10.1.2), wäre sie aus statistikrechtlichen Gründen auch dann rechtswidrig gewesen, wenn die Sorgeberechtigten auch insoweit - also hinsichtlich dessen, was die Statistiker „Erhebungsprogramm“ nennen, und in den statistischen Zweck - eingewilligt hätten. Dieser die Erarbeitung der *Empfehlung* überschießende Teil der Untersuchung hatte ausschließlich statistische Zwecke. Eine Einwilligung ist für die Frage der Rechtmäßigkeit der Datenerhebung insoweit unbeachtlich. Denn nach sächsischem Statistikrecht - dies ist in manchen Bundesländern anders - bedarf die Erhebung und Weiterverarbeitung personenbezogener und ähnlicher Daten zu statistischen Zwecken auch dann einer besonderen Rechtsvorschrift als Rechtsgrundlage, wenn die Statistik ohne Auskunftspflicht, d. h. also mit Einwilligung der Betroffenen durchgeführt wird (vgl. §§ 6 Abs. 3 Satz 1, Abs. 6 Satz 2, 11 Abs. 1 SächsStatG).

Unterstellt, diejenigen Daten, die nötig waren, um die für die *Empfehlungen* notwendigen Feststellungen zu treffen, seien rechtmäßig erhoben worden (dazu, wie schon erwähnt, unten in Abschnitt 10.1. 2), dann wären diese Daten im Verwaltungsvollzug angefallen. Gemäß § 7 Abs. 1 SächsStatG hätte das Gesundheitsamt und die ihm übergeordneten Stellen, also RP und SMS, die Daten zur Durchführung einer Statistik verwenden dürfen, unter Einhaltung des Gebotes der frühestmöglichen statistikunschädlichen Anonymisierung (§ 1 Abs. 2, a. E., SächsStatG). Aber es hätten keine Daten in die Statistik Eingang finden dürfen, deren Erhebung für das Aussprechen der Empfehlungen nicht benötigt worden wäre.

Es ist mir wohl gelungen, das SMS von seiner Auffassung abzubringen, dass die Aufgabenzuweisungen in § 11 Abs. 1 Satz 2 Nr. 2 SächsGDG i. V. m. § 6 Abs. 2 Satz 2 SächsKitaG oder doch § 21 SGB V (vgl. Absatz 2 und 3 der Vorschrift: Dokumentation gerade nicht kinderbezogen!) eine hinreichende Erlaubnis für die Erhebung und Weiterverarbeitung der Daten zu Statistikzwecken darstellen.
Es ist mir wohl auch gelungen, das SMS davon zu überzeugen, dass ärztliches Standesrecht nicht ohne weiteres die Brücke von der Datenverarbeitung zu Empfehlungszwecken mit kleinem Erhebungsprogramm zur landesweiten Statistik mit großem Erhebungsprogramm sein kann. Berufsrechtliche Dokumentationspflichten begründen für sich genommen noch keine Datenverarbeitungsbefugnisse ärztlicher Amtsträger gegenüber Privaten: Wenn sie auch von starkem Einfluss auf den Maßstab sein dürften, der an die übliche ordnungsgemäße Dokumentation der Grundlage derartiger von Ärzten zu verantwortender Entscheidungen - oder doch jedenfalls Äußerungen - der Verwaltung anzulegen ist, so darf ärztliches Standesrecht doch nicht herangezogen werden, um das Erhebungsprogramm, das als Dokumentationshintergrund der den Eltern ausgesprochenen Empfehlungen dient, so auszudehnen, wie man es für die Auswertung zugunsten der Statistik gerne hätte.

Einigkeit hat mit dem SMS darüber hergestellt werden können, dass es im Wesentlichen nur zwei Möglichkeiten gibt, die bisherige Praxis - oder doch zumindest etwas, was ihr nahe kommt - auf die erforderliche rechtliche Grundlage zu stellen:

Die erste Möglichkeit wäre die Schaffung einer Vorschrift im Range des Landesgesetzes über eine Zahn-Zustands-Statistik betreffend alle Kindergarten-Kinder. Dies wäre eine Primärstatistik. Von dem Versuch, dies zu verwirklichen, habe ich jedoch abraten müssen. Dieser Weg ist möglicherweise überhaupt nicht gangbar, denn es gilt der Grundsatz der Abschottung der amtlichen Statistik vom (übrigen) Verwaltungsvollzug. Aus datenschutzrechtlichen Gründen, die Verfassungsrang haben, darf eine amtliche Statistik, sofern sie Primärstatistik ist, nur durch besondere Statistik-Behörden (Statistisches Bundesamt, Statistisches Landesamt, kommunale Statistikstellen) durchgeführt werden. Dies müsste auch im vorliegenden Falle gelten, in welchem die Ärzte an Gesundheitswesen-Vollzug nicht mehr leisten, als begründete Empfehlungen auszusprechen, sich in - in der Regel privatwirtschaftlich organisierte - zahnärztliche Behandlung zu begeben. Diese gewissermaßen schwache, nämlich ausschließlich beobachtende und empfehlende Tätigkeit ist eine der amtlichen Statistik vergleichsweise ähnliche Form des Verwaltungsvollzuges, sie ist aber gleichwohl als Tätigkeit zu nicht-statistischen Zwecken doch noch genügend Verwaltungsvollzug, um nicht in der Durchführung mit der amtlichen Primärstatistik verbunden werden zu dürfen. Kurz: Es handelt sich um zwei verschiedene Verwaltungszwecke, der datenschutzrechtliche Grundsatz der Zweckbindung kommt zum Tragen und zwingt zur Trennung von schulärztlichen Daten und Statistikdaten von Anfang an.

Daher müsste eine solche Primärstatistik letztlich wohl durchgeführt werden von der zuständigen Statistikstelle (kommunale Statistikstelle der kreisfreien Stadt oder des Landkreises), und von Erhebungsbeauftragten, die natürlich ausgebildete Zahnmediziner sein müssten, die ausschließlich für das Statistische Landesamt oder für eine kommunale Statistikstelle arbeiteten und die keinerlei Empfehlungen zur Zahnbehandlung aussprechen dürften. Dies mag zwar etwas haarspalterisch erscheinen, es zeigt aber im Grunde nur, dass eine staatliche Tätigkeit, die sich darin erschöpft, den Rat zu erteilen, Dienste Privater in Anspruch zu nehmen, ein Fremdkörper im System des Staatshandelns ist. Die Zeiten der allumsorgenden Staatstätigkeit sind - Gott sei Dank - vorbei.

Außerdem ist aus verfassungsrechtlichen Gründen in diesem Fall die Frage zu stellen, ob nicht eine kleine Stichprobe, statt der gegenwärtigen rund 90-prozentigen Erfassung sämtlicher Kinder, ausreicht, um genügend über die Zahngesundheit der Vorschulkinder zu wissen. Dafür dürfte einiges sprechen, zumal unklar und völlig offen geblieben ist, was denn aufgrund der umfänglichen Statistik tatsächlich geschieht, um den Zustand kindlicher Gebisse zu verbessern. Man könnte wirklich darüber nachdenken, ob die Statistik - in Teilen - l'art pour l'art war.

Bleibt die andere Möglichkeit - und für diese hat sich das SMS inzwischen zumindest fürs Erste entschieden: *Herstellung einer Kongruenz zwischen dem Verwaltungsvollzugszweck „Empfehlung zahnärztlicher Behandlung" und dem statistischen Erhebungsprogramm*.

Die Feststellungen zum Zweck der Beratung sind verfeinert worden, d. h. der Empfehlungs-Katalog ist jetzt inhaltlich vielfältiger, also umfangreicher; zugleich ist das - damit jetzt identische, kongruente - Erhebungsprogramm für die Statistik nunmehr gegenüber vorher bedeutend verkleinert. Erhoben und weiterverarbeitet wird nunmehr ein Datensatz mittlerer Größe, der im Umfang zwischen den bis dahin für Beratungszwecke und für Statistikzwecke zugrunde gelegten Erhebungsprogrammen liegt.

Das Ganze findet nunmehr auf Einwilligungsgrundlage statt.

Man könnte schließlich noch die Frage stellen, ob die Statistik im Verwaltungsvollzug (nach § 7 Abs. 1 SächsStatG) durchgeführt werden darf auf der Grundlage eines Verwaltungsvollzuges, der flächendeckend ausschließlich einwilligungsabhängig durchgeführt wird. Wäre es wohl - auch im Hinblick auf § 12 Abs. 3 Satz 1 SächsDSG - zu streng, hierin eine Umgehung der bereits genannten Regel zu sehen, welche für Primärstatistiken auf freiwilliger Grundlage eine Rechtsvorschrift verlangt?

5.8 Archivwesen

5.8.1 Amtsträger-Daten im Archivrecht

Ein Petent war 1956, in der Zeit nach dem Aufstand in Ungarn, auf Antrag des „Pädagogischen Rates der Friedrich-Engels-Oberschule“ in X sowie des „Elternbeirates“ vom Minister für Volksbildung von allen Oberschulen der Deutschen Demokratischen Republik ausgeschlossen, weil er, wie es in dem Beschluss des *Pädagogischen Rates* hieß, den „kapitalistischen Hetzsendern Gehör geschenkt und diese schädlichen Gerüchte weiterverbreitet“ habe. Er selbst hatte, trotz mehrfachen Verlangens, nichts Schriftliches bekommen; der Direktor hatte ihm lediglich mündlich außerhalb des Unterrichts getane Äußerungen der Sympathie mit den ungarischen *Konterrevolutionären* statt mit den *fortschrittlichen Kräften* vorgeworfen, die Zugehörigkeit zur *Jungen Gemeinde* angesprochen sowie sich auf Einwände darauf beschränkt, zu erklären, was *ihm vorzuwerfen sei, stehe fest*.

An mich wandte er sich nun, weil ihm das Kreisarchiv auf seinen Antrag hin den Text des Sitzungsprotokolls des *Pädagogischen Rates* nur mit - pauschal als *datenschutzrechtlich geboten* bezeichneten - Schwärzungen sämtlicher Namen (außer seinem eigenen, versteht sich) zugänglich gemacht hatte.
Zugleich wandte sich auch das Landratsamt an mich, nachdem es durch die Aufforderung des Petenten, die datenschutzrechtlichen Vorschriften, welche die Grundlage der Schwärzungen seien, doch bitte zu nennen, in Verlegenheit gebracht worden war. (Bei aller Kritik sollte man im Hinblick auf § 35 SächsDSG freilich auch die Leistung der Archivverwaltung würdigen: Die Unterlagen waren vorhanden, ja auch greifbar! Das bedeutet: Der Wunsch des Petenten, zu erfahren, wer ihm was seinerzeit vorgeworfen hat, was die Gründe oder auch Hintergründe waren, war erfüllbar!)

Mit seiner Beschwerde, dass es *die Perversion des Datenschutzes wäre*, wenn die Behörde recht hätte, lag der Petent richtiger, als es auf den ersten Blick erscheinen mag. Denn er machte mit seinem Begehren den datenschutzrechtlichen Auskunftsanspruch dessen geltend, der wissen will, was die Behörde über ihn gespeichert hat (§ 17 SächsDSG - hier in der spezialgesetzlichen Gestalt des § 6 Abs. 1 SächsArchivG). Und dann kann es in der Tat eine Verletzung gerade der Datenschutzrechte des Auskunftsbegehrenden sein, wenn man ihm um des Datenschutzes zugunsten Dritter willen deren Äußerungen über ihn insofern vorenthält, als man die Urheber dieser Äußerungen ihm durch Schwärzungen unkenntlich macht.

Worauf es ankam, war also: Genossen die Mitglieder des *Pädagogischen Rates* und des *Elternbeirates* für die von ihnen in den Sitzungen seinerzeit - gemäß Protokoll (Gegendarstellung ist möglich: § 6 Abs. 2 SächsArchivG!) - getanen Äußerungen den Schutz des Grundrechtes auf informationelle Selbstbestimmung? Rechtstechnisch handelte es sich sozusagen um eine doppelte Fragestellung: Gab es für die Schwärzungen eine Rechtsgrundlage - als Einschränkung des schon genannten Auskunftsanspruches des Petenten? Und zugleich: Gab es eine Rechtsgrundlage für die Offenlegung der Namen der betreffenden Sitzungsteilnehmer - als Ausnahme von den als Übermittlungsverbot aufzufassenden persönlichkeitsrechtsschützenden Schutzfristen des § 10 Abs. 1 Satz 3 und 4 SächsArchivG (bis 10 Jahre nach Tod, ersatzweise 100 Jahre nach der Geburt)?

Die Antwort war dem Gesetz leicht zu entnehmen: Gemäß § 10 Abs. 2 Satz 3, 1. Halbs. SächsArchivG gelten die dem Persönlichkeitsschutz dienenden Schutzfristen (des § 10 Abs. l Satz 3 und 4 SächsArchivG) nicht für *Amtsträger in Ausübung ihrer Ämter*. Der 2. Halbs. des § 10 Abs. 2 Satz 3 SächsArchivG gilt für die vielen öffentlichen Einrichtungen aus DDR-Zeiten (unabhängig davon, ob es dafür heutzutage noch Entsprechungen gibt): Wie für die Mitglieder der *Schulkonferenz* (§ 43 SchulG) oder des *Elternrates* (§ 47 SchulG) gibt es auch für Mitglieder des früheren *Pädagogischen Rates* und des früheren *Elternbeirates* keinen Datenschutz, soweit es um deren Handeln in diesen Gremien geht. (Übrigens: Soweit es für Einrichtungen in der DDR auch heute noch Entsprechungen gibt, hat der Gesetzestext lediglich klarstellende Funktion, wie das Beispiel dies zeigt.) Die Betreffenden üben insoweit ein von der öffentlichen Gewalt verliehenes oder doch jedenfalls eingerichtetes Amt aus; im Falle der Elternvertreter ist es ein Wahl- und Ehrenamt. Die Betreffenden sind insoweit „Obrigkeit“. Ihrem Handeln den Schutz des Grundrechtes auf informationelle Selbstbestimmung zu gewähren hieße, Handeln der öffentlichen Gewalt der Kritik und Kontrolle zu entziehen. Das aber ist gerade nicht der Sinn des Grundrechtes, welches dafür sorgen soll, dass der Privatmensch wissen können soll, was die Obrigkeit in welchem Zusammenhang über ihn weiß. Und die Obrigkeit ist nicht etwa nur eine Rechtsfigur, sie besteht aus Menschen, die insofern öffentlich handeln und es ertragen müssen, dass ihr Handeln veröffentlicht wird. So will es die Grundrechtslehre.

Die Namen dieser Amtsträger, also der Lehrer und Elternvertreter, mussten daher nicht geschwärzt werden, weil die Schutzfristen als Übermittlungsverbote nicht eingriffen, und sie durften auch nicht geschwärzt werden, weil für die darin liegende Einschränkung des Auskunftsanspruchs des Petenten keine Grundlage bestand.

Zu schwärzen waren hingegen die Namen der neben dem Petenten als politisch unzuverlässig genannten anderen Schüler (sofern nicht zufällig bekannt war, dass diese schon länger als 10 Jahr tot waren, § 10 Abs. 1 Satz 3 SächsArchivG); das gilt höchstwahrscheinlich auch für denjenigen unter ihnen, der FDJ-Sekretär war (und den es laut Protokoll nach Auffassung des Direktors zu *entlarven* galt): Vermutlich hatte er seine oppositionelle Haltung gerade nicht in seiner amtlichen Eigenschaft betätigt; er war wohl „privat" mutig gewesen.

Der Fall zeigt: Die Tätigkeit der Archivare ist datenschutzrechtlich anspruchsvoll; und die Verfassung sorgt für Gerechtigkeit.

5.8.2 Kein Ausweg bei Behinderung des Zuganges der zeitgeschichtlichen Forschung zu noch nicht archivierten Altdaten: § 299 Abs. 2 ZPO

Zum Fall 7/5.8.1 und 7/5.8.4 hat das SMJus einen Ausweg darin gesehen, dass die Doktorandin Zugang zu den von der Justiz aufbewahrten Akten aus Verfahren der DDR-Arbeitsgerichtsbarkeit auf der Grundlage des § 299 Abs. 2 ZPO erhalten könne, der besagt, dass das Gericht *dritten Personen ohne Einwilligung der Parteien die Einsicht in die Akten nur gestatten darf, wenn jene ein rechtliches Interesse glaubhaft machen*.

Dazu habe ich vorgetragen:

1. Nach § 299 Abs. 2 ZPO ist Voraussetzung der Einsichtsgewährung, als einer Übermittlung personenbezogener Daten, das (glaubhaft gemachte) *rechtliche Interesse* dessen, der die Einsicht erhalten soll, also des Übermittlungsempfängers.
   Ein (glaubhaft gemachtes oder nachgewiesenes) *rechtliches Interesse* ist nach vielen Vorschriften Voraussetzung einer durch Einsichtsgewährung stattfindenden Datenübermittlung durch Gerichte (z. B. §§ 1953 Abs. 3 Satz 2, 2010, 2081 Abs. 2 Satz 2, 2146, 2228, 2384 Abs. 2 BGB; vgl. ferner § 810 BGB); in Verfahrensordnungen wird derselbe Ausdruck zur begrifflichen Beschreibung der Voraussetzung prozessualer Gestaltungsbefugnisse (§§ 66 Abs. 1, 256 ZPO, 57 FGG) wie auch der Gewährung von Akteneinsicht, eben im Falle des § 299 ZPO, benutzt.
   Was *rechtliches Interesse* im Sinne von § 299 Abs. 2 ZPO ist, hat die Rechtsprechung nach und nach genauer bestimmt. Zunächst haben RG und BGH als *Mindestanforderungen* (BGHZ 4, 323, 325), die durch Verwendung des Ausdruckes *rechtliches Interesse* gestellt werden - allgemein für diese Vorschriften, aber namentlich auch im Hinblick auf § 299 Abs. 2 ZPO - bestimmt, dass
   > *das rechtliche Interesse sich stets unmittelbar [also nicht bloß als Reflex] aus der Rechtsordnung selbst ergeben muss,* also *das rechtliche Interesse ein auf Rechtsnormen beruhendes oder durch solche geregeltes, gegenwärtig bestehendes Verhältnis einer Person zu einer anderen Person oder zu einer Sache voraussetzt* (BGH a.a.O. S. 324/325). Das bedeutet, dass *ein bloß [mittelbares] wirtschaftliches oder gesellschaftliches Interesse kein rechtliches Interesse sein kann* (BGH a.a.O. S. 325). Dabei ist *der Begriff des rechtlichen Interesses enger ist als der des 'berechtigten Interesses'*, der gleichfalls vom Gesetzgeber als Voraussetzung von Akteneinsichtsgewährung durch Gerichte verwendet wor-

den ist (§ 34 Abs. 1 Satz 1 FGG), aber später dann auch in die Datenschutzgesetze Eingang gefunden hat (z. B. § 16 Abs. 1 Nr. 2 BDSG, § 15 Abs. 1 Nr. 2 SächsDSG).

Diese Ausführungen des BGH liegen weiterhin der neueren Rechtsprechung zugrunde, sei es in der Sache (KG NJW 1988, 1738, 1739 oben), sei es expressis verbis (z. B. OLG Hamm NJW-RR 1997, 1489, 1490), sind aber von ihr präzisiert worden, und zwar dahin, dass

Rechte des Dritten (=Einsichtbegehrenden) möglicherweise *durch den Akten· inhalt berührt sein müssen* (OLG Hamm NJW 1989, 533),

was damit erläutert wird, dass

auf Seiten des Dritten *ein rechtlicher Bezug zum Streitstoff der Akten* bestehen muss (OLG Hamm a.a.O. und KG NJW 1988, 1738, 1739; ebenso Zöller/ Greger, 21. A. 1999, Rdnr. 6 zu § 299 ZPO).

Dafür hat unlängst das OLG Hamm (NJW-RR 1997, 1489 ff.) die noch prägnantere Formel gefunden, dass

der eigene Rechtskreis des Dritten unmittelbar vom Verfahrensgegenstand berührt sein muss (zustimmend Zöller/Greger a.a.O.).

Dieselbe OLG-Entscheidung hebt hervor, dass

mit Rücksicht auf das verfassungsrechtlich gewährleistete Recht auf informationelle Selbstbestimmung *an das Vorliegen eines rechtlichen Interesses i. S. d. § 299 Abs. 2 ZPO hohe Anforderungen zu stellen sind* (a.a.O.).

Was demnach mit dem *rechtlichen Interesse* im Sinne von § 299 Abs. 2 ZPO gemeint ist, wird noch deutlicher, wenn man eine vom Bayerischen Obersten Landesgericht im Hinblick auf den insoweit gleichlautenden § 61 Abs. 1 Satz 3 PStG verwendete Formulierung heranzieht:

Ein rechtliches Interesse setzt voraus, dass die Kenntnis von in den Akten enthaltenen Daten *zur Verfolgung von Rechten oder zur Abwehr von Ansprüchen erforderlich ist* (BayObLGZ 1998, 119, 121 m.w.N.; zustimmend Keidel/ Kuntze/Winkler, 14. A. 1999, Rdnr. 13 zu § 34 FGG).

Einen ähnlichen Formulierungsbestandteil verwendet die Dissertation von Brigitta Liebscher, Datenschutz bei der Datenübermittlung im Zivilverfahren, Berlin 1994, S. 104/105: *Ein rechtliches Interesse hat nur derjenige, der ein auf Rechtsnormen beruhendes gegenwärtiges Verhältnis zu einer [Prozess-]Partei hat und mit der Akteneinsicht bezweckt, eine tatsächliche Unsicherheit über ein Rechtsverhältnis zu klären, das Verhalten in rechtlich bedeutsamer Weise nach dem Ergebnis der Akteneinsicht auszurichten oder eine gesicherte Grundlage für die Verfolgung eines Anspruchs zu erhalten.*

Man könnte verdeutlichen:

Wer rechtliches Interesse am Akteninhalt hat, gestaltet nach Kenntnisnahme auf dieser Grundlage bestimmte Rechtshandlungen. Wer ein wissenschaftliches Interesse hat, gestaltet demgegenüber aufgrund der Akteneinsicht Realakte, nämlich den Text einer von ihm zu verfassenden wissenschaftlichen Abhandlung.

Vereinfacht kann man das auch so ausdrücken: Wenn der Forscher die Akten-Daten hat, verfolgt er keine eigenen unmittelbaren Rechte mehr; bei ihm erschöpft sich die Rechtsverfolgung in dem Bemühen um Datenzugang. Beim rechtlich Interessierten hingegen geht es, salopp formuliert, nach der Datenerlangung juristisch erst richtig los.

2. Nur im Schrifttum finden sich Stimmen, die in § 299 Abs. 2 ZPO eine Erlaubnis zur Akteneinsichtsgewährung auch zu Forschungszwecken - statt zu Zwecken der Rechtsverfolgung - sehen:
   Stein/Jonas/Leipold (Stand: XI/1996) beschränkt sich (Rdnr. 21 a zu § 299; ihm folgend Peglau, NJ 1993, 440, 441 m. Fn. 21) auf eine bloße Behauptung, die lediglich durch den - zutreffenden - Hinweis erweitert ist, dass die Entscheidung KG OLZ 1976, 158, 161 (= NJW 1976, 1326) eine solche Auslegung erwäge (eine Erwägung, die überdies durch die oben zitierte strenge KG-Entscheidung aus dem Jahre 1988 überholt sein dürfte).
   Auch den Ausführungen Prüttings in ZZP 106 (1993) 427 ff., 457 ist keine Begründung für eine entsprechende Auslegung des Gesetzes zu entnehmen.

3. Aus alledem folgt mit großer Eindeutigkeit, dass nach geltendem Recht die Gewährung von Akteneinsicht zu Forschungszwecken nicht durch § 299 Abs. 2 ZPO erlaubt ist.

4. Diese Auslegung von § 299 Abs. 2 ZPO gibt zugleich durchaus Raum für eine ergänzende Anwendung solcher Vorschriften aus den allgemeinen Datenschutzgesetzen, welche speziell die Erlaubnis einer Datenübermittlung zu Forschungszwecken aussprechen, z. B. eben § 15 Abs. 1 Nr. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG.
   Die Begründungen, die Prütting (a.a.O. S. 456, unter b) und Liebscher (a.a.O. S. 104) für die gegenteilige Auffassung geben, können nicht überzeugen: Prütting geht von der, wie gezeigt, falschen Voraussetzung aus, auch der Verarbeitungszweck „wissenschaftliche Forschung“ werde von der Tatbestandsvoraussetzung „rechtliches Interesse“ des § 299 Abs. 2 ZPO erfasst; Liebscher verkennt, dass nach den Grundlagen des Datenschutzrechtes der Verarbeitungszweck (hier: Zweckänderung zugunsten der wissenschaftlichen Forschung) zu den Standard-Tatbestandsvoraussetzungen von Verarbeitungserlaubnissen gehört. Gibt es nach allgemeinen und vielfach auch nach neueren spezielleren Datenschutzvorschriften Regeln über den privilegierten Zweckänderungsgrund „wissenschaftliche Forschung“, so kann man bei einem älteren und im Wesentlichen ausschließlich auf die Rechtspflege (als Datenverarbeitungs-Zweck) zugeschnittenen Gesetz wie der ZPO nicht unterstellen, es regele Zweckänderungen über den Rechtspflege-Bereich hinaus abschließend (d. h. mit Spezialitätsvorrang).
   Dies dürfte im Hinblick auf Art. 5 Abs. 3 GG auch die verfassungskonforme Auslegung des § 299 Abs. 2 ZPO in seiner Rechtssatzkonkurrenz mit Vorschriften der genannten Art sein.

   Im Übrigen bietet der datenschutzrechtliche Grundsatz der Zweckbindung (BVerfGE 65, 1, 46 f.) auch ein zusätzliches Argument für die oben dargelegte Auslegung des § 299 Abs. 2 ZPO durch die Rechtsprechung: Setzt die Vorschrift wirklich ein *rechtliches Interesse* in diesem strengen Sinne voraus, so sorgt sie nämlich dafür, dass die Zweckbindung der Daten, also die Beschränkung auf den Verarbeitungszweck ‘Rechtspflege’, gewahrt bleibt.

   Der Wortlaut des § 299 Abs. 2 ZPO wie auch seine herkömmliche und ganz

herrschende Auslegung durch die Rechtsprechung erweisen sich damit unter datenschutzrechtlichem Blickwinkel als ausgesprochen zeitgemäß.

Das SMJus hat danach nicht zu erkennen gegeben, dass es an seiner zu Lasten des Datenschutzes großzügigeren Auslegung des § 299 Abs. 2 ZPO festhalten wolle.

Vgl. auch unten 9.4.2.

5.9 Polizei

5.9.1 Anwendungshinweise des SMI zum Erlass von Aufenthaltsverboten gemäß § 21 Abs. 2 SächsPolG

Zu den polizeilichen Standardmaßnahmen gehört der Platzverweis nach § 21 Abs. 1 SächsPolG, der es der Polizei erlaubt, eine Person zur Abwendung einer Gefahr für die öffentliche Sicherheit oder Ordnung oder zur Beseitigung einer Störung vorübergehend von einem Ort zu verweisen oder ihr vorübergehend das Betreten eines Ortes zu verbieten.
Der durch die Novellierung des Polizeigesetzes des Freistaates Sachsen vom 21. Juni 1999 (SächsGVBl. S. 330) neu eingefügte Absatz 2 des § 21 ermöglicht es der Polizei jetzt auch, längerfristige Aufenthaltsverbote auszusprechen, wenn Tatsachen die Annahme rechtfertigen, dass die Person dort eine Straftat begehen oder zu ihrer Begehung beitragen wird (sog. Negativprognose).

Das SMI hat hierzu Anwendungshinweise entworfen, die mir zur Stellungnahme übersandt wurden; die darin enthaltenen „besonderen Bestimmungen zum Datenschutz für den Polizeivollzugsdienst“ fanden nicht meine uneingeschränkte Zustimmung. Zwar regelten sie sachgerecht die Voraussetzungen, unter denen personenbezogene Daten im „Polizeilichen Auskunftssystem Sachsen (PASS)“ gespeichert werden (z. B. bei Erlass eines Aufenthaltsverbotes, bei Verstoß gegen ein solches Verbot etc.). Präzisierungsbedürftig waren die Anwendungshinweise allerdings, soweit es um den weiteren Umgang mit den erhobenen Daten ging. Bloße Verweise auf ohnehin zu beachtende Vorschriften im Sächsischen Polizeigesetz erschienen mir jedenfalls zu pauschal, um die Dauer der Speicherung auf das erforderliche Maß zu beschränken und das Verfahren zur Löschung nicht mehr benötigter Daten hinreichend konkret zu regeln. Zudem galt es, spezifische Regelungen für die Fälle vorzusehen, in denen sich die dem Aufenthaltsverbot ursprünglich zugrunde gelegte Gefahr später nicht realisiert, z. B. weil die Versammlung, an deren Teilnahme ein gewaltbereiter Demonstrant durch Erlass eines Aufenthaltsverbotes rechtmäßig gehindert wird, später gar nicht stattfindet.

Das SMI hat meine Empfehlungen in einer entsprechend geänderten Fassung der Anwendungshinweise berücksichtigt:
Die Verarbeitung der Daten richtet sich nunmehr ausdrücklich nach der Errichtungsanordnung des Landeskriminalamtes für die „PASS“-Datei. Dadurch wird der Kreis der Polizeibeamten, die zur Prüfung der Negativprognose auf die hier gespeicherten Daten zugreifen dürfen, sachgerecht und effektiv begrenzt.

Nach Ablauf des Aufenthaltsverbotes, d. h. spätestens drei Monate nach seinem Erlass, entscheidet die Polizei jetzt in jedem Einzelfall über die Löschung der gespeicherten personenbezogenen Daten; Daten ohne erkennbaren Gefahrenabwehrhintergrund oder mögliche Strafrechtsrelevanz werden dann umgehend gelöscht.

Ob die modifizierten Anwendungshinweise auch in der Praxis datenschutzgerecht umgesetzt werden, werde ich noch in diesem Jahr kontrollieren.

5.9.2 Entwurf einer Verwaltungsvorschrift zum automatisierten Verfahren für Auskunftsersuchen von Sicherheitsbehörden im Bereich der Telekommunikation

Ein mir vom SMI zur Prüfung vorgelegter Entwurf einer Verwaltungsvorschrift für das automatisierte Abrufverfahren im Rahmen von Auskunftsersuchen nach § 90 TKG sah vor, dass die Polizeipräsidien den gemeinsamen Leitstellen der Feuerwehr und des Rettungsdienstes „Amtshilfe zur Erlangung von Auskünften“ gewähren sollten. Diese Regelung habe ich kritisiert, weil nach der Rechtssprechung des Bundesverfassungsgerichts „Amtshilfe“ zur Erlangung personenbezogener Daten nur zulässig ist, wenn hierdurch keine Befugnisüberschreitung der ersuchenden Stelle geschaffen wird. Jegliche personenbezogene Datenverarbeitung muss also „amtshilfefest“ sein.

§ 90 Abs. 3 TKG verleiht der Regulierungsbehörde lediglich die Befugnis, Auskünfte aus den Kundendateien der Verpflichteten (dies sind die Netzbetreiber) automatisiert abzurufen und den Polizeibehörden für Zwecke der Gefahrenabwehr zu übermitteln, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Dies bedeutet, dass eine Weiterleitung der durch die Polizeibehörden abgerufenen Daten an die Leitstellen nur dann zulässig ist, wenn der zugrunde liegende Sachverhalt auch Anlass für die Polizeibehörde wäre, im Wege der Gefahrenabwehr tätig zu werden (polizeiliche Aufgabenerfüllung); es müsste also Anlassidentität bestehen.

Ich habe das SMI gebeten, diese Überlegung bei der weiteren Gestaltung der Verwaltungsvorschrift zu beachten und im Interesse der Klarheit statt des Begriffes „Amtshilfe“ den Begriff „Datenübermittlung“ zu verwenden.

5.9.3 LKA fordert Apotheker zur Offenbarung geschützter Daten auf

Mit einer „Warnmeldung“ wandte sich das LKA an die Sächsische Landesapothekerkammer: Das Amt bat die Apotheker um „Präventivmaßnahmen“ gegenüber einer Person, der vorgeworfen wurde, unter Angabe falscher Personalien bei Ärzten Rezepte für Betäubungsmittel erschlichen zu haben.

Die „Warnmeldung“ enthielt die biographischen Daten sowie die der betroffenen Person zur Last gelegten Tatvorwürfe und schloss mit der Frage „Ist o. g. Beschuldigter bereits in Erscheinung getreten?“

Diese Art polizeilicher Datenverarbeitung ist mit zentralen Inhalten unserer Rechts-

ordnung nicht zu vereinbaren. Messerscharf könnte jemand behaupten, hier sei eine Anstiftung zum Geheimnisbruch nach § 203 StGB im Spiel. Denn die „Warnmeldung“ - wenn sie von den sächsischen Apothekern befolgt worden wäre - hätte bewirkt, dass die Adressaten ihre nach § 203 StGB strafbewehrte Pflicht verletzen, die ihnen als Apotheker anvertrauten Geheimnisse zu wahren. Auch derjenige, der den Träger der Schweigepflicht betrügt oder belügt, genießt grundsätzlich den Schutz, den die Schweigepflicht bietet. Bereits der bloße Umstand, dass sich ein Patient zum Zweck der Medikamentierung durch Vorlage einer ärztlichen Verordnung anvertraut, ist ein im Sinne des § 203 Abs. 1 StGB „anvertrautes“ Geheimnis. Dieses - dem Arztgeheimnis entsprechende - Apothekergeheimnis darf nur nach einer wirksam erklärten Einwilligung des Patienten oder bei Vorliegen einer gesetzlichen Offenbarungsbefugnis oder unter den Voraussetzungen eines rechtfertigenden Notstandes (§ 34 StGB) durchbrochen werden. Wie ich bereits in einem ähnlich gelagerten Fall in 3/5.9.7 erläutert habe, kann die Durchbrechung dieses Geheimnisschutzes zu polizeilichen Zwecken nur bei besonders schweren und den Rechtsfrieden nachhaltig störenden Verbrechen (z. B. wiederholte Begehung schwerster Delikte, terroristische Gewalttaten) gerechtfertigt sein. Ferner darf z. B. der Apotheker seine Schweigepflicht brechen, wenn er eigene Ansprüche durchsetzen will oder es gilt, persönliche Vorwürfe abzuwehren.

Diese Konstellation bestand jedoch im vorliegenden Fall nicht, wie ich bei meiner datenschutzrechtlichen Kontrolle im LKA feststellen konnte. Das LKA zeigte sich einsichtig und sicherte zu, entsprechende „Warnmeldungen“ künftig zu unterlassen.

5.10 Verfassungsschutz

Landesamt für Verfassungsschutz

Im Rahmen der gesetzlich gebotenen Anhörung meiner Behörde nach § 8 Abs. 2 SächsVSG sowie anlässlich mehrerer Kontrollen habe ich die personenbezogene Datenverarbeitung im Landesamt für Verfassungsschutz überprüft. Meine Empfehlungen zur Ergänzung von Dienstvorschriften und zur Ausgestaltung der Aktenführung wurden vom Landesamt ausnahmslos umgesetzt. Wegen der Einstufung der Dienstvorschriften und der kontrollierten Akteninhalte als Verschlusssachen ist es mir verwehrt, an dieser Stelle über weitere Einzelheiten zu berichten.

5.11 Landessystemkonzept / Landesnetz

In diesem Jahr nicht belegt.

5.12 Ausländerwesen

Mitwirkung der Ausländerbehörden bei der Erteilung ausländischer Reisepässe

Einem ausreisepflichtigen abgelehnten Asylbewerber, der freiwillig in sein Heimatland zurückzukehren beabsichtigte, wurde von der Ausländerbehörde ein ausländi-

scher Passbeschaffungsantrag zum Ausfüllen ausgehändigt. Dort waren u. a. sinngemäß folgende Angaben „Im Namen Gottes“ verlangt:

- Grund für die Ausreise aus dem Heimatland und illegale Tätigkeit im Heimatland,
- kurze Lebenslaufschilderung in der BRD bis jetzt,
- Asylart und Verfahrensergebnisse sowie Grund der Zurückstellung des Asylantrages,
- falls sich Familienangehörige in der BRD befinden, die Personalien angeben.

Bei wahrheitswidrigen Angaben wurden Sanktionen angedroht.
Der Antrag enthält also eine Reihe von Fragen, die nach deutschem Recht datenschutzrechtlich unter keinen Umständen hinnehmbar sind. Und diesen - ausgefüllten - Bogen wollte die Ausländerbehörde an die Botschaft weiterleiten.

Da nicht auszuschließen war, dass diese Verfahrensweise auch von anderen sächsischen Ausländerbehörden praktiziert wurde, habe ich dem SMI mitgeteilt, dass ich es für unabdingbar halte, dass sich die sächsischen Ausländerbehörden keinesfalls „vor den Karren“ eines Herkunftslandes spannen lassen und an der von dort initiierten und offensichtlich rechtswidrigen Datenerhebung mitwirken dürfen. Die Daten könnten nämlich bei verständiger Würdigung die Grundlage für staatliche Aktivitäten des Heimatlandes gegen den Betroffenen bzw. seine Angehörigen sein. Von hier aus kann nicht verlässlich beurteilt werden, ob dies in Form und Inhalt mit freiheitlichen und demokratischen Prinzipien vereinbar ist.

Ich habe deshalb gebeten bei den Ausländerbehörden sicherzustellen, dass diese sich nicht (mehr) an der Erhebung und Übermittlung der aus unserer Sicht für rechtsstaatliche Zwecke nicht erforderlichen Daten beteiligen. Das SMI hat daraufhin bei den Ausländerbehörden für Klarheit gesorgt, die künftig hoffentlich anhält.

5.13 Wahlrecht

In diesem Jahr nicht belegt.

5.14 Sonstiges

5.14.1 Novellierung des Sächsischen Vermessungsgesetzes

Letztmals habe ich mich in 6/5.14.1 zu den Novellierungsabsichten des SMI geäußert. Über einen überarbeiteten Referentenentwurf des „Gesetzes über die Landesvermessung und das Liegenschaftskataster im Freistaat Sachsen“, Stand Januar 2000, ist man bisher nicht hinausgekommen. Auch dieser Referentenentwurf war aus datenschutzrechtlicher Sicht, insbesondere was manuelle und automatisierte Datenübermittlungen (Auskunft, Einsicht, Weitergabe von Liegenschaftskatasterdaten) betraf, äußerst problembehaftet; vorgesehene Regelungen waren widersprüchlich, Datenübermittlungen *„auf Antrag“* wurden *„regelmäßigen“* Datenübermittlungen gleichgesetzt und automatisierte Abrufe aus dem Liegenschaftskataster *durch Private* sollten ermöglicht werden.

Die im Entwurf vorgesehene Einzelfallprüfung, die vor Datenübermittlungen grundsätzlich durchzuführen ist, wurde durch eine kontroverse Bestimmung über die „*Offenlegung*“ von Änderungen im Liegenschaftskataster *ohne jede Vorbedingung* auf den Kopf gestellt.

Neben meiner kritischen Stellungnahme habe ich dem SMI ein klärendes Gespräch angeboten. Die weitere Entwicklung bleibt abzuwarten.

5.14.2 Unzulässige Presseinformation eines Landkreises

Auf einer Pressekonferenz informierte der Erste Beigeordnete eines sächsischen Landkreises über Einzelheiten eines im Kreiskrankenhaus durchgeführten Schwangerschaftsabbruchs. Dabei gab er der Öffentlichkeit in einer schriftlichen „Presseinformation“ Diagnose- und Therapiedaten einer Patientin sowie Daten aus dem Beschäftigungsverhältnis des aufgrund des medizinischen Eingriffs entlassenen Arztes der Öffentlichkeit bekannt.
Diese „Öffentlichkeitsarbeit“ des Landkreises habe ich förmlich beanstandet, weil sie aus den folgenden Gründen eklatant gegen Vorschriften des Datenschutzes verstieß: Das Sächsische Datenschutzgesetz zieht in § 15 der Übermittlung personenbezogener Daten durch öffentliche Stelle an nicht-öffentliche Stellen enge Grenzen. Die dort aufgeführten Erlaubnistatbestände standen bei der Verbreitung dieser sensitiven Daten ersichtlich nicht zur Debatte. Bereits an der Grundvorausetzung, wonach die Datenübermittlung an private Stellen der Aufgabenerfüllung der öffentlichen Stelle dienen muss, fehlte es. Denn dass es - wie der Landkreis in einer zunächst abgebenen Rechtfertigung behauptete - zu den gesetzlichen Aufgaben einer öffentlichen Stelle gehöre, mittels Grundrechtseingriffen der vorliegenden Art gegenüber „Spekulationen durch die Medien ... Position zu beziehen“, kann ernsthaft nicht vertreten werden. Auch die Einlassung des Landkreises, die in seiner Pressemitteilung aufgeführten Sachverhalte seien infolge vorausgegangener Presseberichte „offenkundig“ gewesen, war unbeachtlich. Denn ein Vergleich der vom Ersten Beigeordneten veröffentlichten Detaildichte mit sämtlichen in dieser Sache zuvor verbreiteten Pressemitteilungen zeigte, dass für die in Rede stehende Presseinformation des Landkreises besonders heikle Interna (darunter exakte Diagnosedaten und Zeitabläufe im Krankenhaus), die aus der Verwaltung und aus dem medizinischen Bereich stammen mussten, Verwendung fanden. Insofern wurde auch der erweiterte Geheimnisschutz des § 203 StGB unterlaufen. Man fragt sich, wie das Landratsamt überhaupt an solche medizinischen Daten kommt.

Der verantwortliche Landrat reagierte sofort auf meine Beanstandung und sicherte zu, dass künftige Pressemitteilungen des Landkreises den datenschutzrechtlichen Erfordernissen entsprechen werden.

5.14.3 Landrat verweigerte Antworten

Im Rahmen einer Kontrolle der Personalakten eines Landratsamtes habe ich dem Landrat Fragen gestellt, die dieser zunächst nicht beantwortete. Erst aufgrund meiner förmlichen Beanstandung wegen Verletzung der gesetzlichen Pflicht zur Unterstüt-

zung nach § 25 SächsDSG erhielt ich nach mehr als vier Monaten die erbetenen Angaben.

Die Missachtung der Auskunftspflicht durch einen Landrat halte ich für einen gravierenden Rechtsbruch, zumal ein Landrat in seinem Zuständigkeitsbereich seinerseits zur Überwachung der Einhaltung des Rechts gesetzlich verpflichtet ist. Die Behörden der Kommunalaufsicht, also das SMI und das Regierungspräsidium Chemnitz, habe ich über den vorliegenden Fall informiert, um rechtsaufsichtliche Konsequenzen prüfen zu lassen. Nach dem späten Einlenken des Landrats waren Weiterungen nicht nötig.

5.14.4 Überprüfung von Gemeinderäten und Kreistagsmitgliedern auf eine frühere Zusammenarbeit mit dem MfS/AfNS

Nach den sächsischen Kommunalwahlen 1999 wandten sich Gemeinderäte und Kreistagsmitglieder an mich. Sie wollten wissen, in welchem Umfang BStU-Unterlagen für die Überprüfung von Mitgliedern kommunaler Vertretungskörperschaften zur Verfügung stehen und ob es für diese Nutzung bestimmte Formvorschriften einzuhalten sind. Nachdem ich mit dem SMI die Thematik erörtert habe, bin ich zu folgendem Ergebnis gelangt:

Einschlägige Normen sind die §§ 20 und 21 StUG. Sie sind gleichermaßen zum einen die notwendigen Datenübermittlungsvorschriften für den BStU und zum anderen die notwendigen Erhebungsvorschriften für die im Sinne dieser Vorschriften zuständigen öffentlichen Stellen des Freistaates Sachsen. Denn der dort benutzte Begriff der „Verwendung“ von Unterlagen umfasst gemäß § 6 Abs. 9 StUG die Weitergabe von Unterlagen, die Übermittlung von Informationen aus Unterlagen sowie die sonstige Verarbeitung und die Nutzung der Informationen. Die Vorschriften wenden sich nicht nur an den BStU, sondern eröffnen Befugnisse für sämtliche öffentliche und nichtöffentliche Stellen, auch solche des Freistaates Sachsen (§ 4 Abs. 1 Satz 1 StUG). Folglich enthält das StUG eine Rechtsgrundlage für die Erhebung und die Verarbeitung solcher personenbezogener Daten durch sächsische kommunale Vertretungskörperschaften, die ihnen vom BStU übermittelt wurden.

Der Zweck dieser Verarbeitung personenbezogener Daten von Angehörigen kommunaler Vertretungskörperschaften liegt in der Feststellung, ob der Betroffene hauptamtlich oder inoffiziell für den Staatssicherheitsdienst der DDR tätig war. Diese Feststellung allein ist als Verarbeitungszweck im Gesetz auszumachen. Denn weitere gesetzliche Vorschriften über die Überprüfung von Mitglieder von Kreistagen und Gemeinderäten/Stadträten sind in der Rechtsordnung nicht ersichtlich, folglich sind auch keine anderen Verarbeitungszwecke normiert. Die Aufarbeitung der Vergangenheit ist ein sowohl allgemeines als auch im Einzelfall bestehendes Anliegen, dem der Gesetzgeber im StUG Ausdruck verliehen hat (§ 1 Abs. 1 Nr. 3 StUG). Es geht ihm darum, dass die Wahrheit auf den Tisch kommt.

Verbindliche Konsequenzen, etwa im Sinne eines Mandatsverlustes, dürfen hier jedoch - mangels Rechtsgrundlage - an die Feststellung nicht geknüpft werden. In der

Praxis darf aber ein feststellender Beschluss - wie jeder Beschluss - veröffentlicht werden. Die Absicht der öffentlichen Stelle, von der Möglichkeit der Offenlegung Gebrauch zu machen, bedarf einer Willensbildung, also eines (Mehrheits-)Beschlusses, der die Anfrage beim BStU initiiert und durch die Geschäftsstelle der Vertretungskörperschaft oder durch einen speziell Beauftragten (Bürgermeister, Landrat, speziell beauftragte Person) durchführen lässt.

Daneben ist es auch möglich und zur Vermeidung nochmaliger Diskussionen sehr sinnvoll, eine entsprechende Satzung zu beschließen. Sie hätte nämlich den Vorteil, auf Dauer zu wirken, insbesondere dann, wenn sich die Zusammensetzung des Rates ändert, also neue, noch nicht überprüfte Mitglieder hinzutreten.

Das Prinzip der „Freiwilligkeit“ im Sinne des § 4 SächsDSG spielt in diesem Zusammenhang keine Rolle. Mit anderen Worten: Eine Minderheit kann überstimmt werden. Dies liegt im Wesen der demokratischen Willensbildung der Vertretungskörperschaft und widerspricht im Übrigen nicht den Vorschriften des StUG. Im Ergebnis werden also auch Personen überprüft, die der Entscheidung der Vertretungskörperschaft (Satzung bzw. Beschluss) nicht zugestimmt haben.

Jedem Mitglied der Vertretungskörperschaft ist es aber als selbst zu entscheidende Konsequenz gestattet, die (weitere) ehrenamtliche Tätigkeit aus dem Grund abzulehnen, weil sich aufgrund der Mitteilung des BStU seine eigene Mitarbeit für das MfS herausgestellt hat. Dies dürfte ein wichtiger Grund im Sinne des § 18 Abs. 1 SächsGemO (§ 16 SächsLKrO) sein, das Mandat freiwillig aufzugeben. Auf das Wort „insbesondere“ in Satz 2 verweise ich insoweit.

Mithin begegnet es aus datenschutzrechtlicher Sicht keinen Bedenken, wenn die Feststellung einer Stasi-Mitarbeit in der politischen Auseinandersetzung dazu führt, einem Mitglied der Vertretungskörperschaft die Niederlegung des Mandates zu empfehlen.

Dem SMI und dem SMJus habe ich meine Rechtsauffassung mitgeteilt.

5.14.5 Risiken und Grenzen der Videoüberwachung

Nunmehr hat wohl auch die Öffentlichkeit in ihr Bewusstsein aufgenommen, was bislang offenbar nur interessierte Kreise, zum Beispiel die Datenschutzbeauftragten, bewegte: Der öffentliche Einsatz der Videotechnik. Mit „Big Brother“ auf der privatunterhaltsamen und flächendeckender Verkehrsraumbeobachtung auf der öffentlichernsten Seite gewinnt die Problematik von (Grund-) Rechtseingriffen eine populäre, d. h. gemeinverständliche Dimension.

Quasi im Vorgriff auf den rasant fortschreitenden Einsatz dieses Informationsmediums beriefen die Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe zur Videoüberwachung ein, die auf zwei in Dresden stattfindenden Sitzungen versuchte, die rechtlichen Zulässigkeitskriterien für den Einsatz der Videotechnik zu definieren. Hierbei wurden folgende Grundpositionen herausgearbeitet:

Der Einsatz der Videotechnik (wohl besser: der optisch-elektronischen Datenverarbeitung) zur Erfassung personenbezogener Informationen birgt besondere Risiken für das Recht auf informationelle Selbstbestimmung. Analoge oder digitale Erfassung, Aufzeichnung oder Übertragung von Bilddaten führen zur Ungewissheit des Einzelnen, ob und von wem er beobachtet wird und zu welchen Zwecken dies geschieht. Nicht einschätzbare Distanzen zwischen dem Beobachter, der Kamera, dem Betroffenen und der weiteren Datenverarbeitung (zum Beispiel Internet) die technische und inhaltliche Verknüpfbarkeit gewonnener Informationen mit multimedial verarbeiteten Datenbeständen und die breite Gewinnung von Überschuss- und Kontextinformationen schaffen Verunsicherung. Dies beeinträchtigt den individuellen Entfaltungswillen und stört deshalb das Gemeinwohl.

Soweit öffentliche Stellen optisch-elektronische Datenverarbeitung betreiben, müssen die verfassungsrechtlich garantierten Freiheitsrechte des Einzelnen gewahrt bleiben. Insbesondere darf die ungehinderte Bewegungs- und Entfaltungsfreiheit nur auf normenklarer Rechtsgrundlage und nur unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes eingeschränkt werden.

Auch die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtssprechung reichen nicht aus, wenn Private den öffentlich zugänglichen Raum beobachten. Der Gesetzgeber ist daher aufgefordert, im BDSG entsprechende Regelungen zu schaffen, die zu einem gerechten Interessenausgleich der Beteiligten führen.

Allgemein müssen die gesetzlich zu normierenden Grundsätze der klaren Zweckbestimmung, des grundsätzlichen Verbotes heimlicher Beobachtungen und Aufnahmen, der Transparenz und der frühestmöglichen Löschung, besonderer Verfahrensvorkehrungen entsprechend der Eingriffstiefe, der Datenvermeidung, der Datensparsamkeit, der Vorabkontrolle und regelmäßigen Evaluierung gelten. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, zum Beispiel für die Reduzierung auf tatsächlich erforderliche Daten, bieten, sind zu nutzen. Der Gesetzgeber hat ferner zu berücksichtigen, dass die Aufzeichnung regelmäßig tiefer in das Persönlichkeitsrecht eingreift als die Beobachtung und damit das Missbrauchsrisiko erhöht wird. Werden die Daten einer bestimmten Person zugeordnet, so ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird. Eine gezielte Beobachtung einzelner Personen darf nur erfolgen, wenn dies zur Abwehr erheblicher und konkreter Gefahren oder zur Strafverfolgung unerlässlich ist.

Die unbefugte Weitergabe heimlicher Aufnahmen muss ebenso strafbewehrt werden wie der Missbrauch videotechnisch gewonnener biometrischer Daten und deren Abgleiche sowie der Missbrauch anderer Methoden von besonderer Eingriffstiefe.

Mit dem freiheitlichen Menschenbild des Grundgesetzes wäre ein flächendeckender Einsatz von Videotechnik unvereinbar; dies selbst dann, wenn jeder Einsatz für sich betrachtet zu rechtfertigen wäre.

Diese auf den Dresdner Arbeitsgruppensitzungen einvernehmlich erarbeiteten Positionen fanden Eingang in eine Entschließung der Datenschutzbeauftragten des Bundes und der Länder (siehe unten 16.1.6).

6 Finanzen

6.1 Anerkennung von Werbungskosten - Aufforderung des Finanzamtes an Mitreisende und Reiseveranstalter, Namen und Anschriften der Teilnehmer mitzuteilen und Kontrollmitteilungen

Die Stellungnahme der Staatsregierung zu 7/6.2 lässt kein Einlenken des SMF erkennen.
Namen und Anschriften der Mitreisenden sind nicht geeignet, die Homogenität des Teilnehmerkreises festzustellen. Personenbezogene Kontrollmitteilungen an die Finanzämter der übrigen Reiseteilnehmer werden nach wie vor - wenn auch in Einzelfällen - für erforderlich gehalten, ohne dass bisher dargetan wurde, welche Einzelfälle gemeint sein könnten (meine Phantasie reicht jedenfalls nicht aus, mir Fälle vorzustellen, in denen Namen und Anschriften von Mitreisenden für ein konkretes Besteuerungsverfahren erforderlich sein sollen).

Die modifizierte OFD-Verfügung, die das Verfahren transparenter machen sollte, bringt uns einer datenschutzgerechten Behandlung ein wenig näher. Die jahrelangen Bemühungen, die bisherige aus datenschutzrechtlicher Sicht rechtswidrige Verfahrensweise auf ein den Grundsätzen des Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf gerecht werdendes Fundament zu stellen, sollten aber in der in Aussicht genommenen „Konkretisierung“ der o. a. OFD-Verfügung nicht enden.

Für die Finanzämter seien zwar die „ausgeübten Berufe“ der weiteren Reiseteilnehmer ein entscheidendes Kriterium für die Homogenität des Teilnehmerkreises. *Weshalb* aber „Namen und Anschriften“ (nicht also die Berufe) der Mitreisenden vom Steuerpflichtigen nach § 93 AO verlangt werden (soweit dies für das konkrete Besteuerungsverfahren von Bedeutung ist), hat sich mir bisher nicht erschlossen.

Der Wortlaut des § 93 Abs. 1 Satz 1 AO, wonach die Beteiligten (und andere Personen) der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes *erforderlichen* Auskünfte zu erteilen haben, schließt jedoch unter Beachtung des auch für die Finanzverwaltung verbindlichen Verhältnismäßigkeitsgrundsatzes Fragen nach „Namen und Anschriften“ der Mitreisenden schon deshalb aus, weil diese Daten für die Feststellung des „homogenen“ Teilnehmerkreises ungeeignet sind, wogegen mir die (nicht vorgesehene) Frage nach dem „Beruf“ der Mitreisenden einleuchten würde.

Niemand, der sich bei einem ordentlichen Veranstalter einer Studienreise anmeldet, kann beeinflussen, wer mitreist. Die Homogenität des Teilnehmerkreises wird damit zu einer Voraussetzung, die außerhalb der Verantwortung des einzelnen Steuerpflich-

tigen liegt. Außerdem ist es Zufall, ob Namens- Adressen- und Berufslisten (wahrheitsgemäß) ausgegeben werden. Wer bewahrt so etwas nach der Reise auf? Darf der Einzelne solche Listen für (Steuer-)Zwecke, die außerhalb der Reise liegen, verwenden? Muss er sich dann nicht wie ein Denunziant fühlen? Alle diese ganz praktischen Fragen sind ungeregelt. Ich habe vorgeschlagen, stattdessen die objektiven Unterlagen/Prospekte/Beschreibungen von Bildungsinhalten, die der Veranstalter vor der Reise mitteilt, zur Grundlage der Entscheidung zu nehmen, ob eine steuerlich wirksame Studienreise vorliegt. Denn nur darauf kann sich der Steuerpflichtige bei seiner Entscheidung, ob er die Reise antritt, verlassen. Die Homogenität des Teilnehmerkreises kann nur als objektives, nämlich vom Reiseveranstalter festgelegtes Kriterium eine Rolle spielen; deshalb sind auch nur *dessen* Unterlagen aussagekräftig.

Da neben der eigentlichen Feststellung des „homogenen" Teilnehmerkreises auch „Kontrollmitteilungen" an die Wohnsitzfinanzämter der Mitreisenden (merkwürdigerweise nur bei Versagen der Anerkennung des Steuerabzugs) vorgesehen sind, käme hierfür m. E. die Erhebung des Datums „Wohnsitzgemeinde" der Mitreisenden in Frage. *Personenbezogene* „Kontrollmitteilungen" sind nicht erforderlich; es würde genügen, den Wohnsitzfinanzämtern mitzuteilen, dass für eine näher zu bezeichnende Studienreise Betriebsausgaben oder Werbungskosten aus den und den Gründen anerkannt/nicht anerkannt wurden.

Ich habe dem SMF deshalb geraten, die vorgesehene Änderungsverfügung im Sinne meiner Vorschläge zu überarbeiten, um eine Beanstandung (wegen Anweisung der nachgeordneten Behörden zu rechtswidrigen Datenerhebungen und Datenübermittlungen) zu vermeiden.

Zwar hat man mir eine erneute Überarbeitung der OFD-Verfügung in Aussicht gestellt; auf einen Verzicht von personenbezogenen Kontrollmitteilungen ist jedoch den jüngsten Äußerungen des SMF zufolge nicht zu hoffen.

6.2 Einführung der elektronischen Steuererklärung (ELSTER)

Mit dem vom BMF geplanten Projekt „Elektronische Steuererklärung - ELSTER" ist beabsichtigt, mittelfristig auf die Steuererklärung in Papierform vollständig verzichten zu können. Dazu soll in absehbarer Zeit die bisher mit der Lohnsteuerkarte verbundene Lohnsteuerbescheinigung durch eine elektronische Übermittlung von Lohnsteuerbescheinigungsdaten der Arbeitgeber an die Finanzverwaltung ersetzt werden. Gleichzeitig sollten auch die von der Sozialversicherung zu bescheinigenden Daten über geleistete Lohnersatzleistungen auf elektronischem Wege an die Finanzverwaltung übermittelt werden. Hierzu wurde die Verwendung der Sozialversicherungs-Nummer als einheitlicher Ordnungsbegriff ins Auge gefasst.

Einzelheiten, die seitens des BMF bekannt wurden, ließen Ausblicke auf Vorhaben zu, die mir in dieser Dimension bisher nicht deutlich waren.

Während bislang technisch-organisatiorische Gesichtspunkte im Zusammenhang mit der Abgabe elektronischer Steuererklärungen im Vordergrund standen, ließ das

BMF-Schreiben Tendenzen in Richtung Verknüpfung sämtlicher für die Finanzverwaltung relevanten Dateien erkennen, wobei die Sozialversicherungs-Nummer eine wesentliche Rolle spielen sollte. Die PKZ lässt grüßen.

Es sieht zunächst harmlos aus, wenn anstelle persönlicher Steuererklärungen Lohnsteuerbescheinigungen und von der Sozialversicherung zu bescheinigende Daten über geleistete Lohnersatzleistungen an die Finanzverwaltung elektronisch übermittelt werden sollen. Stehen die entsprechenden Verfahren aber erst einmal zur Verfügung, wird es nur ein kleiner Schritt sein, die Verknüpfung mit Banken, Versicherungen, Krankenkassen, Religionsgesellschaften und sonstigen Institutionen, die für das Besteuerungsverfahren relevant sind, in Angriff zu nehmen. Einen anderen Schluss lassen die Äußerungen des BMF nicht zu.

Zwischenzeitlich wurde dem Vernehmen nach von der Absicht, die Sozialversicherungsnummer als Ordnungsbegriff zu verwenden, Abstand genommen, weil durchgreifende datenschutzrechtliche, nämlich verfassungsrechtliche Bedenken bestehen. Zu fordern bleibt derzeit allerdings, dass die rechtmäßige Einrichtung des Verfahrens ELSTER einer Rechtsverordnung nach § 150 Abs. 6 AO bedarf.

Ich habe das SMF um weitere Beteiligung gebeten. Denn mit Sicherheit wird über kurz oder lang ein elektronischer Abruf sämtlicher steuerrelevanter Informationen erneut ins Gespräch kommen.

6.3 Steuerliche Behandlung der Ausgaben für Telefongespräche in der Wohnung des Arbeitnehmers und der Aufwendungen für die Benutzung eines Autotelefons und anderer Mobiltelefone

Aus der Presse erfuhr ich von der Absicht des BMF, per Verwaltungsanweisung das Verfahren der steuerfreien Behandlung von außerbetrieblichen dienstlichen Telefonaten neu zu regeln.

Unter anderem muss der Arbeitgeber nicht nur wie bisher die private Nutzung von für dienstliche Zwecke in der Wohnung des Beschäftigten eingerichteten Telefonanlagen untersagen, sondern er muss künftig zusätzlich die Beachtung des Verbots auch überwachen.

Neu ist auch bei ISDN-Anschlüssen in der Wohnung des Beschäftigten, dass die Erstattung von Aufwendungen durch den Arbeitgeber nur dann steuerfrei ist, wenn anhand einer *detaillierten Abrechnung* der Telefongesellschaft nachzuweisen ist, dass eines der Geräte so gut wie ausschließlich dienstlich genutzt wird. In anderen Fällen dienstlicher Telefongespräche außerhalb des Betriebes, also vor allem bei Telefonaten vom Apparat des Arbeitnehmers in seiner Wohnung (ohne ISDN-Zweitanschluss), muss der Beschäftigte die Gebühren, die auf dienstliche Gespräche entfallen, durch eine *detaillierte Abrechnung* der Telefongesellschaft nachweisen. Wenn er diesen Nachweis über einen repräsentativen Zeitraum von zwölf Monaten

(bisher drei Monate) führt, kann er das Ergebnis in den folgenden zwei Jahren bei der Berechnung seiner Ausgaben für Dienstgespräche zugrunde legen und auf dieser Basis auch den Grundpreis anteilig dem Arbeitgeber zur steuerfreien Erstattung berechnen.

Da diesem Verfahren personenbezogene Daten sowohl der Beschäftigten als auch der Angerufenen immanent sind, deren Verarbeitung einer gesetzlichen Grundlage bedarf (eine Verwaltungsanweisung dürfte nicht ausreichen), habe ich das SMF und den BfD über meine Sichtweise - nicht zuletzt im Hinblick auf das durch Art. 10 GG geschützte Fernmeldegeheimnis - unterrichtet. Der BfD hat meine Argumente aufgegriffen und dem BMF mitgeteilt.

Letzten Informationen zufolge wurde der entsprechende Entwurf des BMF-Schreibens dahingehend modifiziert, dass für private Nutzungen im Einzelverbindungsnachweis
- Datum der Verbindung,
- Zielrufnummer (einschl. Ortsnetzvorwahl),
- Entgelt für die Verbindung

unkenntlich gemacht werden können. Wie ich meine, ein Schritt in die richtige Richtung.

6.4 Veröffentlichung personenbezogener Daten bei Verurteilungen und strafbewehrten Unterlassungserklärungen im Kammerbrief der Steuerberaterkammer des Freistaates Sachsen

Das seit 1996 andauernde Hick-Hack um die aus meiner Sicht rechtswidrigen Veröffentlichungen (vgl. letztmals 7/6.4), fand im April 1999 in einem Kompromiss sein Ende.

Das SMF hat (wohl bestärkt durch Äußerungen des Hessischen Datenschutzbeauftragten, der die personenbezogenen Veröffentlichungen nicht für unzulässig hält) in einer von der Steuerberaterkammer akzeptierten Empfehlung darauf hingewirkt, dass die Veröffentlichung von personenbezogenen Daten bei Verurteilungen und strafbewehrten Unterlassungserklärungen nicht mehr im Kammerbrief selbst, sondern in einer ausschließlich für Kammermitglieder vorgesehenen Anlage erfolgt. Zudem hat die Steuerberaterkammer zugesagt, die Kammermitglieder ausdrücklich auf die Vertraulichkeit hinzuweisen. Nichtmitglieder dürften somit keine Kenntnis mehr von den Wettbewerbssündern erhalten.

6.5 Führung von Fahrtenbüchern durch Ärzte für steuerliche Zwecke

Letztmals habe ich mich in 7/6.1 mit der nach Ansicht der Datenschutzbeauftragten des Bundes und der Länder vertretenen Auffassung, die Verpflichtung der Ärzte in ihren Fahrtenbüchern neben Reisezweck, Reiseziel, Reiseroute, Datum und Kilome-

terstand ohne Ausnahme auch den Patientennamen eintragen zu müssen, sei als Verstoß gegen die ärztliche Schweigepflicht rechtswidrig, auseinandergesetzt.

Inzwischen hat das SMF ein mit dem BfD abgestimmtes Schreiben des BMF den nachgeordneten Finanzbehörden bekanntgegeben. Dieses Schreiben enthält - trotz nach wie vor gegenteiliger Rechtsansicht zu § 102 Abs. 1 Nr. 3 Buchstabe c AO - einen tragfähigen Kompromiss: Die von einem Arzt aufgesuchten Patienten werden nicht bereits im Fahrtenbuch selbst, sondern erst in einem separaten Verzeichnis festgehalten. Dieses Verzeichnis wird vom Finanzamt nur angefordert, soweit dies von ihm im Einzelfall als erforderlich angesehen wird. Die strittige Frage, ob der Arzt sich auf § 102 Abs. 1 Nr. 3 Buchstabe c AO berufen und die Bekanntgabe von Namen und Anschriften seiner Patienten verweigern darf, ist damit zwar nicht vom Tisch, aber deutlich nach hinten verlegt. Da nach dem oben erwähnten BMF-Schreiben davon auszugehen ist, dass das Finanzamt bei Weigerung der Herausgabe des Patientenverzeichnisses den Nutzungswert des Arzt-Pkw's zum Nachteil des Arztes pauschal ansetzt, ist die Entscheidung über die Reichweite des § 102 Abs. 1 Nr. 3 Buchstabe c AO letztlich der Rechtsprechung überlassen. Damit kann man leben.

6.6 Flächendeckende Hundebestandsaufnahme

Zwei Firmen bieten den Gemeinden eine flächendeckende Datenerhebung über Hundehalter mit der Folge an, dass diese ggf. zur gemeindlichen Hundesteuer veranlagt werden.

Obwohl ich Bedenken gegen diese Aktion angemeldet hatte, waren sich SMI, SMF und der SSG einig, dass die Beauftragung solcher Unternehmen mit der Datenerhebung im Wege der „Verwaltungshilfe" mit dem geltenden Abgabenrecht zu vereinbaren sei.

Gegen einen entsprechenden Erlassentwurf habe ich eingewandt, dass es sich bei der Erhebung von Besteuerungsgrundlagen um eine hoheitliche Tätigkeit im Bereich des Abgabenrechts handelt, die nicht ohne weiteres im Wege der Verwaltungshilfe auf Private übertragen werden kann. Grundlage für meine Haltung war der Beschluss des Bayerischen Obersten Landesgerichts vom 5. März 1997 - 1ObOWi 785/96 (DÖV 1997, 601 f.), der die Ausübung von Staatsgewalt durch Heranziehung von Verwaltungshelfern einschränkend konkretisiert.

Nach dem Beschluss ist z. B. eine planmäßige Durchführung von Geschwindigkeitsmessungen durch private Auftragnehmer selbst dann unzulässig, wenn die zuständige Behörde Ort, Zeit und Umfang der Kontrolle bestimmt und die einzelnen Mitarbeiter direkt den Weisungen unterworfen sind. Die Übertragung von Hoheitsaufgaben auf Private kann allenfalls in Gestalt der Beleihung erfolgen, die jedoch der gesetzlichen Ermächtigung bedarf. Diese Ausführungen gelten gleichermaßen für die Bestandsaufnahme der in der Gemeinde gehaltenen Hunde.

Dass die Erhebung von Besteuerungsgrundlagen zum Kernbereich hoheitsrechtlicher Aufgabenerfüllung gehört, ergibt sich bereits aus den §§ 85, 86, 88 bis 93 AO, die

eindeutig das Über- und Unterordnungsverhältnis zwischen Obrigkeit und Steuerpflichtigen dokumentieren.

Insofern war es auch fehlerhaft anzunehmen, dass die Übertragung dieser hoheitsrechtlichen Aufgaben auf ein Privatunternehmen im Wege der Auftragsdatenverarbeitung (§ 7 SächsDSG) möglich sei. Da Datenverarbeitung für sich gesehen keine Aufgabe der Verwaltung, sondern lediglich ein (technisches) Hilfsmittel zur Erledigung der öffentlichen Aufgabe darstellt, muss die Beauftragung eines Privatunternehmens im Rahmen des § 7 SächsDSG ebenso ausscheiden wie die Übertragung der Erhebung von Besteuerungsgrundlagen auf einen Verwaltungshelfer.

Schließlich habe ich zu bedenken gegeben, dass insbesondere die Finanzverwaltung wegen ihrer dem Kernbereich hoheitsrechtlicher Verwaltung zuzurechnenden Staatsaufgaben und im Hinblick auf das Steuergeheimnis (§ 30 AO) nach meiner Kenntnis bislang von der Beauftragung Privater in jedweder Form abgesehen hat. Weshalb sollte es plötzlich bei kommunalen Steuern anders sein?

Ob sich das SMI meinen Argumenten anschließt bleibt abzuwarten. Jedenfalls sind die Gemeinden gut beraten, wenn sie die Hundebestandsaufnahme in Eigenregie durchführen.

7 Kultus

7.1 Zuschüsse für Schulen in freier Trägerschaft

Nach der Verordnung der Sächsischen Staatsregierung über die Gewährung von Zuschüssen für Schulen in freier Trägerschaft bemisst sich der Zuschuss für allgemeinbildende und berufsbildende Schulen nach festen Jahressätzen pro Schüler. Komplizierter ist die Berechnung bei den als Ersatzschulen genehmigten Förderschulen. Außer einem Sachkostenzuschuss pro Schüler erhalten sie einen Zuschuss zu den Personalkosten, der - auf den individuellen Einzelfall bezogen - nicht höher sein darf als das, was ein vergleichbarer Beschäftigter im öffentlichen Dienst an Bezügen erhält (§ 2 Abs. 3 ZuschussVO). Es liegt auf der Hand, dass eine solche konkrete Bezügeberechnung eine umfangreiche Datenerhebung erfordert. Ein Träger empfand dies als Zumutung und wandte sich an mich.

Ich habe mich mit der Angelegenheit eingehend befasst. Wie sich herausstellte, müssten bei den Regionalschulämtern, die die Zuschüsse zu gewähren haben, im Grunde „Bezügeakten“ geführt und kompliziertes Tarifrecht angewendet werden, damit die jetzige Regelung vollzogen werden kann. Dies können sie mit angemessenem Aufwand nicht leisten. Das für Bezügeangelegenheiten zuständige Landesamt für Finanzen könnte es, darf jedoch ohne entsprechende gesetzliche Grundlage diese dem Schulbereich obliegende Aufgabe nicht übernehmen. Vor diesem Hintergrund haben SMK und SMF nunmehr einvernehmlich eine neue Verfahrensweise festgelegt, „die es ermöglicht, die Obergrenze der zu erstattenden Personalausgaben für

Lehrkräfte an Förderschulen in freier Trägerschaft *ohne* die Verarbeitung individueller personenbezogener Daten zu ermitteln". Einzelheiten der künftigen Regelung, die ich prüfen werde, stehen noch nicht fest. Ich denke aber, dass meine datenschutzrechtliche Intervention, viel Aufwand einzusparen, angeregt hat.

7.2 Angabe von Fehltagen in Zeugnissen

Vor dem Hintergrund einer bundesweit geführten Diskussion zur Angabe von Fehltagen in Zeugnissen hat mich das SMK um eine datenschutzrechtliche Bewertung dieser in einigen Bundesländern geübten Praxis gebeten. Dazu habe ich Folgendes vertreten:

Ich habe keine Bedenken dagegen, dass Fehltage oder auch Fehlstunden in Zeugnissen (mit der Unterscheidung, ob entschuldigt oder unentschuldigt) ausgewiesen werden. In Abgangszeugnissen jedoch ist davon abzusehen. Der Grund liegt darin, dass die Angabe der Fehlzeiten der pädagogischen Führung dient, folglich vom Erziehungsauftrag der Schule getragen ist. Dieser Auftrag endet jedoch mit der Aushändigung des Abgangszeugnisses, so dass ein legitimer Zweck mit einer solchen Angabe auf dem Abgangszeugnis nicht mehr verfolgt wird.

7.3 Förderschulen - Schulbezeichnungen

In 7/7.2 habe ich auf die nicht zu unterschätzende und grundrechtsverletzende Prangerwirkung hingewiesen, die mit der exakten Bezeichnung der jeweiligen Förderschule einhergeht.

Eine erste Stellungnahme des SMK hat mich nicht überzeugt, weil lediglich auf die bestehende Rechtslage und auf Rahmenempfehlungen der Kultusministerkonferenz der Bundesrepublik Deutschland hingewiesen wurde, wonach angeblich die von mir kritisierten Schulbezeichnungen als statthaft und nicht ehrverletzend akzeptiert werden. Außerdem wies das SMK darauf hin, dass eine Änderung der Namen der Förderschulen „zwangsläufig eine Schulgesetzänderung zur Folge" hätte.

Ich hatte große Probleme, solche Äußerungen des SMK mit Art. 1 Abs. 1 GG, 14 SächsVerf in Einklang zu bringen. Wenn es dort jeweils in Satz 2 heißt, dass es Verpflichtung aller staatlichen Gewalt ist, die Würde des Menschen zu achten und zu schützen, so muss dies durch positives Tun, insbesondere auch im Förderschulbereich, durchgesetzt werden. Im Lichte dieser Verfassungslage gewinnt der zwar anders gemeinte, aber dennoch richtige Hinweis in oben angeführter Stellungnahme, nämlich dass eine Änderung des Namen der Förderschulart zwangsläufig eine Schulgesetzänderung zur Folge hätte, an Bedeutung. Da es aus Sicht des SMK keine mildere Variante gibt, die Beeinträchtigung der Menschenwürde der Förderschüler auf ein Mininum zu reduzieren oder ganz zu vermeiden, mag in der Tat nur eine entsprechende Änderung des Schulgesetzes als Ausweg genommen werden. Was wäre dagegen einzuwenden?

Ich meine aber, es gibt eine andere, noch einfachere Lösung:

Der allumfassende amtliche Fürsorgegedanke früherer Zeiten ist mit unserer freiheitlichen Ordnung nicht mehr zu rechtfertigen. Er ist eben gerade nicht „durch das Schulgesetz abgedeckt“. Vielmehr entnehme ich dem Sächsischen Schulgesetz keine Vorschriften in Bezug auf den Namen oder die Bezeichnung von Schulen. Deshalb sehe ich keine Verpflichtung, die Differenzierung der Nummer 1 bis 9 des § 13 Abs. 1 SchulG nach außen durch den Namen oder die Bezeichnung der Schule zu dokumentieren. Man sollte in Frage stellen, ob und bei welcher Gelegenheit es erforderlich (!) ist, den Begriff der „Förderschule“ in amtlichen Schreiben zu benutzen. Bei Schülerausweisen, in einfachen Verwaltungsschreiben allgemeiner Korrespondenz, in Bescheinigungen, in Zeugnissen scheint dies nicht nötig zu sein.

Die Rahmenempfehlung der Kultusministerkonferenz halte ich weder für einschlägig noch für verbindlich, denn zu der Verbreitung der Informationen, dass ein Schüler eine bestimmte Förderschulart besucht, gibt auch sie keine Rechtsgrundlage an. Dies ist aber von Verfassungs wegen notwendige Grundlage für eine solche Datenverarbeitung.

Da ich das Problem für bedeutsam halte, sollte im Ergebnis erreicht werden, dass auch Förderschulen einen neutralen amtlichen Namen führen, der keinen Hinweis auf die Tatsache enthält, dass es sich um eine Förderschule handelt; erst recht ist es m. E. weder erforderlich noch statthaft, auf die Art der Förderzweiges hinzuweisen.

In einem Gespräch mit dem Amtschef des SMK konnte ich die Problematik noch vertiefen und stieß auf großes Verständnis. Für Mitte 2000 ist ein weiteres Treffen vorgesehen, bei dem möglicherweise schon konkrete Überlegungen zur Problementschärfung zur Sprache kommen.

8 Justiz

8.1 Datenschutzrechtliche Kontrolle im SMJus und bei drei Gerichten

Im Berichtszeitraum habe ich eine umfangreiche datenschutzrechtliche Kontrolle im SMJus und beim Oberlandesgericht sowie bei einem Landgericht und einem Verwaltungsgericht abgeschlossen. Die Kontrolle umfasste sieben Prüftermine. Als wesentliches Ergebnis habe ich hierbei Folgendes festgestellt:

8.1.1 Datenverarbeitung im SMJus

Obgleich der Schwerpunkt der Kontrolle der Umgang mit Beschäftigtendaten war, wurde auch die personenbezogene Datenverarbeitung zweier Fachabteilungen untersucht. Anlass für diese Erweiterung des Kontrollgegenstandes war das (erstmalig nach Ankündigung meiner Kontrolle erstellte!) Dateienverzeichnis, das - zusammen mit einem Geräteverzeichnis - bei Kontrollbeginn vorgelegt wurde.

Die Sichtung des Dateienverzeichnisses ergab, dass

- die Dateienbezeichnungen überwiegend sehr allgemein gehalten waren und nicht den eigentlichen Dateinamen entsprachen,

- eine Rechtsgrundlage häufig nicht aufgeführt oder lediglich auf das allgemeine Datenschutzrecht verwiesen wurde,

- Sperrungs- und Löschungsfristen oft und Anweisungen zu deren Überprüfung oder zur Protokollierung noch häufiger fehlten,

- bei mehreren Dateianwendungen Beschäftigtendaten verarbeitet wurden, ohne dass das nach § 31 Abs. 7 SächsDSG gebotene Benehmen mit dem Sächsischen Datenschutzbeauftragten herbeigeführt worden war.

Hingegen zeigten mehrere Besuche in der Registratur des SMJus, die u. a. die zentrale Verwaltung der Personalnebenakten des höheren Justizdienstes zur Aufgabe hat, dass das dortige Personal kompetent und sachgerecht die Aktenbestände führte.

Eine Fachabteilung des SMJus („Strafrecht“) betrieb die im Dateienverzeichnis als Datei aufgeführte „Statistik zum Stand der Aufarbeitung des ‘SED-Unrechts’“. Als Aufgabe war die „Dokumentierung aller Einzelverfahren und Verfahrensergebnisse“ zum „SED-Unrecht“ nach Erhebung der öffentlichen Klage durch die Staatsanwaltschaft angegeben. Gespeichert waren die Namen aller wegen „SED-Unrechts“ Angeklagten, die Aktenzeichen der Staatsanwaltschaft und des SMJus sowie die Verfahrensergebnisse. Als Rechtsgrundlage für diese automatisierte Datenverarbeitung gab das SMJus § 147 Nr. 2 GVG an; dies ist die Vorschrift, die die Dienstaufsicht der Landesjustizverwaltung über die Staatsanwaltschaft regelt. Diese Vorschrift kommt jedoch nur in dem Umfang als Befugnisnorm für Eingriffe in Grundrechte (Dritter) in Betracht, der für die „Aufsicht und Leitung“ (§ 147 Nr. 2 GVG) der Staatsanwälte im Sinne des verfassungsmäßigen Verhältnismäßigkeitsgrundsatzes geboten ist.

Vor diesem auf dienstrechtliche Aspekte reduzierten Aufsichtshintergrund halte ich es für nicht begründbar, die biographischen Daten der einschlägig Angeklagten sowie die diesen Daten zugeordneten Verfahrensergebnisse dem jederzeitigen Zugriff des Staatsministeriums zu öffnen. Denn eines muss man wissen: Staatsanwälte sind in ihrer Ermittlungstätigkeit Organe der Rechtspflege, so das Bundesverfassungsgericht in ständiger Rechtsprechung. Das Staatsministerium gehört aber zur Exekutive. Wenn also das aus dem Jahr 1878 stammende Gerichtsverfassungsgesetz von „Aufsicht und Leitung“ spricht, so muss man diese Begriffe nach den heutigen verfassungsrechtlichen Grundsätzen auslegen. Der Justizminister ist - entgegen seinen eigenen Verlautbarungen - nicht Repräsentant der 3. Gewalt, er hat nur exekutiv und dienend dafür zu sorgen, dass die Justiz unbeeinflusst und effizient arbeiten kann. Jedes andere amtliche Selbstverständnis ist ein vermeidbarer Irrtum, der fundamentale Folgen für den Rechtsstaat hat und die Unbeirrbarkeit und Neutralität der Staatsanwälte in peinliche Zweifel zieht.

Wenn ein Datenschutzbeauftragter sich darüber Sorgen macht, so ist dies keine Einmischung in fremde Sach- und Rechtsgebiete: Es ist vielmehr sichtbarer Ausdruck dessen, dass die gesetzlichen Regeln zur Verarbeitung personenbezogener Daten über Beschuldigte, Zeugen, Opfer, Sachverständige, aber auch Daten über die sachbearbeitenden Staatsanwälte von der Verfassungslage geprägt und begrenzt werden. Es gehört nicht zu meinen Amtspflichten, die Unabhängigkeit der Judikative, z. B. auch des ermittelnden Staatsanwalts zu verteidigen - dazu sind andere berufen -, aber ich habe ihre Unabhängigkeit zu berücksichtigen, wenn ich mich zur fehlenden Rechtmäßigkeit der Datenverarbeitung durch das SMJus äußere.

„Aufsicht und Leitung“ über die staatsanwaltschaftlichen Beamten können durchgeführt werden, ohne dass es flächendeckend zum Abruf bereitstehender automatisierter Dateien bedarf, deren Inhalte nur zu Ermittlungszwecken im landesweiten staatsanwaltschaftlichen Verfahrensregister abrufbar sind. Erklärungen der Art, dass die Datei „zur Information des Staatsministers“ (so der Leiter der Fachabteilung) zu führen ist, sind nicht geeignet, den in Grundrechte Dritter eingreifenden Dateieinsatz zu rechtfertigen. Sie sollten nicht den Eindruck vermitteln, der Staatsminister sei der „Oberste Staatsanwalt“. Das SMJus hat mir inzwischen mitgeteilt, dass es die vorgenannte Datei nicht weiter betreiben wird.

Die in einer weiteren Fachabteilung („Justizvollzug“) durchgeführten datenschutzrechtlichen Prüfungen ergaben keine Anhaltspunkte für Datenschutzverstöße. Bei der Datenverarbeitung dieser Fachabteilung war ihre Praxis positiv hervorzuheben, z. B. BStU-Unterlagen zu ausgeschiedenen Mitarbeitern nach Beendigung des jeweiligen Dienst-/Arbeitsverhältnisses und evtl. damit zusammenhängender Gerichtsverfahren dem BStU zurückzusenden.

Die Personaldatenverarbeitung im SMJus (Abteilung „Allgemeine Verwaltung“) ergab folgendes Bild:

- Wie bereits oben ausgeführt, wurden die *automatisierten Dateien* der Personalabteilung, die Beschäftigtendaten enthielten, betrieben, ohne dass das gesetzliche Verfahren nach § 31 Abs. 7 SächsDSG beachtet worden war.

Im Einzelnen begegneten folgende automatisierten Dateien meiner Kritik:

- Die „Bewerberdatei“ enthielt Daten zum Klausurendurchschnitt der Bewerber für den höheren Justizdienst (Richter, Staatsanwälte). Ungeachtet der Tatsache, dass die Validität dieser Datei angesichts der Unterschiedlichkeit der Bewertungsmaßstäbe (Notenskalen) der Bundesländer und der gleichzeitigen Einstellung der Daten von Bewerbern mit und ohne Staatsexamen zu bezweifeln ist, fehlt es an einer die Grundrechtseingriffe rechtfertigenden Rechtsgrundlage.

- Dieses Manko besteht auch bei den Dateien „Examensnoten“ und „Regelbeurteilungen“. Bei Letzterer war besonders die Möglichkeit zu kritisieren, im Bestand aller Richter und Staatsanwälte des Freistaates Sachsen automatisiert Recherchen nach Examens- und Beurteilungsnoten durchzuführen. Ausweislich

des Dateienverzeichnisses dient diese Datei der „Vorbereitung von Personalentscheidungen“. Ich habe gegenüber dem SMJus mit Nachdruck deutlich gemacht, dass das SMJus mit dem Betrieb dieser Datei Gefahr läuft, gegen die EG-Datenschutzrichtlinie zu verstoßen, die in Art. 15 ein Verbot automatisierter Einzelentscheidungen statuiert. Denn die komfortable Recherchemöglichkeit nach Examensnoten birgt die Gefahr, dass bei der (die Personalentscheidung vorbereitenden) Sachbearbeitung „automatisiert vorgefiltert“ wird. Weder Examensnoten noch (Regel-)Beurteilungen sind für sich allein Maßstäbe für Personalentscheidungen, die nach Eignung, Befähigung und Leistung sowie nach den gesetzlichen Regeln zu erfolgen haben. Welche sachliche Bedeutung für eine Vorschlags- oder Beförderungsentscheidung z. B. eine 20 Jahre alte Examensnote haben soll, konnte mir niemand begründen.
Gesprächen, die ich aus Anlass meines Kontrollberichts mit dem SMJus geführt habe, entnahm ich, dass das SMJus diese Dateien auflösen wird, nachdem ein automatisiertes, zentrales Personalinformationssystem eingeführt worden ist. Sollte sich dessen Einführung jedoch verzögern, werde ich den weiteren Betrieb der vorgenannten automatisierten Dateien beanstanden.

Bei der *Personalaktenführung* des SMJus sind folgende Mängel zutage getreten:

- Häufig befanden sich in den Akten Vermerke des Personalreferates zum Vorstellungsgespräch der (später eingestellten) Bewerber. Die Vermerke enthielten vielfach negative und subjektiv geprägte Einschätzungen über den Bewerber. So wurde vermerkt: Der Bewerber mache einen „glatten“ Eindruck (mehrfach festgestellter Vermerk) oder „... in Stresssituationen ist er nicht in der Lage zur Schwerpunktsetzung und schnellen Entscheidung“ oder „er spricht sehr schnell“. Solche Dinge gehören nicht in Personalakten; sie sind zu vernichten.

- Auch finden sich in den Personalnebenakten belastende Vermerke des Personalreferates; z. B. „Leistungen lassen zu wünschen übrig ...“; „Problemfall“; „... geplanter Urlaub storniert (Kosten: 50 % des Reisepreises), um seinen Arbeitsrückstand aufzuholen“. Akteninhalte dieser Art sind für die Bediensteten ungünstig oder können für sie nachteilig werden. Deshalb sieht die Verwaltungsvorschrift Personalakten Beamte vom 11. Dezember 1998 (SächsABl. vom 14. Januar 1999, S. 10) unter C vor, dass die Bediensteten über solche Bewertungen zu informieren sind. Die kontrollierten Personalnebenakten ließen infolge Fehlens einschlägiger Vermerke nicht erkennen, dass dieses Anhörungsrecht durch das Personalreferat gewährleistet wurde. Ich habe daher das SMJus dringend aufgefordert, die Praxis der Personalreferate an der verfassungsmäßigen Rechtsschutzgarantie auszurichten.

- Schließlich habe ich die Verwendung von in den Akten enthaltenen ausgefüllten Formblättern mit der Erklärung „Ich bin weder mit einem Richter noch mit einem Staatsanwalt, Rechtsanwalt oder Notar verwandt oder verschwägert“ kritisiert, weil sie einer Rechtsgrundlage entbehrt. Selbst auf die allgemeinen Datenerhebungsbefugnisse des Sächsischen Datenschutzgesetzes (§ 11) kann diese Erfassung von Verwandschaftsverhältnissen nicht gestützt werden, zumal sie nicht

zur Aufgabenerfüllung (hier: Personalverwaltung) des SMJus erforderlich ist. Die Vernichtung der Formblätter und die Löschung der mit ihnen erhobenen Daten habe ich angemahnt.

- Weitere datenschutzrechtliche Verstöße gegen Grundsätze der Personalaktenführung habe ich auch darin gesehen, dass in den Personalnebenakten der Personalabteilung Schriftstücke mit sensitiven Gesundheitsdaten (z. B. Schwangerschaftsdiagnosen mit Daten zu Kindsbewegungen und serologischen Untersuchungsergebnissen) unverschlossen abgeheftet waren sowie Kopien von Lohnsteuerkarten in Teilakten aufbewahrt wurden.

Das SMJus hat mir inzwischen versichert, im Rahmen einer umfassenden Bereinigungsaktion diese Mängel abzustellen. Ich hoffe, das geht flott.

8.1.2 Kontrolle der Personalakten bei einem Landgericht und bei einem Verwaltungsgericht

Damit die im SMJus aufbewahrten Personalnebenakten mit den bei den dienstaufsichtsführenden Präsidialgerichten geführten Personalgrundakten verglichen werden konnten, umfasste die Kontrolle auch die Bestände zweier Präsidialgerichte. Abgesehen von Mängeln wie fehlende Inhaltsverzeichnisse sowie fehlende Hinweise auf Teil- und Nebenakten fielen folgende datenschutzrechtliche Defizite auf:

- So enthielt eine drei Seiten umfassende Beurteilung durch den Präsidenten des Gerichts zunächst ein Formblatt, die zweite Seite war bis zur Hälfte mit Text beschrieben und die dritte völlig leere Seite trug am unteren Seitenrand - quasi als Blankett - die Unterschrift des Präsidenten.

- Einige Akten enthielten neben den Beurteilungen auch deren Entwurf und Vorentwurf.

- Eine Beurteilung enthielt unter Nennung der Parteien eine Liste von Verfahren, die der Richter bearbeitet hatte, sowie Bemerkungen des Beurteilers wie „seither geschieht nichts“ und „noch nichts geschehen“. Inhalte einzelner Prozesse haben in den Personalakten des zuständigen Richters aber nichts verloren.

- Eine Beurteilung (mit dem Abschlussvotum „nicht geeignet“) war ausweislich der Aktenlage des Gerichts per Telefax an das SMJus übermittelt worden. Es bedarf keiner weiteren Ausführungen, dass sich diese gewählte Übertragungsart für Übermittlungen von Daten der bezeichneten Qualität verbietet. Ich verweise insofern auf meine Bekanntmachung vom 14. Juni 1993 zum Gebrauch der Telefax-Übertragung (SächsABl. vom 8. Juli 1993, S. 894).

- In einigen Fällen waren amtsärztliche Zeugnisse sowie Bescheinigungen über die Schwangerschaft unverschlossen abgeheftet. Des Weiteren befanden sich in den Akten Kopien von Lohnsteuerkarten längst vergangener Jahre. Eine plausible Begründung konnte hierfür nicht gegeben werden.

Auf meine Kritik an dieser Personalaktenführung bei den Gerichten hat das SMJus reagiert und zugesichert, die gebotene Aktenbereinigung zu veranlassen. Ich werde in diesem Jahr kontrollieren, ob dies geschehen ist.

8.1.3 Kontrolle beim Oberlandesgericht

Die Kontrolle der Personalakten im SMJus und bei den dienstaufsichtsführenden Präsidialgerichten zeigte, dass in der sächsischen Justizverwaltung von dem in der Personalaktenführung geltenden Prinzip der Einheitlichkeit der Personalakte nicht gesprochen werden kann. Denn die beim dienstaufsichtsführenden Gericht geführte Akte und die ihr korrespondierende SMJus-Akte sind grundsätzlich - jedenfalls nach dem Willen des SMJus - von gleichem Umfang und Inhalt. Insofern wird die Vorgabe der Verwaltungsvorschrift zur Personalaktenführung, wonach eine Grundakte besteht und die Führung von Teil- und Nebenakten erlaubt ist, von der Praxis der Justizverwaltung nicht beachtet. Hinzukam, dass die Akten nicht selten ganz unterschiedliche Informationen enthielten.

Das Beamtenrecht (§ 117 SächsBG) sieht die Führung *einer* Personalakte vor, die nach sachlichen Gesichtspunkten - entsprechend den gesetzlichen Aufgaben der jeweils zuständigen Behörde - in Grund-, Teil- und Nebenakten gegliedert werden kann. Nebenakten dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerfüllung unerlässlich ist.

Hinzu kommt, dass - wie sich während der Kontrolle herausstellte - eine weitere Stelle eine Personalakte führt: das OLG. Die Überprüfung der dortigen Personaldatenverarbeitung ergab Folgendes:

- Das OLG betrieb mehrere automatisierte Verfahren zur Verarbeitung von Beschäftigtendaten. Das nach § 31 Abs. 7 SächsDSG gebotene Benehmen mit dem Sächsischen Datenschutzbeauftragten war einzig für die Telekommunikations-Anlage und das an diese gekoppelte Zeiterfassungssystem hergestellt.

- Das - vom Vortag der angekündigten Kontrolle datierende - Dateien- und Geräteverzeichnis entsprach nicht in allen Fällen den tatsächlichen Anwendungen: So umfasste die Datei „Beurteilungsfristen“, die allein der Verwaltung von Beurteilungsterminen dient, Felder, in denen - den Bediensteten zugeordnet - pauschale Wertungen wie „geeignet“ und „nicht geeignet“ festgehalten wurden. Aufgrund meiner Kritik sicherte der Präsident des OLG noch während der Kontrolle zu, diese Daten der Datei zu löschen.

- Die Kontrollen der Personalakten, die vom OLG bzw. dem Generalstaatsanwalt geführt werden und die den gesamten Personalbestand des höheren Dienstes der ordentlichen Gerichtsbarkeit bzw. der Staatsanwaltschaften umfassen, zeigte, dass auch im OLG komplette Personalgrundakten geführt werden, die in Umfang und Detailfülle den zusätzlich im SMJus und den bei den Gerichten geführten gleichkommen. Als Begründung gab das SMJus später das Bedürfnis der sächsischen

Justizverwaltung an, einen landesweiten „Überblick“ über den Personalkörper besitzen zu müssen. Dies entspräche auch der Praxis in einigen anderen Bundesländern.

Eine Rechtsgrundlage für eine solche - angebliche - „Praxis“ ist nicht ersichtlich. Von der Beachtung des Verhältnismäßigkeitsprinzips - zu welcher (Allein-)Entscheidung sind welche Daten geeignet und erforderlich - kann auch nicht ansatzweise die Rede sein. Für den Betroffenen ist es unerträglich, sich drei komplette Personalakten führenden Stellen ausgeliefert zu sehen, die - wie die Beispielsfälle erwiesen - speichern, was ihnen gerade in den Sinn kommt, ohne dass ein klares Regelwerk über Aufgaben, Befugnisse und Beteiligungsformen besteht, das die Datenverarbeitung ordnet, vorhersehbar macht und auf das geeignete und erforderliche Maß beschränkt. Ich erwarte, dass das SMJus ein solches Regelwerk zur Führung der Personalakten (u. a. zu Zweck, Ort, Inhalt, Löschung, Verantwortlichkeiten) erstellt, wenn es überhaupt begründen kann, in der Justiz sei eine Abweichung von den allgemeinen Grundsätzen der Personal(akten)führung rechtmäßig und nötig. Gründe dafür sind hier bislang nicht bekannt geworden. Ich muss - wegen der Rechtslage - darauf bestehen, dass *eine* Personalakte (mit Teil- und Nebenakten zu klar bestimmten Zwecken) geführt wird.

8.1.4 Zusammenfassung

Die Querschnittskontrolle hat die strukturellen Datenschutzdefizite der Personalaktenführung der sächsischen Justizverwaltung offen gelegt. Aus guten Gründen ist die Einheitlichkeit der Personalakte althergebrachtes Prinzip einer ordnungsgemäßen und Belange des Dienstherrn wie des Bediensteten wahrenden Aktenführung. Dieses Prinzip hat die einschlägige sächsische Verwaltungsvorschrift konsequent umgesetzt; in der sächsischen Justizverwaltung scheint es hingegen unbekannt zu sein.

Welche Gründe das SMJus bewegen, von dieser „monolithischen“ Struktur der Personalakte abzuweichen und - wie die Kontrolle gezeigt hat - parallel drei Personalgrundakten unter großem Aufwand führen zu lassen, deren überwiegender Inhalt identisch ist, konnten die Beamten - auch in Besprechungen im Anschluss an die Kontrolle - nicht plausibel dartun, sondern nur auf den persönlichen Willen des Staatsministers verweisen. Spezielle, nur im Bereich der Justiz auftauchende Aufsichts- und Kontrollaufgaben, die nur mit dieser „Dreigleisigkeit“ bewältigt werden könnten, gibt es nicht. Das deutsche Richtergesetz will nicht, dass ein Richter sich „personalpolitisch flexibel“ zeigt, es will ihn vielmehr fest auf seiner Stelle, unbeeinflusst von (im Ergebnis der Kontrolle: unklaren) Absichten einer Personalverwaltung, deren Datensammlungen und ihren Auswertungen. Die Personaldatenverarbeitung der sächsischen Justiz durch die Justizverwaltung habe ich in einem schlechten Zustand vorgefunden. Ich fordere: Weil Staatsanwälte weitgehend und Richter völlig unabhängig arbeiten müssen, müsste die personalrechtliche dienstaufsichtliche Datenverarbeitung auf das erforderliche Minimum reduziert werden.

Wegen der Bedeutung der Sache habe ich mir gegenüber dem SMJus vorbehalten, mich an den Sächsischen Landtag zu wenden.

8.2 Unterlassung staatsanwaltschaftlicher Ermittlungstätigkeit

Eine sächsische Staatsanwaltschaft untersuchte im Rahmen eines Prüfungsvorgangs (sog. AR-Verfahren; es dient zur Prüfung, ob zureichende Anhaltspunkte für einen aufklärungsbedürftigen strafrechtlichen Vorwurf vorliegen) mehrere strafrechtlich relevante Vorwürfe, die ein auf Grund eigenen Geständnisses verurteiltes Mitglied eines „Kinderschänderringes“ gegen ein Mitglied des Sächsischen Landtages erhoben hatte. Nach der Personalienfeststellung möglicher Zeugen unter Beiziehung einschlägiger Verfahrensakten sowie weiterer Aufklärungshandlungen berichtete der Leitende Oberstaatsanwalt der Generalstaatsanwaltschaft sowie dem SMJus, dass nun konkrete Ermittlungen veranlasst und beabsichtigt seien, die er im Einzelnen aufführte. Dem Bericht war beigefügt der Entwurf eines bereits ausformulierten Schreibens des Leitenden Oberstaatsanwaltes an den Präsidenten des Sächsischen Landtages als Anzeige der Immunitätsaufhebung.

Zur Einleitung eines förmlichen Ermittlungsverfahrens kam es jedoch nicht, weil das SMJus ausweislich der Aktenlage auf das Verhalten der Generalstaatsanwaltschaft insoweit einwirkte, als gebeten wurde, die Staatsanwaltschaft dahin zu beeinflussen, die Versendung des vorgenannten Schreibens an den Landtagspräsidenten „zurückzustellen“. Ob diese Einflussnahme eine förmliche „Weisung“ war, konnte dahinstehen: Wie aus den Akten ersichtlich, sollten Maßnahmen „angeregt“ und von einer „schriftlichen Weisung“ abgesehen werden. So geschah es denn auch: Die Anregung erfolgte fernmündlich und der zuständige Beamte der Generalstaatsanwaltschaft hatte dafür „Sorge zu tragen“, dass das Verfahren abgeschlossen wurde, also eine Datenverarbeitung im Ermittlungsverfahren nicht stattfand. Spätere Remonstrationen der Staatsanwaltschaft blieben unbeachtet.

Begründet wurde die vom Staatsminister persönlich ausgelöste Einflussnahme auch mit der angeblichen Gefahr einer Persönlichkeitsrechtsverletzung durch Veröffentlichung personenbezogener Daten des Abgeordneten im Zuge eines Ermittlungsverfahrens. Das kam an die Öffentlichkeit.

Wegen der datenschutzrechtlichen Bedeutung des Falles habe ich mich gemäß § 27 Abs. 2 SächsDSG an den Landtag gewandt und ein Gutachten mit der folgenden Bewertung vorgelegt:

Das Unterlassen von Ermittlungshandlungen ist integraler Bestandteil des Datenschutzrechts. Denn gemäß § 160 Abs. 2 StPO hat die Staatsanwaltschaft nicht nur die zur Belastung, sondern auch die zur Entlastung dienenden Daten zu erheben und zu verarbeiten. Damit ist aus der Sicht des betroffenen Einzelnen garantiert, dass die Datenverarbeitung der Staatsanwaltschaft nach objektiven Gesichtspunkten erfolgt und auch dazu dient, Vorwürfe vom Betroffenen zu nehmen, wenn sie sich als ungerechtfertigt erweisen sollten. Daher wirkt das Aufrechterhalten einer ungesicherten Ermittlungssituation persönlichkeitsrechtswidrig, wenn bereits - wie hier - Vorwürfe öffentlich erörtert und benannt werden. Die Ermittlungsbehörden haben gegenüber dem Beschuldigten die Amtspflicht, Verdachtsmomente gründlich zu ermitteln. Ein Verstoß dagegen vermag zwar - wegen der gesetzlichen Unschuldsvermutung -

keinen subjektiven Anspruch des Beschuldigten begründen, auch dann die Ermittlungen fortzuführen, wenn die Staatsanwaltschaft keinen hinreichenden Tatverdacht sieht. Gerade dies war aber vorliegend nicht der Fall. Weil die Staatsanwaltschaft zunächst begründeten Anlass für ein Ermittlungsverfahren sah (und dies auch später bekannt wurde), wirkte es persönlichkeitsrechtsverletzend, wenn (dann) nicht weiter ermittelt wurde. Nur durch Ermittlungen - als zwingender Teil rechtsstaatlichen Zusammenlebens - kann garantiert werden, dass Verdächtigungen, Anwürfe und Nachreden aus der Ebene des Unverantwortlichen und Ehrenrührigen in rechtsstaatliche Dimensionen gehoben und damit nachweisbar, d. h. überprüfbar werden und somit zu verantworten sind. Wer es unterlässt, strafrechtlich relevanten Vorwürfen mit den gebotenen Mitteln der Rechtsordnung nachzugehen, läuft Gefahr, sich dem Angriff auszusetzen, er könne den diffusen Anwürfen gegen den Betroffenen auch in Zukunft nicht ordnungsgemäß entgegentreten oder er wolle dem Betroffenen selbst diese Möglichkeit vorenthalten.

Im Sinne des Grundsatzes der Verhältnismäßigkeit sind nur vollständige Ermittlungshandlungen zur Wahrheitsermittlung geeignet.

Die Verpflichtung, allen strafrechtlich relevanten - erst recht öffentlichen - Vorwürfen mit den gebotenen Mitteln nachzugehen, ist ein objektives Gebot des Rechtsstaates, das sich von Rechts wegen den subjektiven Bewertungen einer Person, die nicht Staatsanwalt ist, entzieht. Die gesetzlich gebotene Datenverarbeitung gemäß § 160 StPO hat nicht nach subjektiv als belastend empfundenen Beeinträchtigungen des Betroffenen, sondern nach der Dringlichkeit des Tatverdachts zu fragen. Ein solch missverstandener Datenschutz wäre Täterschutz. Denn es ist eine illegitime Erwägung, Ermittlungen etwa zu unterlassen, wenn ein Prominenter betroffen ist.

Eine davon zu unterscheidende Frage ist es, dass die gebotenen Ermittlungshandlungen datenschutzgerecht, also das Persönlichkeitsrecht schonend, durchgeführt werden. Dieser Datenschutz darf aber keinen Einfluss darauf haben, *ob* ermittelt wird.

Unter den vorgenannten Aspekten begegnet ein externes - d. h. seitens des SMJus wahrgenommenes - Weisungsrecht erheblichen rechtsstaatlichen Bedenken, wenn im konkreten Einzelfall die Unterlassung von Ermittlungshandlungen „erbeten“ wird. Auf spätere Nachfrage hat der Staatsminister der Justiz mit seinen Spitzenbeamten großen Wert darauf gelegt, dass seine Anregungen oder Bitten, die er der Staatsanwaltschaft über die Generalstaatsanwaltschaft übermitteln ließ, keine förmlichen Weisungen, sondern eher so etwas wie Ratschläge seien. Das hört sich so leise und vornehm an, dass dem Uneingeweihten dieses Zusammenspiel als Harmlosigkeit vorkommt. Richtig ist, dass sich hinter diesen vermeintlich kollegialen Tönen ein stringenter und kategorischer Vorgesetztenukas verbirgt. So sind halt die Formulierungen: Hinter zurückhaltenden Worten stehen traditionell klare Verbindlichkeiten, Befehl und Gehorsam. Und nur der Eingeweihte weiß, dass so ein bestimmender Einfluss auf Art, Umfang und Auswertung der Ermittlungsdaten genommen wird und genommen wurde.

Geschieht dies ohne Kenntnis der Gesamtumstände, d. h. ohne Kenntnis der bereits angelegten Akten und ohne die fallbezogene Kenntnis des allein sachbearbeitenden Staatsanwalts, so ist eine derartige, unter dem Gesichtspunkt der verfassungsrechtlich gebotenen Unschuldsvermutung vorgenommene Unterlassung gebotener Datenverarbeitung ein Eingriff in das Persönlichkeitsrecht. Die vom SMJus vorgenommene Einflussnahme war daher aus Datenschutzgründen rechtswidrig.

Ich habe die Gelegenheit wahrgenommen, meinen Rechtsstandpunkt in einer Sitzung des Verfassungs- und Rechtsausschusses des Sächsischen Landtages darzulegen.

8.3 Dienstaufsicht durch das SMJus

Mit dem Entwurf eines Sächsischen Justizgesetzes (SächsJG) wollte die sächsische Staatsregierung etwas regeln, was in bundesgesetzlichen Vorschriften (§ 26 DRiG und § 147 GVG) - durchaus nuanciert formuliert - bereits geregelt ist, nämlich: Die Dienstaufsicht über die ordentliche Gerichtsbarkeit und die Staatsanwaltschaften soll das SMJus ausüben. Diese lapidar gehaltene Zuweisung von Eingiffsbefugnissen, die mit der Verarbeitung oft sensibler Personaldaten einhergeht, habe ich in einer Stellungnahme gegenüber dem SMJus aus den folgenden Gründen problematisiert:

- Dienstaufsicht über Richter

  Voraussetzung für die Zuweisung von Aufgaben und Befugnissen an die über Richter aufsichtsführenden Behörden, also auch Voraussetzung für die Legitimität ihrer Datenverarbeitung und deren Zwecke, ist die richterliche Unabhängigkeit, die nach dem Wortlaut des § 26 DRiG die rechtmäßigen Zwecke einer Verarbeitung personenbezogener Daten bestimmt und begrenzt. § 26 Abs. 1 DRiG lautet: „Der Richter untersteht einer Dienstaufsicht nur, soweit nicht seine Unabhängigkeit beeinträchtigt wird.“ Deshalb ist jede Verarbeitung personenbezogener Daten, die zum Zweck der Durchführung von Handlungen stattfindet, mit denen eine dienstaufsichtsführende Stelle die Unabhängigkeit des Richters beeinträchtigt, von vornherein rechtswidrig.

  Daher musste ich im Berichtszeitraum gegenüber dem SMJus eine förmliche Beanstandung aussprechen: Das Staatsministerium hatte nämlich versucht, per Erlass einzelne verfahrensbezogene Informationen über die richterliche Termingestaltung eines Verwaltungsgerichts in Erfahrung zu bringen. Die Terminierung des einzelnen Prozesses ist aber ureigene richterliche, d. h. ministeriell unbeeinflussbare Tätigkeit; deshalb gehen das Staatsministerium personenbezogene Daten im Zusammenhang mit der Terminierung bestimmter Prozesse - mit Verlaub - nichts an. Ihre Erhebung ist rechtswidrig. Als Ausnahme ließe sich allenfalls denken, dass das Staatsministerium sich auf konkretes fallbezogenes Beschwerdevorbringen hin einschaltet, wenn z. B. Tatsachen den hinreichenden Verdacht begründen würden, dass ein Richter aus persönlichem Interesse eine bestimmte Prozesspartei bewusst benachteiligt hätte. Solche Fälle sind bislang aber in der sächsischen Justiz unbekannt.

- Dienstaufsicht über die Staatsanwälte

  Bei dieser Aufsichtskonstellation ist zu beachten, dass das externe Weisungsrecht des Staatsministers der Justiz keinesfalls dem Legalitätsprinzip widersprechen darf; die Staatsanwaltschaft ist nicht „verlängerter Arm" der Exekutive (vgl. zum Stand der Diskussion Karlsruher Kommentar zur Strafprozeßordnung, 4. Auflage 1999, § 146 GVG, Rdnr. 2; § 141 GVG, Rdnr. 3). Weder in Rechtsprechung noch Literatur sind bislang Stimmen bekannt geworden, die es unter Beachtung der vorgenannten Grundsätze in Betracht ziehen, das Justizministerium etwa als „Wächter des Gesetzes" in Bezug auf die Tätigkeit der Staatsanwaltschaft anzusehen. Denn das Staatsministerium der Justiz handelt primär und legitimerweise nach politischen Erwägungen auf der Grundlage des Prinzips der Opportunität. Demgegenüber ist die Staatsanwaltschaft strikt an das Legalitätsprinzip gebunden; auf der ministeriellen Seite handelt die Exekutive; die Staatsanwaltschaft wird als Organ der Rechtspflege und damit - jedenfalls in ihrer Ermittlungstätigkeit - als Teil der Judikative angesehen (BVerfGE 32, 199 ff. [216]). Nach anderer wissenschaftlich begründeter Auffassung gilt sie als eine Gewalt „sui generis". Die Rechtspflege ist jedenfalls nach dem rechtsstaatlichen Prinzip der Gewaltenteilung frei von Einflussnahme durch die Exekutive. Daraus folgt, dass das externe Weisungsrecht des Staatsministers nicht zur Beeinflussung der Staatsanwälte in fachlichen Einzelfragen konkreter Ermittlungsverfahren berechtigt. Das bedeutet, dass die Datenverarbeitung im Rahmen staatsanwaltschaftlicher Ermittlungstätigkeit nicht durch das Staatsministerium gesteuert werden darf.

  Die Verwaltungsvorschrift, die Staatsanwaltschaften müssten dem SMJus über den Generalstaatsanwalt über solche Verfahren berichten, die „die Öffentlichkeit, insbesondere auch parlamentarische oder sonstige politische Kreise beschäftigen oder voraussichtlich beschäftigen werden" (VwV OrgStA vom 12. Januar 1998), kann sich nicht auf das Gesetz stützen. Sie ist rechtswidrig, weil „Aufsicht und Leitung" i. S. des § 147 GVG nur unter sachlichen Gesichtspunkten - z. B. sachliche oder persönliche Folgen einer Tat, Strafmaß oder auch besondere juristische Schwierigkeiten - stattfinden dürften. Politische, d. h. etwa von der öffentlichen Meinung getragene oder ihr angepasste Einflüsse sind niemals gestattet. Deshalb ist der Auslöser der Berichtspflicht in der Verwaltungsvorschrift grundfalsch gewählt: Öffentliches Aufsehen ist in der heutigen Welt kein sachlicher Maßstab. Hinzutritt, dass unter dem Gesichtspunkt der Gewaltenteilung eine sachliche Einflussnahme des Staatsministeriums aus politischen Gründen im Einzelfall unerträglich wäre. Die Vergangenheit hat bewiesen, dass exekutiver oder gar - von welchen Motiven auch immer getragener - politischer Einfluss auf strafrechtliche Ermittlungen dem Rechtsstaat an die Substanz geht. Ich fordere das SMJus auf, die Verwaltungsvorschrift zu ändern.

Zusammengefasst:
Die Chance, im Rahmen eines Sächsischen Justizgesetzes das Prinzip einer gestuften Dienstaufsicht unter Berücksichtigung der vorstehenden Erwägungen einzuführen, wie es sich aus dem Verhältnismäßigkeitsgrundsatz und der Gewaltenteilung zwingend ergibt (auch in § 38 VwGO einen verbindlichen Niederschlag gefunden hat),

sollte genutzt werden. Der verfassungsmäßige Grundsatz der Verhältnismäßigkeit verpflichtet zur Beachtung des Prinzips der Subsidiarität der jeweiligen dienstaufsichtsführenden Stellen; eine Übermittlung personenbezogener Daten darf daher an die jeweils nächsthöhere dienstaufsichtsführende Stelle nur dann und soweit erfolgen, wenn diese Daten zur Aufgabenerledigung geeignet und erforderlich sind. Nur bei einer entsprechenden Ausgestaltung einer sächsischen Gesetzesregelung könnte dies gestattet sein - in der Form des Gesetzentwurfs jedenfalls bleibt sie infolge des Defizits an Normenklarheit hinter den ohnehin zu beachtenden Vorschriften des Deutschen Richtergesetzes und des Gerichtsverfassungsgesetzes zurück. So wie die Vorschrift im Entwurf formuliert war, wäre sie überflüssig und rechtswidrig. In diesem Zusammenhang sei noch Folgendes angemerkt:

In früheren Gesprächen haben Mitarbeiter des SMJus angedeutet, Aufsichtsmaßnahmen dienten „der politischen Information des Staatsministers“. Da der Staatsminister keineswegs der Repräsentant der Dritten Gewalt ist, sondern als Exekutive auf gesetzlich zugewiesene - und verfassungskonform begrenzte - Aufgaben und Befugnisse beschränkt wird, kommt ein allgemeines Informationsrecht des Staatsministers ohne normenklare Rechtsgrundlage in Bezug auf personenbezogene Daten nicht in Betracht. Dies werde ich auch bei künftigen Kontrollen berücksichtigen. Jedenfalls stehen dem Staatsminister personenbezogene Informationen aus laufenden Ermittlungsverfahren - ohne konkreten dienstaufsichtlichen Anlass - nicht zu.

8.4 DNA-Analyse zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

Mit dem vor zwei Jahren in Kraft getretenen DNA-Identitätsfeststellungsgesetz ist in der Strafprozessordnung gesetzlich geregelt, dass im Bundeskriminalamt eine zentrale Datei über schwer straffällige Personen mit ungünstiger Prognose aufgebaut wird, in der die unverwechselbaren DNA-Analysedaten der einzelnen Betroffenen gespeichert werden. In Zukunft soll an Tatorten Zellmaterial (z. B. Haare, Blut, Körpersekrete, Zigarettenkippen mit Speichelanhaftungen etc.) gesammelt, analysiert und mit der Datei verglichen werden. Dies ermöglicht die sichere Erkenntnis, dass sich eine ganz bestimmte Person am Tatort aufgehalten bzw. sich an einem Opfer vergriffen hat. Damit werden die Methoden und konkreten Möglichkeiten zur sicheren Straftäterbestimmung entscheidend verbessert.

Ich habe dieses Verfahren von Anfang an positiv begleitet und halte die Datei für eine rechtsstaatlich einwandfreie und überaus erfolgreiche Methode, Straftaten aufzuklären - vorausgesetzt, die gesetzlichen Verfahrensvorschriften, die dem rechtsstaatlichen Schutz der Betroffenen dienen, werden eingehalten.

Weil jeder, der mit seinen DNA-Analysedaten unverwechselbar in die Datei aufgenommen wird, als potentieller Straftäter, d. h. als rückfallgefährdet unterschiedslos für alle schweren Straftaten, also z. B. auch für Sexualstraftaten gilt, ist es für jeden sicherlich mit einem schwer wiegenden gesellschaftlichen Makel verbunden, wenn er in die Datei aufgenommen wird. Dies auch deshalb, weil die Löschung der Daten selbst bei guter Führung und Rückfallfreiheit ungesichert ist.

Wegen dieser besonderen Bedeutung der Datei bedarf die Prognose, ob aus vergangenen Taten und aus der Täterpersönlichkeit auf Rückfallgefahren geschlossen werden kann, einer richterlichen Anordnung. Dies ist im Gesetzestext des § 81 g StPO geregelt; dort heißt es, dass die Entnahme von Körperzellen und deren Untersuchung nur angeordnet wird, „wenn wegen der Art und Ausführung der Tat der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sind". Weiter verweist die Vorschrift dann auf § 81 f StPO: Die Untersuchungen werden durch den Richter angeordnet.

Das Verfahren ist also im Gesetz rechtsstaatlich einwandfrei und vernünftig geregelt. Dennoch ist es im Freistaat Sachsen Praxis, die Prognoseentscheidung und die anschließende Untersuchung auf der Grundlage einer Entscheidung der Gefangenen durchzuführen. Die Gefangenen werden aber über die Tragweite und die Konsequenzen ihrer Entscheidungen nur bruchstückhaft informiert. Weil nämlich das SMJus der Auffassung ist, dass die Fülle der anstehenden Entscheidungen durch die sächsische Richterschaft nicht erbracht werden könnten, wird versucht, auf die Strafgefangenen zuzugehen und sie zu bitten, „freiwillig" mit einer Entnahme und Analyse ihrer Körperzellen (Speicheltest) einverstanden zu sein, obwohl dies nicht durch den gesetzlichen Richter, sondern nur durch die Staatsanwaltschaft angeordnet ist. Der klare Gesetzestext wird damit umgangen. Denn die Prognoseentscheidungen sind keine Willensentscheidungen der Gefangenen, sondern müssen durch einen unabhängigen Richter nach objektiven Maßstäben getroffen werden. Grundrechtsschützende Verfahrensvorschriften können in einem Rechtsstaat nämlich über Einwilligungen nicht zur Disposition der Betroffenen gestellt werden. Das ist in einer Reihe anderer Bundesländer erkannt worden. Dort wird nur auf der Grundlage einer richterlichen Entscheidung gehandelt.

Ich habe deshalb die sächsische Praxis gegenüber dem verantwortlichen Staatsministerium der Justiz wegen Verstoßes gegen die persönlichkeitsrechtsschützenden Vorschriften der Strafprozessordnung gemäß § 26 SächsDSG beanstandet. Weil meine Beanstandung jedoch unberücksichtigt blieb, habe ich mich an die Anstaltsbeiräte der sächsischen Justizvollzugsanstalten gewandt, damit die Strafgefangenen in geeigneter Weise auf die Problematik aufmerksam gemacht werden. Denn jeder Strafgefangene, der seine Daten durch seine Einwilligung in die Zentraldatei einstellen lässt, sollte wissen, dass er sich damit selbst gegen seine eigene positive Sozialprognose entscheidet. Er äußert nämlich damit, dass Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen schwerer Straftaten zu führen sind. Er qualifiziert sich damit selbst als einen potentiellen Wiederholungstäter. Ferner erklärt er sich selbst damit einverstanden, dass er auch künftig in den Kreis von Verdächtigen x-Beliebiger schwerer Straftaten gehört.

Weil sich bei dieser Thematik erweist, in welchem Maße der Staat tatsächlich rechtsstaatliche Grundsätze einhält, werde ich auch künftig alle Anstrengungen unternehmen, die sächsische „Einwilligungspraxis" zu stoppen.

8.5 Forschungsvorhaben zur Telefonüberwachung (TÜ)

Das SMJus bat mich, die datenschutzrechtliche Zulässigkeit eines Forschungsvorhabens zu prüfen, das das BMJ beim Max-Planck-Institut für ausländisches und internationales Strafrecht - ein privater Forschungsträger - in Auftrag gegeben hatte.

Ziel des Projektes ist es, auf wissenschaftlicher Basis Kriterien zu finden, um die Rechtsgrundlagen für Eingriffe in das durch Art. 10 GG geschützte Brief-, Post- und Fernmeldegeheimnis grundrechtskonform neu zu gestalten und die Praxis daran auszurichten. Dazu sollen (möglichst abgeschlossene) Ermittlungsakten der Staatsanwaltschaften sowie Strafprozessakten der Gerichte analysiert werden, die Anordnungen zur Telekommunikationsüberwachung nach §§ 100 a, 100 b StPO enthalten. Ergänzt wird dieser Datenbestand durch Interviews mit den Amtsträgern, denen in den Verfahren die Sachbearbeitung oblag.

Bei der datenschutzrechtlichen Bewertung des Forschungsvorhabens, das ich grundsätzlich als wünschenswerte Evaluierungsmaßnahme ansehe, bin ich zu folgendem Ergebnis gelangt:

Wenn personenbezogene Daten, über die öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung verfügen, für Forschungszwecke genutzt werden sollen, bedeutet dies eine Änderung des ursprünglichen Verwendungszwecks, die einer rechtlichen Grundlage bedarf (vgl. insbesondere Art. 6 Abs. 1 b EG-Datenschutzrichtlinie). Als einzige auf den TÜ-Bereich ausgerichtete spezielle Zweckbindungsregelung existiert lediglich die Vorschrift des § 100 b Abs. 5 StPO. Diese Vorschrift ist für die vorliegende Fallkonstellation allerdings nicht einschlägig, weil sie nur die Verwendung der Daten für andere Strafverfahren regelt. Weitere bereichsspezifische strafrechtliche Befugnisnormen gibt es derzeit noch nicht. Zwar enthält der neueste (aus dem Jahre 1999 datierende) Entwurf eines Strafverfahrensänderungsgesetzes (BT-Ds. 14/1484) in § 477 Abs. 2 Satz 3 i. V. m. § 476 StPO die Regelung, dass TÜ-Unterlagen einer wissenschaftlichen Forschung zugänglich gemacht werden können. Bis zum In-Kraft-Treten dieser Gesetzesänderung muss freilich auf bestehende datenschutzrechtliche Auffangvorschriften zurückgegriffen werden: Somit verbleibt als alleinige Befugnisnorm § 12 Abs. 2 Nr. 4 SächsDSG.

Bei der Anwendung dieser Vorschrift (i. V. m. § 15 Abs. 1 Nr. 1 SächsDSG) ist zunächst zu berücksichtigen, dass ausweislich der Konzeption des Forschungsvorhabens eine Kenntnisnahme der Gesprächsinhalte aus TÜ-Protokollen erforderlich ist, da insbesondere auch untersucht werden soll, in welchem Umfang die Ermittlungsmaßnahme (die Kommunikationsüberwachung) Erkenntnisse für das Verfahren erbracht hat. Hingegen ist eine Kenntnis der Identität der Betroffenen für die Wissenschaftler wohl nicht erforderlich. Aus diesem Grunde - und auch vor dem Hintergrund der anstehenden Novellierung des BDSG und der Landesdatenschutzgesetze - sollte daran gedacht werden, die personenbezogenen Unterlagen soweit wie möglich *vor* der Kenntnisnahme der Wissenschaftler zu pseudonymisieren. Nur wenn der Forschungszweck mit pseudonymisierten Daten nicht erreicht werden kann, dürfte

auch eine (teilweise) personenbezogene Auswertung in Betracht gezogen werden. In diesem Fall sollten die Daten zum frühestmöglichen Zeitpunkt pseudonymisiert werden, wenn möglich bereits bei der aktenführenden Stelle.

Weitere Voraussetzung für die Anwendbarkeit der Zweckänderungsnorm des § 12 Abs. 2 Nr. 4 SächsDSG ist das erheblich überwiegende öffentliche Interesse an der Durchführung des Forschungsvorhabens. Ob dieses Interesse besteht, ist vor dem Hintergrund der folgenden Erwägungen des Bundesverfassungsgerichts in seinem Urteil vom 14. Juli 1999 (BvR 2226/94) zu prüfen:

Danach kommt dem Fernmeldegeheimnis aus Art. 10 GG herausragende Bedeutung zu. Art. 10 GG entfaltet dem Bundesverfassungsgericht zufolge seinen Schutz nicht nur gegenüber staatlicher Kenntnisnahme von Fernmeldekommunikationen, die die Kommunikationspartner für sich behalten wollen (Inhaltsdaten). Vielmehr erstreckt sich seine Schutzwirkung auch auf den Informations- und Verarbeitungsprozess, der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt (Anschluss- und Verbindungsdaten), sowie auf den Gebrauch, der von diesen erlangten Kenntnissen gemacht wird. Beschränkungen des Fernmeldegeheimnisses unterliegen somit besonderen Anforderungen. Da die Kommunikation ihren von Art. 10 GG vermittelten Geheimnisschutz nicht dadurch verliert, dass bereits eine staatliche Stelle von dem Fernmeldevorgang Kenntnis erlangt hat, beziehen sich die Anforderungen des Grundrechts auch auf die Weitergabe der Daten und Informationen, die unter Aufhebung des Fernmeldegeheimnisses erlangt worden sind. Dies gilt dem Bundesverfassungsgericht zufolge umso mehr, als es sich bei der Weitergabe regelmäßig nicht nur um eine Ausweitung der Stellen und Personen handelt, die über die Kommunikation informiert werden, sondern um die Überführung der Daten in einen anderen Verwendungszusammenhang. Dieser andere Verwendungszusammenhang ist für die Betroffenen mit zusätzlichen, unter Umständen schwereren Folgen verbunden als dies im ursprünglichen Verwendungszusammenhang der Fall wäre. Die Zweckänderungen bedürfen daher ihrerseits einer gesetzlichen Grundlage, die formell und materiell mit dem Grundgesetz vereinbar ist. Dazu gehört, dass die Zweckänderungen durch Allgemeinbelange gerechtfertigt sind, die die grundrechtlich geschützten Interessen überwiegen. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Stelle beziehen, der die Daten übermittelt werden, und hinreichend normenklar geregelt sein. Ferner dürfen der Verwendungszweck, zu dem die Erhebung erfolgt ist, und der veränderte Verwendungszweck nicht in einem unvereinbaren Verhältnis zueinander stehen (BVerfGE a.a.O. S. 65 ff.).

Diesen vom Bundesverfassungsgericht gestellten Anforderungen kann das Forschungsvorhaben durchaus genügen, denn zum einen kommen die vom Gericht geforderten Allgemeinbelange darin explizit zum Ausdruck, dass der Gesetzgeber in § 12 Abs. 2 Nr. 4 SächsDSG die wissenschaftliche Forschung mit dem Zweckänderungsprivileg ausgestattet hat. Zum anderen ist der veränderte Verwendungszweck mit dem ursprünglichen Verwendungszweck deshalb vereinbar, weil die in Aussicht genommene Nutzung gerade dazu dienen soll, die weitere Existenzberechtigung der TÜ-Eingriffsnormen (§§ 100 a, 100 b StPO) zu überprüfen.

Weil somit das Forschungsprojekt auf das Sächsische Datenschutzgesetz gestützt werden kann, habe ich gegenüber dem SMJus keine datenschutzrechtlichen Bedenken erhoben.

8.6 Versendung von Justizpost

Meine Empfehlungen, das Verfahren der Versendung von Justizpost datenschutzgerecht zu gestalten (vgl. 7/8.7), hat das SMJus nach längerer kontroverser Diskussion nunmehr aufgegriffen: Per Erlass ist jetzt geregelt, dass die Justizbehörden im Postverkehr mit Gemeinden personenbezogene Daten enthaltende Post ausschließlich an das bei der Empfängergemeinde zuständige Fachamt adressieren und insoweit keine Sammelumschläge mehr verwenden. Es ist damit sichergestellt, dass mitzuteilende Daten unmittelbar den beim Empfänger funktionell zuständigen Bediensteten erreichen. Den Anforderungen des Justizmitteilungsgesetzes (§ 18 Abs. 2 EGGVG) und des Sächsischen Datenschutzgesetzes (§ 9 Abs. 2 Nr. 2) ist so in ausreichender Weise Genüge getan.

8.7 Mitteilungen an Anzeigeerstatter

Das SMJus fragte mich, ob es zulässig sei, dass die Staatsanwaltschaften den Anzeigeerstattern detaillierte Mitteilungen über den Gang von nach § 154 StPO eingestellten Ermittlungsverfahren zuteil werden lassen. Die Vorschrift des § 154 StPO kann die Staatsanwaltschaft anwenden, wenn sie wegen Straftaten ermittelt, die gegenüber anderen dem Beschuldigten angelasteten Taten nicht ins Gewicht fallen (so genannte „unwesentliche Nebenstraftaten“).

Für die datenschutzrechtliche Klärung der vom SMJus gestellten Frage musste ich auch die im Freistaat Sachsen gängige Mitteilungspraxis bewerten: Danach wird mit einem Vordruck der Staatsanwaltschaft der Anzeigeerstatter darüber unterrichtet, aus welchen der in § 154 Abs. 1 StPO aufgeführten Gründen von der Verfolgung der angezeigten Tat abgesehen wurde. Je nach Einzelfall erfährt der Anzeigeerstatter dabei auch, durch welches Gericht gegen den Beschuldigten eine Strafe oder Maßregel wegen eines anderen schwerer wiegenden Tatvorwurfs ausgesprochen wurde.

Diese Praxis einer pauschalen Datenübermittlung halte ich vor dem Hintergrund der einschlägigen Erlaubnisnorm des § 171 Satz 1 StPO für bedenklich, darf hiernach doch nur „nach Abschluss der Ermittlungen eine Bescheidung erfolgen“. Von der Einstellung nach § 154 StPO soll aber gerade bereits in einem möglichst frühen Stadium der Ermittlung Gebrauch gemacht werden, d. h. schon beim Erkennen von Anhaltspunkten für eine Straftat im Sinne des § 152 Abs. 2 StPO, also in einem Stadium, in dem von einem „Abschluss der Ermittlungen“ nicht die Rede sein kann.

Deshalb ist zu bedenken, dass dem durch Einstellung nach § 154 StPO beendeten Verfahren häufig völlig ungesicherte, d. h. invalide Daten zugrunde liegen. In vielen Fällen werden weder Opfer noch Täter als sicher festgestellt. So wird aus diesen Gründen in der Literatur zurecht die Auffassung vertreten, dass im Falle des § 154

Abs. 1 StPO dem Anzeigeerstatter keine konkreten Mitteilungen über die „andere“ Straftat oder Verurteilung gemacht werden sollen.

Vor diesem Hintergrund habe ich dem SMJus empfohlen, den aktuellen Vordruck zur Einstellung nach § 154 StPO nicht mehr zu verwenden. Erst recht kann die vom SMJus offenbar in Aussicht genommene Detaillierung des Vordrucks nicht in Betracht kommen.

Das SMJus hatte darüber hinaus erwogen, bei „entsprechender Anwendung“ von § 406 d Abs. 1 StPO und § 171 Satz 1 StPO dem Verletzten auf Antrag die Erhebung der öffentlichen Klage wegen der von ihm angezeigten Straftat mitzuteilen. Diesem Gedanken habe ich angesichts des von Bundesverfassungsgericht an die Verarbeitung personenbezogener Daten gestellten Voraussetzung der Normenklarheit widersprochen. Ein Rückgriff auf die datenschutzrechtlichen Auffangbestimmungen kommt hier ebenfalls nicht Betracht, weil der Gesetzgeber in der Strafprozessordnung die einschlägigen Informationsflüsse abschließend geregelt hat. Etwaige darüber hinausgehende Mitteilungen könnten somit nicht auf eine tragfähige Rechtsgrundlage gestützt werden.

Ich gehe davon aus, dass das SMJus aufgrund meiner Kritik sein Vorhaben nicht weiter verfolgen wird.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

In diesem Jahr nicht belegt.

9.2 Gewerberecht

In diesem Jahr nicht belegt.

9.3 Industrie- und Handelskammern; Handwerkskammern

Datenabgleichverfahren zwischen den Industrie- und Handelskammern, Handwerkskammern und der Arbeitsverwaltung

In 7/9.3.1 habe ich über die Unzulässigkeit des Abgleichverfahrens mangels Rechtsgrundlage hingewiesen, ohne dass seinerzeit ein endgültiges Einlenken der Bundesanstalt für Arbeit (als Initiator des Verfahrens) absehbar war.

Auf Betreiben des BfD, der über die datenschutzrechtlichen Bedenken der Landesbeauftragten für den Datenschutz bestens unterrichtet war, stellte die Bundesanstalt für Arbeit im Mai 1999 schließlich das Abgleichverfahren ein.

9.4 Offene Vermögensfragen

9.4.1 Kleine Anfrage zu Einzelangaben zu Rückübertragungs- und ähnlichen Verwaltungs-Verfahren betreffend Vermögensgegenstände, die in der sog. demokratischen Bodenreform enteignet worden sind

Unter Bezugnahme auf eine Liste vom Februar 1947, welche die 51 größten seinerzeit in Sachsen enteigneten Grundbesitzer, jeweils mit Angabe einer Hektar-Anzahl, umfasste, wollte ein Abgeordneter von der Staatsregierung wissen, auf wie viele Hektar Land von den Benannten Rückübertragungsansprüche geltend gemacht worden seien, einschließlich Ansprüchen auf bloße Entschädigung oder Ausgleichsleistung, in welchem Maß diese Ansprüche bestandskräftig anerkannt bzw. bestandskräftig abgelehnt worden seien, und ferner, inwieweit aus dem Personenkreis der in der Liste Aufgeführten bzw. ihrer Rechtsnachfolger (Erben) zusätzliche Rückübertragungsansprüche auf Grundstücke oder andere Vermögensgegenstände geltend gemacht worden seien; schließlich wollte der Fragesteller, soweit man erkennen konnte, sogar, dass die Staatsregierung zu allen einzelnen danach im Verwaltungsverfahren oder auch im gerichtlichen Verfahren noch anhängigen Anträgen angebe, wie voraussichtlich entschieden werde.

Jede der Fragen enthielt die bezeichnende Formulierung *„im Einzelnen“*.

Die Beantwortung der Fragen hätte einen unverhältnismäßigen Eingriff in das allen Betroffenen zustehende Grundrecht auf informationelle Selbstbestimmung dargestellt, wie ich der Staatsregierung im Einzelnen dargelegt habe:

Auszugehen war von folgenden bereits unter 4/2 herangezogenen allgemeinen Regeln:
Art. 51 Abs. 2 SächsVerf ist, wegen der Bindung aller öffentlichen Gewalt an Gesetz und Recht (Rechtsstaatsprinzip, vgl. Art. 20 Abs. 3 GG, Art. 3 Abs. 3 SächsVerf) und namentlich an die Grundrechte (vgl. Art. 1 Abs. 3 GG, Art. 36 SächsVerf), so zu verstehen, dass die Staatsregierung eine Abgeordneten-Anfrage nicht nur nicht beantworten muss, sondern gar nicht beantworten darf, soweit der Beantwortung gesetzliche Regelungen oder Rechte Dritter entgegenstehen (vgl. auch Kunzmann u. a., Verfassung des Freistaates Sachsen, 2. Auflage, 1997, Rdnr. 5 zu Art. 51).

Die Ausübung des mit Verfassungsrang gewährleisteten Kontrollrechts des Parlaments ermächtigt nur unter Wahrung des Grundsatzes der Verhältnismäßigkeit zu Eingriffen in betroffene Grundrechte (hier das Grundrecht auf informationelle Selbstbestimmung; vgl. BVerfGE, 67, 100 [142, 144]).

Das bedeutete hier: Zur Ausübung des parlamentarischen Kontrollrechtes benötigte der Fragesteller entweder Aussagen zu einem einzelnen oder wenigen Einzelfällen, welche als Verwaltungsvorgang aufgefallen waren und Fragen hinsichtlich des Vorgehens der Exekutive aufwarfen, oder er benötigte Auskünfte über die allgemeinen Verhältnisse auf einem bestimmten, möglicherweise auch eng begrenzten Gebiet.

Dass *ersteres* der Fall sein könnte, war nicht ersichtlich. Der Personenkreis, auf den sich die Frage bezog, war dafür zu groß. Auch ließ die Anfrage keinen gezielten Bezug auf die der Öffentlichkeit bekannten Verhandlungen des Freistaates mit dem Haus Wettin erkennen, die möglicherweise einen besonderen Einzelfall darstellten.
Daher blieb nur der als z*weites* genannte Inhalt eines von der Ausübung des parlamentarischen Kontrollrechtes gedeckten Auskunftsanspruches, eben nach den allgemeinen Verhältnissen. Dieser Auskunftsanspruch konnte mit einem beschränkten Eingriff in das Grundrecht der Betroffenen erfüllt werden, nämlich indem die personenbezogenen Daten genutzt wurden, um sie zu aggregieren, so dass nur statistische Daten, also Daten ohne jede Namensnennung, in die Antwort auf die Anfrage Eingang fanden, mithin von der Staatsregierung dem Landtag übermittelt wurden.
Das bedeutete im Ergebnis, dass die in allen Einzelfragen vorkommende Formulierung *„im Einzelnen"* bei der Beantwortung unbeachtet blieb.
Die Antwort durfte sich also nur zusammensetzen aus Angaben zu Hektar-Zahlen, Prozenten oder Anzahlen von in die Liste aufgenommenen enteigneten Großgrundbesitzern, welche selbst oder in Gestalt ihrer Rechtsnachfolger Ansprüche gestellt oder eben auch keine Ansprüche gestellt hatten.

Auch im vorliegenden Fall war dem Zweck der parlamentarischen Kontrolle - sofern diese wie hier nicht das Verhalten der Exekutive oder auch Privater in einem auffällig gewordenen Einzelvorgang von öffentlichem Interesse überprüfen will - ohnehin mehr durch die Zusammenstellung eines übersichtlichen Gesamtbildes gedient als mit einer Fülle nicht anonymisierter Einzelangaben (womöglich mit Flurstücksbezeichnung oder Beschreibung einzelner Kunstgegenstände).

Die Staatsregierung hat dann dementsprechend mit datenschutzrechtlicher Begründung eine Beantwortung der einzelnen Fragen abgelehnt.

9.4.2 Auskünfte der Ämter zur Regelung offener Vermögensfragen an das Bundesvermögensamt

Das Bundesvermögensamt - es verwaltet das Finanzvermögen des Bundes, insbesondere Grundstücke - hatte von einem sächsischen ARoV die Vorlage sämtlicher bestandskräftiger vermögensrechtlicher Bescheide verlangt, die ein im Zuständigkeitsbereich des Amtes belegenes Grundstück betreffen. Begründung war, dass aus Mitteln des Staatshaushaltes der DDR nach dem Tod einer früheren Eigentümerin des Grundstückes auf diesem lastende Grundpfandrechte abgelöst worden seien, und diese Aufwendungen begründeten einen nunmehr dem Bund zustehenden Erstattungsanspruch.

Zunächst war, in Zusammenarbeit mit dem betreffenden ARoV, herauszuarbeiten, auf welche Fallgestaltungen sich das Begehren des Bundesvermögensamtes bezog bzw. sinnvoll beziehen konnte:

(1) Ein sinnvolles Auskunftsbegehren des Bundesvermögensamtes ist nicht möglich in denjenigen Fällen, in denen eine Quasi-Rückübertragung aus nicht-vermögensrechtlichen, nämlich zivilrechtlichen Gründen stattfindet, etwa wegen Berichtigung

der Erbfolge (Kassieren von Fiskalerbscheinen). In diesen Fällen ist nie ein vermögensrechtlicher Anspruch gestellt worden, existiert also kein Antrag und dementsprechend auch kein vermögensrechtlicher Bescheid.
(2) Die Überlassung von Bescheiden an das Bundesvermögensamt scheidet auch in denjenigen Fällen aus, in denen ein Rückübertragungs-Antrag positiv beschieden ist und im Tenor gemäß § 18 Abs. 1 und 2 VermG Ablösebeträge festgesetzt worden sind. Denn den Anspruch auf den Ablösebetrag hat der Entschädigungsfonds (§ 18 b Abs. 1 Satz 2 und Abs. 5 VermG). Der Entschädigungsfonds ist ein nicht rechtsfähiges Sondervermögen des Bundes (§ 9 Abs. 1 EntschG), welches ausschließlich vom Bundesamt zur Regelung offener Vermögensfragen (BARoV) vertreten wird (§ 9 Abs. 2 EntschG), also nicht vom Bundesvermögensamt.
(3) Richtigerweise geht es offenbar nur um solche Bescheide der Vermögensämter, in denen ein Rückübertragungs-Antrag - zumindest - deswegen abschlägig beschieden wird, weil die Voraussetzungen des § 1 Abs. 2 VermG nicht erfüllt sind, nämlich das vermietete Gebäudegrundstück im Zeitpunkt der Abgabe an den Staat nicht überschuldet gewesen ist: In diesen Fällen gehört es zur notwendigen Begründung des Bescheides, für den maßgeblichen Zeitpunkt einen Vergleich zwischen dem Wert (Einheitswert) des Grundstückes und den Grundpfandrechten in der damals valutierten Höhe anzustellen. In solchen Fällen kann, im Wege der Rechtsnachfolge des Bundes (vermutlich vermittelt über die DDR-Staatsbank) in das Vermögen des damaligen Grundpfandgläubigers (bzw. Darlehensgebers), in der Tat ein Anspruch des Bundes gegen die Rechtsnachfolger der damaligen Eigentümer, insbesondere gegen rechtmäßige Erben, bestehen, für den das Bundesvermögensamt zuständig ist.
(4) In solchen Fällen sind die Ausführungen zur Höhe der dinglichen Grundstücksbelastung im maßgeblichen Zeitpunkt, einschließlich der möglichen genauen Angabe des seinerzeitigen Grundpfandgläubigers, also in der Regel eines Kreditinstitutes, ein sehr kleiner Teil des Bescheides (im Ausgangsfall waren es drei Sätze von neun Seiten!). Zu der Frage, wer wann in welcher Höhe das Grundstück entschuldet und daher möglicherweise einen Aufwendungsersatzanspruch hat, hat sich der Bescheid in solchen Fällen gar nicht zu verhalten. Außerdem stammen die Angaben, auf welche die Entscheidung des ARoV insoweit gestützt wird, aus Unterlagen, welche - jedenfalls grundsätzlich, vgl. dazu nachstehend - dem Bundesvermögensamt zur Verfügung stehen, nämlich aus dem Grundbuch und gegebenenfalls aus dem von öffentlich-rechtlichen Kreditinstituten, in der Regel also von der Sparkasse der Stadt oder des Landkreises, stammenden Schriftgut. Sollte ausnahmsweise das ARoV über andere Erkenntnisquellen verfügen, könnte es diese Quellen dem Bundesvermögensamt angeben.
(5) Allerdings konnten sich die Ausführungen des Bundesvermögensamtes auch dahingehend verstehen lassen, dass das Amt bei der Suche nach dem Schuldner des Ersatzanspruches lediglich die Negativ-Information haben wollte, dass der eine oder andere in seiner Identität bestimmte Rückübertragungs-Antragsteller bestandskräftig abschlägig beschieden worden sei. In diesem Falle benötigte das Bundesvermögensamt aber allenfalls Rubrum und Tenor - und davon nur Nr. 1 - des Rückübertragungsbescheides, ja genaugenommen wohl nur ein grundstücksbezogenes Negativ-Attest, also die verbindliche Erklärung des ARoV, dass bezüglich des Grundstückes ein positiver Rückübertragungsbescheid nicht ergangen sei (und zusätzlich wohl, dass ein fristgemäß eingereichter Rückübertragungsantrag nicht mehr offenstehe).

(6) Demnach sind Bescheide der ÄRoV dem Bundesamt nicht zur Verfügung zu stellen.
Anderes gilt aber *gegebenenfalls* für Auskünfte aus Unterlagen, welche das ARoV bei der Abfassung seines Bescheides benutzt hat.
Dabei wird unter dem Gesichtspunkt der Amtshilfe freilich möglicherweise zu prüfen sein, inwieweit der Bund nicht selbst schon über Unterlagen mit den benötigten Daten verfügt.

Sofern die ÄRoV über Unterlagen im Sinne von § 4 Satz 2 SächsArchivG verfügen, also über Unterlagen aus der Zeit vom 8. Mai 1945 bis zum 2. Oktober 1990, oder auch insoweit, als sie über Unterlagen aus den Jahren 1933 bis 1945 verfügen, müssten diese nach dem Buchstaben des Gesetzes gemäß § 5 Abs. 2 bzw. § 5 Abs. 1 Satz 2 SächsArchivG den staatlichen Archiven angeboten werden. Andererseits ist es vernünftige, keineswegs auf die ÄRoV beschränkte Praxis, dass Aktenbestände aus dieser Zeit, welche von Behörden zur gegenwärtigen Aufgabenerfüllung noch benötigt werden, noch nicht den staatlichen Archiven angeboten worden sind.
Diese Praxis darf andererseits nicht dazu führen, dass Dritten, insbesondere auch dritten Behörden, der Zugang zu den in solchen Unterlagen vorhandenen Daten im Vergleich zu dem Fall einer Archivierung dieser Unterlagen erschwert würde. Konkret bedeutet dies, dass grundsätzlich die ÄRoV Einsicht in oder Auskünfte aus diesen Unterlagen, die ihnen mehr oder weniger ‘zugefallen’ sind, erteilen müssen, also etwa aus Grundbuchunterlagen, Sparkassenunterlagen, Unterlagen der staatlichen (zugleich ‘kommunalen’) Liegenschaftsverwaltung zu DDR-Zeiten einschließlich der Enteignungs-Unterlagen.

Datenschutzrechtlich handelt es sich dann um Übermittlungen. Der legitime Datenbedarf wird sich vermutlich mit Hilfe der allgemeinen Regeln der §§ 13, 15 SächsDSG decken lassen, so dass es der Überlegung einer Als-ob-Anwendung des Archivrechtes wohl nicht bedürfen wird. Dies erfordert möglicherweise noch genauere Prüfung im Einzelnen. Im Ergebnis kann aber kein Zweifel bestehen, dass z. B. aus Unterlagen über Rechte, die auf den Bund übergegangen sind, diesem Auskünfte zu erteilen sind, auch wenn damit zugleich Daten Dritter, also etwa der Schuldner, übermittelt werden.

Das Sächsische Landesamt zur Regelung offener Vermögensfragen hat sich dieser Auffassung angeschlossen und dabei zu recht hervorgehoben, dass im Falle einer Übermittlung nach § 13 SächsDSG die um Übermittlung ersuchende Behörde - was im Falle der Anfrage des Bundesvermögensamtes gerade nicht geschehen war - jeweils genau zu prüfen hat, welche personenbezogenen Daten sie für ihre Aufgabenerfüllung tatsächlich benötigt (vgl. § 13 Abs. 2 SächsDSG!).
Auch das Bundesvermögensamt hat sich anscheinend überzeugen lassen.

9.4.3 Pflicht der Behörden, auch ein unbegründetes Datenschutz-Verlangen zu beantworten

Jemand, der vom SED-Regime politisch verfolgt worden ist (Haft in Bautzen), hatte nach strafrechtlicher Rehabilitierung einen Antrag bei einem sächsischen ARoV

gestellt. Im Rahmen der Vorgangsbearbeitung hatte das Amt verschiedene Unterlagen erhalten, vor allem vom Antragsteller selbst, aber auch vom BStU.
Aus Misstrauen gegen die Behörde („*immer noch alte SED-Kader an maßgeblichen Stellen*“) hatte der Antragsteller dann von dieser verlangt, die *beigezogenen ihn betreffenden persönlichen Unterlagen, namentlich das DDR-Strafurteil, an ihn auszuhändigen.*
Nachdem das ARoV längere Zeit dieses Verlangen ignoriert hatte, hatte der Petent sich dann an mich gewandt.

Es ist mir wohl gelungen, bei ihm Verständnis dafür zu wecken, dass sein Verlangen *in der Sache* unbegründet war: Unterlagen, die einer Behörde zur Verwendung in deren Verwaltungsverfahren übermittelt werden, werden Bestandteil der Akte, in der die Führung des Verwaltungsverfahrens dokumentiert ist; die Behörde darf allenfalls solche Unterlagen durch Rückgabe an den Absender aus der Akte entfernen, die unter keinem in Frage kommenden rechtlichen Gesichtspunkt von Erheblichkeit für die Führung und den Ausgang des Verfahrens sein können. Dies gilt auch für solche Unterlagen, welche der BStU in Erfüllung seiner Aufgaben nach dem Stasi-Unterlagengesetz Behörden wie z. B. auch den ÄRoV zukommen lässt.
Angesichts dessen gab es keine Anzeichen dafür, dass die vom ARoV zum Verfahren geführte Akte Unterlagen enthielt, welche durch Rückgabe oder durch Übersendung an den Petenten aus der Akte entfernt werden mussten oder auch nur hätten entfernt werden dürfen.
Ich konnte dabei auf die Beiträge 9.4.1 und 9.4.2 im 5. TB verweisen: Rechtsstaatliches Verfahren verlangt, dass die Unterlagen, welche für die Entscheidungsfindung nicht unter jedem nur denkbaren rechtlichen Gesichtspunkt unerheblich sind, in der Akte sind und den Verfahrensbeteiligten zur Verfügung stehen. Nur so kann ein rechtsstaatliches, faires Verfahren durchgeführt werden.

Anderes galt für die *Verfahrensweise der Behörde:* Es wäre Pflicht der Behörde gewesen, das nachvollziehbare, wenn auch rechtlich unbegründete Datenschutz-Verlangen des Antragstellers durch eine Antwort zu bescheiden.

Der Anspruch auf eine solche Bescheidung ergibt sich in derartigen Fällen einmal aus Art. 17 GG. Insoweit kann sich die Beantwortung nach der - im Schrifttum heftig angegriffenen - Rechtsprechung des Bundesverfassungsgerichtes darauf beschränken, mitzuteilen, wie die Behörde verfahren wird. Die Antwort brauchte, wenn nur das Grundgesetz anzuwenden wäre, eine Begründung dieser Verfahrensweise also nicht unbedingt zu enthalten (Dreier/Bauer Rdnrn. 28, 41 zu Art. 17 GG m. w. N.). Da aber zugleich in solchen Fällen Art. 35 SächsVerf anzuwenden ist, besteht nach dessen Satz 2 gegenüber sächsischen Behörden ein Anspruch auf einen mit einer Begründung versehenen Bescheid.

Den Petenten habe ich gebeten, die ihm von mir erteilte Antwort als Erfüllung des Antwort-Anspruchs gelten zu lassen, der ihm gegenüber dem ARoV zustand. Was sein durch die rechtswidrige Verfahrensweise der Behörde genährtes Misstrauen gegenüber weiten Teilen der in den neuen Bundesländern nach der demokratischen Revolution und der Wiedervereinigung entstandenen Verwaltung betraf, habe ich ihm

erklärt, dass man dafür Verständnis haben müsse, ihm aber zugleich versichert, dass sehr viele Bedienstete der Verwaltung alles daran setzen, die Einhaltung der rechtsstaatlichen Regeln durchzusetzen und die rechtsstaatlichen Institutionen fest zu verankern, und dass dies auch in einem Maße gelungen ist, für welches dankbar zu sein alle, die wir daran interessiert sind, Grund haben.

9.5 Sonstiges

9.5.1 Korruptionsvorbeugung in der Verwaltung des Freistaates Sachsen

Das SMI beabsichtigte, seinen Geschäftsbereich auf mögliche Korruptionsgefahren zu überprüfen. Zu diesem Zweck sollten in einzelnen nachgeordneten Behörden die einzelnen Aufgabengebiete im Wege einer Selbst- und Fremdbewertung auf eventuell vorhandene Ansatzpunkte für Korruption untersucht werden. Hierzu entwickelte das SMI einen Fragebogen für Bedienstete, mit dessen Hilfe korruptionsrelevante Merkmale abgefragt werden sollten, um Maßnahmen zur Korruptionsvorbeugung (z. B. Personalrotation, Intensivierung der Fach- und Dienstaufsicht, Prüfungen durch die Innenrevision) einzuleiten.

Nach Prüfung des Fragenkatalogs, der aus meiner Sicht nicht erforderlich und vor allem nicht geeignet war, konnte ich in einer Besprechung vom SMI erreichen, dass auf die beabsichtigte Erhebung subjektiver Einschätzungen von Beschäftigtendaten in dieser Form verzichtet wurde und andere - weniger in das Recht auf informationelle Selbstbestimmung eingreifende, vor allem eben objektive - Methoden zur Feststellung korruptionsgefährdeter Bereiche entwickelt werden.

Durch Teilnahme an Sitzungen der entsprechenden Arbeitsgruppe ist meine weitere Beteiligung gesichert.

9.5.2 Korruptionsbekämpfung - Einrichtung eines Korruptionsregisters

Zu 7/8.6 hat sich die Staatsregierung zur Frage der Zulässigkeit eines „Korruptionsregisters“ wie folgt geäußert:

> *„Im Rahmen der ressortübergreifenden Anti-Korruptions-Arbeitsgruppe wird der Aufbau eines sogenannten „Korruptionsregisters“ geprüft, in dem Verfehlungen und Vergabesperren von Gewerbetreibenden gespeichert werden sollen. Nach Auffassung des Sächsischen Staatsministeriums der Justiz soll zunächst eine Grundsatzentscheidung der zuständigen Ressorts über die Frage der Einrichtung eines solchen Registers und die Schaffung einer entsprechenden Rechtsgrundlage herbeigeführt werden, die auch den datenschutzrechtlichen Anforderungen Rechnung trägt.“*

In der Folge wurde eine Unterarbeitsgruppe „Korruptionsregister“ gegründet, die sich zunächst u. a. mit der Frage evtl. bereits existierender gesetzlicher Grundlagen für die Einrichtung eines solchen Registers zu befassen hatte.

Vorsorglich habe ich mich wie folgt geäußert:

Überlegungen, die Rechtmäßigkeit eines Korruptionsregisters auf §§ 97 ff. GWB oder § 55 SächsHO zu stützen, scheitern nach meinem Dafürhalten bereits an den Grundsätzen des Volkszählungsurteils vom 15. Dezember 1983 (BVerfGE 65, 1, 43 ff), wonach Einschränkungen des Rechts auf informationelle Selbstbestimmung, wie sie mit der einem zentralen Register innewohnenden Intensität einhergehen, nur im überwiegenden Allgemeininteresse und nur auf einer verfassungsmäßigen normenklaren gesetzlichen Grundlage unter Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig sind (siehe auch Art. 33 SächsVerf). Weder das GWB noch § 55 SächsHO kommen wegen Fehlens dieser Anforderungen als Ermächtigungsgrundlage in Betracht. Auch ein Rückgriff auf die Vorschriften der allgemeinen Datenschutzgesetze scheidet wegen deren generalklauselartigen Charakters aus. So hat der Landesbeauftragte für den Datenschutz Baden-Württemberg das dortige Innenministerium wegen des ohne ausreichende Rechtsgrundlage eingerichteten Korruptionsregisters bereits am 26. September 1997 förmlich beanstandet und die Schaffung einer entsprechenden Rechtsgrundlage gefordert.

Ein Korruptionsregister enthält personenbezogene Daten über letztlich immer persönliche Verfehlungen (Vergabesperren), die von einer Vielzahl von Stellen des Landes und der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts zur zentralen Speicherung gemeldet wurden und die solchen Stellen übermittelt werden sollen. Einrichtungen vergleichbarer Eingriffstiefe finden wir beispielsweise beim Bundeszentralregister, Gewerbezentralregister, Ausländerzentralregister, Verkehrszentralregister, Fahrerlaubnisregister, die allesamt auf detaillierten bereichsspezifischen gesetzlichen Grundlagen fußen (auch wenn es, wie z. B. beim Ausländerzentralregister, das jahrelang ohne Rechtsgrundlage existierte, des datenschutzrechtlichen Drucks bedurfte, um den Gesetzgeber erfolgreich zum Handeln aufzufordern).

Beratungen der Unterarbeitsgruppe über die Anwendbarkeit des GWB oder der SächsHO als Rechtsgrundlage für die Einrichtung und Führung eines Korruptionsregisters habe ich vor diesem Hintergrund für nicht zielführend gehalten und gefordert, dass eine klare Rechtsgrundlage für ein solches Register geschaffen wird, in dem angeblich/nachweisbar unzuverlässige Firmen und Anbieter mit dem Ziel gespeichert werden, sie landes- oder bundesweit von öffentlichen Aufträgen auszuschließen. Die Voraussetzungen dazu (z. B. rechtskräftige gerichtliche Entscheidungen) müssten nämlich jeweils aktuell vorliegen. Das eröffnet die Frage, wie sich ein Unternehmen von der Unzuverlässigkeit einzelner Mitarbeiter „reinigen“ kann und wie lange das Unternehmen von einem u. U. existierenden Marktgeschehen ferngehalten werden darf. So einfach, wie sich das der eine oder andere dem Wirtschaftsleben Fernstehende vorstellt, lässt sich in einer sozialen Marktwirtschaft staatliche Lenkung durch Vergabeausschlüsse nicht datenschutzkonform durchführen, zumal das Europarecht jedem Unternehmen einen Anspruch auf gerechte und gleichmäßige Berücksichtigung bei öffentlichen Aufträgen zuerkennt.

Die Unterarbeitsgruppe kam schließlich zu dem Ergebnis, dass es Sache des Bundes

sei, eine den Grundsätzen des Volkszählungsurteils (BVerfGE 65, 1, 41 ff.) entsprechende normenklare und verhältnismäßige Rechtsgrundlage zu schaffen.

Die weitere Entwicklung bleibt abzuwarten.

9.5.3 Meldepflichten ortsfremder Personen, die in Kurorten unentgeltlich beherbergt werden

In dem vom SMWA erstellten Muster für eine Kurtaxensatzung, das sich verschiedene Kurorte zu Eigen gemacht haben, sind Bestimmungen enthalten, die zu nicht unberechtigter Kritik führten.
U. a. *müssen* sich ortsfremde Personen, auch wenn sie *unentgeltlich* beherbergt werden (in erster Linie also Verwandte und Freunde), innerhalb von zwei Tagen persönlich in der Gemeindeverwaltung melden. Verstöße gegen diese Meldepflicht können mit einer Geldbuße bis zu 50.000 DM geahndet werden.

Ich habe das SMWA gebeten, für eine bürgerfreundlichere und gerechtere Gestaltung dieser Bestimmungen zu sorgen, zumal die Meldepflicht ortsfremder Personen verständlicherweise negative Erinnerungen an Vorwendezeiten weckt (Meldepflichten von Westbesuchern).

Das SMWA hat meine Vorschläge aufgegriffen und wird zusammen mit dem SSG adäquate Regelungen erarbeiten.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1 Wird die Praxis halten, was sich der Gesetzgeber von einem bundesweiten „Substitutionsregister“ für Methadon-Patienten und deren Ärzte verspricht?

Am 1. April 2000 ist das Dritte Gesetz zur Änderung des Betäubungsmittelgesetzes in Kraft getreten. Es enthält eine Verordnungsermächtigung zur Einrichtung eines bundesweiten Registers über Ärzte, die zur Behandlung Drogenabhängiger mit Substitutionsmitteln qualifiziert sind, sowie über das patientenbezogene Verschreiben von Substitutionsmitteln. Das Register soll zum einen der Kontrolle dienen, ob die verschreibenden Ärzte über die entsprechende Qualifikation verfügen, zum anderen soll es verhindern, dass ein Patient von mehreren Ärzten Substitutionsmittel verordnet bekommt (Doppelsubstitution) und sie dann missbräuchlich verwendet.

In Gesprächen und einer umfangreichen Stellungnahme zum Gesetzentwurf habe ich dem SMS meine grundsätzlichen Bedenken gegen ein solches Register wie folgt dargelegt:

1. Für die Kontrolle, ob ein Arzt über die zur Substitutionsbehandlung vorgeschriebene Qualifikation verfügt, bedarf es keines Registers. Bestehen Zweifel (z. B.

aufgrund eines Hinweises aus der Bevölkerung), kann die zuständige Behörde den Nachweis ebensogut unmittelbar vom Arzt verlangen. Die Annahme jedoch, dass ein nicht qualifizierter Arzt Verschreibungen von Substitutionsmitteln mitteilt, also die eigene ungesetzliche Handlung offenlegt, dürfte illusorisch sein (siehe aber Nr.5).

2. Dem Entwurfstext zufolge sollten die den Patienten betreffenden Meldungen in *anonymisierter* Form erfolgen. Nach den Begriffsbestimmungen in den Datenschutzgesetzen bedeutet *Anonymisieren* das Verändern personenbezogener Daten in der Weise, dass sie nicht mehr einer bestimmten Person zugeordnet werden können oder dass eine Zuordnung nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft möglich ist. Anonyme Patientendaten sind jedoch zum Erkennen von Doppelsubstitutionen ungeeignet.

   Wie sich herausstellte, war nicht *Anonymisieren* gemeint, sondern Pseudonymisieren, Codieren, Verschlüsseln o. ä. nach einem System, das die Zusammenführung von Meldungen verschiedener Ärzte über denselben Patienten ermöglicht und es damit erlaubt, den meldenden Ärzten entsprechende Hinweise zu geben. Ich habe erfolglos angeregt, dies durch eine entsprechende Terminologie zum Ausdruck zu bringen, damit kein falscher Eindruck entsteht.

3. Das Gesetz ermächtigt zu einer Verordnung, die *Meldungen über das Verschreiben von Substitutionsmitteln* regelt. Damit entsteht ein Kontrollinstrument über das Verschreibungsverhalten der substituierenden Ärzte. Ich hatte mich für eine (verschlüsselte) *Meldung der Patienten* ausgesprochen, falls das Register als unverzichtbar angesehen werden sollte.

4. Anhand des Registers können Doppelsubstitutionen nur „im nachhinein“ erkannt werden. Der Missbrauch wird also erst festgestellt, wenn er bereits stattgefunden hat. Vor dem Hintergrund, dass es für Kassenpatienten bereits ein System zur Erkennung von Doppelsubstitutionen gibt, erschien mir das Register besonders fragwürdig, nicht zuletzt deshalb, weil das System der Krankenkassen den Vorteil hat, dem Missbrauch schon im Vorfeld zu begegnen. Dieses Verfahren sei wie folgt skizziert:

   Nach der Richtlinie zur substitutionsgestützten Behandlung Opiatabhängiger vom 26. April 1999 (Nr. 2 der Anlage A der „Richtlinie des Bundesausschusses der Ärzte und Krankenkassen über die Einführung neuer Untersuchungs- und Behandlungsmethoden und über die Überprüfung erbrachter vertragsärztlicher Leistungen ...“, BAnz. S. 9394) hat der substituierende Arzt der leistungspflichtigen Krankenkasse sowie der Kassenärztlichen Vereinigung Beginn und Ende der Substitution unter Angabe des Namens und der Versicherten-Nummer des Patienten anzuzeigen (§ 7 Abs. 2 der Richtlinie). Zuvor hat er sie bei der Kassenärztlichen Vereinigung zu beantragen und genehmigen zu lassen (die Entscheidung trifft eine Beratungskommission der Kassenärztlichen Vereinigung). Demgemäß kann geprüft werden, ob bereits ein anderer Arzt den Patienten substituiert. In diesem Fall werden die beteiligten Ärzte benachrichtigt, damit sie unter Einbezie-

hung des Patienten schriftlich festlegen können, welcher Arzt die Substitution durchführt (§ 7 Abs. 3 der Richtlinie).

Eine zusätzliche Registrierung der Kassenpatienten in einem Register mit derselben - aber weniger effektiven - Zielsetzung halte ich für nicht erforderlich. Selbst für Privatpatienten, Heilfürsorgeberechtigte und nicht Versicherte ist kein Register notwendig. Als generelle Alternative zur Verhinderung von Doppelsubstitutionen habe ich einen „Substitutionspass“ vorgeschlagen, der dem Patienten von der zur Leistung verpflichteten Stelle oder einem Gesundheitsamt *für einen bestimmten Arzt* ausgestellt werden könnte. Ohne einen solchen Pass dürfte kein Arzt eine Substitutionsbehandlung durchführen.

5. Ferner habe ich darauf hingewiesen, dass nach § 5 Abs. 1 BtMVV Substitutionsmittel *nicht nur zur Behandlung einer Drogenabhängigkeit* verschrieben werden können, sondern auch zum befristeten Austausch eines unerlaubt konsumierten Opiats im Rahmen der Behandlung einer anderen schweren Erkrankung oder zur Verringerung der Risiken einer Opiatabhängigkeit während einer Schwangerschaft und nach der Geburt. Ein Arzt, der aus diesen Gründen ein Substitutionsmittel verschreibt, muss nicht gleichzeitig im Besitz einer besonderen Qualifikation zur Behandlung einer Drogenabhängigkeit sein. Bei der Registerbehörde würde folglich ein „Fehlalarm“ ausgelöst.

   Ich gehe davon aus, dass diese Fallkonstellation in der noch zu erlassenden Rechtsverordnung berücksichtigt werden kann.

Und eine weitere wichtige Frage ist offen: Darf ein Arzt, den die Registerbehörde von der Doppelsubstitution seines Patienten unterrichtet hat, ohne Schweigepflichtentbindung mit dem anderen Arzt überhaupt über „den Fall“ sprechen?

Meine Vorbehalte sind nicht ausgeräumt. Ich werde mir die vorgesehenen Statistiken zu gegebener Zeit ansehen. Sie werden zeigen, ob das Register mehr als eine „politische Beruhigungsspritze“ für diejenigen ist, die mit einigem Recht in der ärztlichen Substitutionsbehandlung eine Unterstützung des Drogenmissbrauchs auf Kosten der Allgemeinheit sehen.

10.1.2 Jugendzahnärztliche Untersuchungen in Kindertageseinrichtungen

Ein Vater empörte sich darüber, dass sein vierjähriges Kind im Kindergarten unangekündigt vom Jugendzahnärztlichen Dienst der Stadt untersucht worden war. Als er sich beim Gesundheitsamt nach den Rechtsgrundlagen erkundigte und statt einer sachdienlichen Auskunft den Hinweis erhielt, er könne strafrechtlich belangt werden, wenn er die Untersuchung seines Kindes nicht dulden würde, wandte er sich an mich. Ich habe mir daraufhin das Verfahren näher angesehen (eine ärztliche Untersuchung ist eine Datenerhebung, ihre Dokumentation eine Datenspeicherung) und erhebliche datenschutzrechtliche Defizite festgestellt.

1. *Die Untersuchungen müssen freiwillig sein und bedürfen der schriftlichen Einwilligung der Sorgeberechtigten*

   Gemäß § 11 Abs. 1 Nr. 2 SächsGDG haben die Gesundheitsämter den Kindertageseinrichtungen zahnärztliche Vorsorgeuntersuchungen anzubieten. Die Träger sollen dieses Angebot gemäß § 6 Abs. 2 SäKitaG annehmen. Aus beiden Vorschriften lässt sich eine Pflichtuntersuchung nicht ableiten. Folglich dürfen sie nur auf freiwilliger Basis und nur mit schriftlicher Einwilligung der Sorgeberechtigten erfolgen (s. §§ 4 Abs. 1 Nr. 2 und Abs. 3, 11 Abs. 2 SächsDSG). Das war hier nicht geschehen.

   Da die bevorstehende Untersuchung üblicherweise durch einen Aushang am „schwarzen Brett" oder auf einem Elternabend angekündigt wurde, erreichte die Information nicht immer alle Eltern.

2. *Auch eine* Sc*hweigepflichtentbindung fehlte*

   Die Untersuchungen erfolgen grundsätzlich in der Kindergruppe sowie im Beisein von Erzieherinnen und ggf. Vätern und Müttern, die ihre Kinder begleiten. Der ärztliche Befund wird angesagt und von einer ärztlichen Hilfskraft auf dem Formblatt „Mitteilung für die Eltern" angekreuzt und für statistische Zwecke festgehalten. Durch das Mithören erfahren die Anwesenden Gesundheitsdaten, die gemäß § 203 StGB der ärztlichen Schweigepflicht unterliegen. Ohne ausdrückliche Schweigepflichtentbindung durch die Sorgeberechtigten besteht für den Arzt keine Befugnis zur Offenbarung der Daten.

3. *Das Untersuchungsergebnis ist den Eltern verschlossen mitzuteilen*

   Wie mir der Petent mitgeteilt hatte, soll die für die Eltern bestimmte Mitteilung über den Befund und die ärztlich empfohlenen Maßnahmen unverschlossen weitergeleitet worden sein (z. B. durch Bereitlegen im Fach des Kindes oder Aushändigung an die Person, die das Kind abholt).

   Die *unverschlossene* Weitergabe ist zum einen ein Verstoß gegen § 9 Abs. 2 Nr. 2 SächsDSG, weil keine Maßnahme getroffen wurde, die das unbefugte Lesen oder Kopieren verhindert. Werden die Daten durch Außenstehende zur Kenntnis genommen, liegt außerdem eine Verletzung des von § 203 StGB geschützten Patientengeheimnisses vor.

4. *Der Statistik fehlte die Rechtsgrundlage*

   Einzelheiten siehe 8/5.7.3.

Über meine Feststellungen habe ich das SMS unterrichtet und die Anforderungen an ein datenschutzgerechtes Verfahren formuliert. Diese wurden umgesetzt und vom SMS den sächsischen Gesundheitsämtern in einem Rundschreiben zur Kenntnis gegeben. Nunmehr wird wie folgt verfahren:

- Das Gesundheitsamt informiert die Eltern schriftlich über den Zweck der Untersuchung und holt unter Hinweis auf die Freiwilligkeit die schriftliche Einwilligung von mindestens einem Sorgeberechtigten ein (§ 11 Abs. 2 SächsDSG). Auf das

Recht zur im Übrigen folgenlosen Verweigerung der Einwilligung wird hingewiesen.
- Nur mit ausdrücklicher Schweigepflichtentbindung darf das Untersuchungsergebnis im Beisein Dritter angesagt werden.
- Das Untersuchungsergebnis wird verschlossen an die Eltern weitergeleitet.

Wegen der fehlenden Einwilligung der Sorgeberechtigten war die weitere Aufbewahrung aller vorhandenen Unterlagen mit den Untersuchungsergebnissen der einzelnen Kinder unzulässig. Als Konsequenz mussten sie von den Gesundheitsämtern gemäß § 19 SächsDSG gelöscht werden. Da sich das Löschungsgebot auf personenbezogene Daten beschränkt, war das statistische, bereits aggregierte Zahlenmaterial davon ausgenommen.

10.1.3 Übermittlung von Patientendaten per Telefax

Immer wieder fragen Krankenhäuser, ob und ggf. unter welchen Voraussetzungen Patientendaten, deren unbefugte Offenbarung nach § 203 Abs. 1 Nr. 1 StGB strafbar ist, per Telefax übermittelt werden dürfen.

In meiner Bekanntmachung vom 14. Juni 1993 (SächsABl. S. 894) habe ich mich dafür ausgesprochen, dass für die Übermittlung von Daten, die wie Patientendaten einem besonderen Berufsgeheimnis unterliegen, grundsätzlich kein Telefaxgerät benutzt wird. Da dies im Einzelfall jedoch (lebens-)notwendig sein kann, bedarf die pauschale Aussage in meiner Bekanntmachung folgender Präzisierung, zumal die technische Entwicklung sich weiterentwickelt hat:

Der Regelfall für die Weitergabe ärztlicher Unterlagen sollte nicht das Telefax sein. Denn Telefaxgeräte befinden sich häufig an zentralen Orten, so dass eine Kenntnisnahme der Patientendaten durch unbeteiligte Dritte und damit eine unbefugte Offenbarung i. S. v. § 203 StGB nicht ausgeschlossen werden kann. Selbst wenn ein Telefaxgerät in einem Raum aufgestellt ist, in dem sich normalerweise stets eine zur Kenntnisnahme befugte Person aufhält (z. B. Sprechzimmer eines niedergelassenen Arztes, Chefarzt-Sekretariat, Sachbearbeiterbüro bei der Krankenkasse), sind Situationen denkbar, die Außenstehenden eine Kenntnisnahme von Patientendaten ermöglichen. Dabei ist z. B. an Reinigungskräfte, Handwerker oder Hausmeister zu denken, die sich in einem solchen Raum unbeaufsichtigt außerhalb der Sprech- oder Arbeitszeiten aufhalten.

Sofern eine Datenübermittlung per Telefax im Einzelfall unumgänglich sein sollte, ist durch eine vorherige telefonische Benachrichtigung des Empfängers sicherzustellen, dass das Telefax von einer befugten Person entgegengenommen wird.

Häufige Ursache für ein fehlgeleitetes Telefax ist das Verwählen. Auch in diesem Fall würden die von der ärztlichen Schweigepflicht geschützten Daten unbefugt offenbart. Deshalb ist die vom empfangenden Gerät abgegebene Kennung sofort zu überprüfen, damit die Verbindung bei Wählfehlern ggf. sofort abgebrochen werden kann. Außerdem ist zu kontrollieren, ob die Übertragung störungsfrei und vollständig den Empfänger erreicht hat.

10.1.4 Übermittlung von Trinkwasseruntersuchungsergebnissen vom Gesundheitsamt an den Trinkwasserversorger

Nach § 8 Abs. 1 Nr. 7 SächsGDG überwachen die Gesundheitsämter u. a. Anlagen zur Trinkwasserversorgung, z. B. private Brunnen, ob die Einhaltung der Hygieneanforderungen eingehalten werden. Verschiedene Trinkwasserversorger fragten, ob und unter welchen Voraussetzungen die Gesundheitsämter die Ergebnisse der Untersuchungen von Brunnentrinkwasser übermitteln dürfen.

Ich habe den Trinkwasserversorgern und dem betreffenden Gesundheitsamt mitgeteilt, dass nach § 57 Abs. 1 SächsWG die Wasserversorger im Rahmen ihrer Leistungsfähigkeit die Pflicht haben, in ihrem Gebiet u.a. die Bevölkerung mit (einwandfreiem) Trinkwasser zu versorgen. Um in die Planung und Projektierung der Trinkwasserversorgung auch die vorhandenen Brunnen einbeziehen zu können, ist es nach meinem Dafürhalten unerlässlich, dass die Gesundheitsbehörde dem Wasserversorger mitteilt, welche Brunnen einwandfreie Trinkwasserqualität aufweisen und welche nicht.

Da das SächsGDG keine bereichsspezifische Übermittlungsnorm enthält, ist das SächsDSG als Auffanggesetz heranzuziehen. In der Gesamtschau der §§ 13, 12 Abs. 2 bis 4, 11 Abs. 4 SächsDSG halte ich die Datenübermittlung an den Wasserversorger, zu dessen (rechtmäßiger) Aufgabenerfüllung für zulässig, unabhängig davon, ob er um Auskunft ersucht hat oder nicht.

10.1.5 Datenerhebung bei Blutspenden

Ein Blutspender fragte, ob der Blutspendedienst berechtigt sei, den Spendewilligen u. a. nach Aufenthalten in einer JVA und nach Kontakten zu HIV-infizierten Personen zu fragen.

Ich habe folgenden Standpunkt vertreten:

Nach § 5 Abs. 1 TFG dürfen nur Personen zur Spendeentnahme zugelassen werden, die unter der Verantwortung einer approbierten ärztlichen Person nach dem Stand der medizinischen Wissenschaft und Technik für tauglich befunden worden sind und die Tauglichkeit durch eine approbierte ärztliche Person festgestellt worden ist. Die Zulassung zur Spendeentnahme soll nicht erfolgen, soweit und solange die spendewillige Person nach Richtlinien der Bundesärztekammer von der Spendeentnahme auszuschließen oder zurückzustellen ist.

Der Blutspender muss sich also nach ärztlicher Beurteilung in einem gesundheitlichen Zustand befinden, der eine Blutspende ohne Bedenken zulässt. Dies gilt sowohl im Hinblick auf den Gesundheitsschutz des Spenders als auch für die Herstellung von möglichst risikoarmen Blutkomponenten und Plasmaderivaten. Die Spendetauglichkeit ist durch Anamnese und ärztliche Beurteilung einschließlich der Laboratoriumsuntersuchungen zu prüfen. Aus der „Richtlinie zur Blutgruppenbestimmung und Bluttransfusion“ sind die Kriterien zu ersehen, die den Arzt veranlas-

sen müssen, den Spendewilligen von der Blutspende auszuschließen. Offensichtlich entspricht es dem Stand der medizinischen Wissenschaft, auch nach den vom Petenten kritisierten Punkten zu fragen. Andererseits halte ich es nach wie vor für fraglich, wenn sich der Blutspendedienst mit einfachen Antworten - ohne Verifikation - begnügt. Und was soll die Fragerei, wenn die Blutspende ohnehin noch auf Infektionen etc. untersucht wird, ehe sie in den Handel kommt?

Ich habe den Petenten aber um Verständnis gebeten, dass sich der Sächsische Datenschutzbeauftragte im wohlverstandenen Interesse der Spender und der Spendenempfänger nicht anmaßen kann, die aus medizinisch-wissenschaftlicher Sicht erforderlichen Angaben zu denkbaren Risikogruppen infrage zu stellen.
Mit dem Thema werde ich mich weiter beschäftigen.

10.1.6 Aufbewahrung von Patientenakten bei Zusammenlegung zweier Krankenhäuser

Im Zusammenhang mit der Zusammenlegung zweier bislang selbständigen Krankenhäuser im Einzugsbereich des ehemaligen Wismutbergbaus wurde ich um Beratung über die Behandlung von Patientenakten gebeten.

Ich habe mich wie folgt geäußert:

1. Patientenakten, die vor der Wende entstanden sind und nach der Wende nicht fortgeführt wurden, wären nach § 35 SächsDSG (Behandlung von DDR-Altdaten, siehe 1/1.3, 1/16.1.1, 2/1.7.1) zu behandeln gewesen. Inzwischen besteht für solche Unterlagen die Verpflichtung zur Abgabe an ein (staatliches) Archiv. Dies gilt ebenso für die so genannten Dispensaireakten als auch für Schularztakten.
   Es reicht nach der bisher geübten Praxis aus, wenn die Unterlagen vom Kreisarchiv statt vom Staatsarchiv übernommen werden. Im Einzugsbereich des ehemaligen Wismut-Bergbaues dürfte es sich für das Kreisarchiv empfehlen, zur Beurteilung der Archivwürdigkeit eine mit den einschlägigen Forschungsarbeiten befasste Stelle, wie das Bundesamt für Strahlenschutz, befragen zu lassen.

2. Patientenakten, die nach der Wende entstanden sind (oder die zwar vor der Wende entstanden sind, aber nach der Wende fortgeführt wurden oder weiter benötigt werden), sind unter Berücksichtigung der unterschiedlichsten Aufbewahrungsfristen (siehe am Ende dieses Beitrages) unter der Obhut des Krankenhauses aufzubewahren. Aus datenschutzrechtlicher Sicht würde ich es nicht beanstanden, wenn die Unterlagen (mit Ausnahme der Buchführungsdaten der Verwaltung) komplett 30 Jahre aufbewahrt werden.

   Zur Aufbewahrung kann sich das Krankenhaus anderer, sicherer Räume (z. B. des Kreisarchivs) unter der Bedingung bedienen, dass die Zugriffsberechtigung ausschließlich beim Krankenhaus verbleibt (Schlüsselgewalt). Nach Ablauf der Aufbewahrungsfrist empfiehlt sich die Anbietung an ein Archiv und die Vernichtung, wenn seitens des Archivs keine Reaktion erfolgt oder die Archivwürdigkeit verneint wird.

3. Patientenakten, die bei einem im Krankenhaus praktizierenden Arzt (Belegarzt, angestellter Arzt mit entsprechender Nebentätigkeitsgenehmigung) entstanden sind/entstehen, sind dessen Akten nach der ärztlichen Berufsordnung zu behandeln (das Krankenhaus darf auf die Führung solcher Patientenunterlagen keinen Einfluss nehmen).

Aufstellung über unterschiedliche Aufbewahrungsfristen im Krankenhaus (nicht abschließend)

Nach § 33 Abs. 6 SächsKHG sind Patientendaten zu löschen, wenn

1. sie zur Erfüllung der in Absatz 2 genannten Zwecke nicht mehr erforderlich *und*

2. *vorgeschriebene Aufbewahrungsfristen* abgelaufen sind und kein Grund zur Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Beispiele für Aufbewahrungsfristen:

Patientendaten zu Buchführungszwecken in der Krankenhausverwaltung:

- § 257 HGB (10 bzw. 6 Jahre)

- § 35 Abs. 2 GemKVO (10 bzw. 6 Jahre).

Patientendaten ärztl. Bereich:

- Ärztliche Berufsordnung (10 Jahre)

- § 32 Strahlenschutzverordnung (30 Jahre)

- § 28 Abs. 4 Nr. 1 Röntgenverordnung (30 Jahre für Aufzeichnungen über Röntgenbehandlungen); § 28 Abs. 4 Nr. 2 Röntgenverordnung (10 Jahre für Röntgenaufnahmen und sonstige Aufzeichnungen)

- § 195 BGB (30 Jahre)

- § 852 Abs. 1 BGB (3 oder 30 Jahre).

10.1.7 Bestattungswesen: Auskünfte über Bestattungsunternehmen an Dritte

Jemand wollte zur Verfolgung zivilrechtlicher Ansprüche vor Gericht von den Gesundheitsämtern des Freistaates Sachsen eine Übersicht über die nicht geschlossenen und nicht aufgehobenen Friedhöfe und deren Träger mit Namen bzw. Bezeichnung

und Anschrift haben. Von diesen Trägern wollte er dann, in der zweiten Stufe der Informationsbeschaffung, Auskunft darüber einholen, wie viele Bestattungen bestimmte, von ihm benannte Bestattungsunternehmer in bestimmten Zeiträumen durchgeführt haben.

Mit diesem Vorhaben musste er letztendlich scheitern, wobei es ihm auch nichts half, dass er sich auf einen zivilgerichtlichen Aufklärungsbeschluss berufen konnte, welcher der betroffenen Prozesspartei auferlegte, diese Daten vor Gericht vorzutragen:

Einer Nennung der Friedhöfe und deren Träger stand das Datenschutzrecht in den meisten Fällen nicht entgegen:
Bei den Trägern der Friedhöfe handelt es sich gemäß §§ 1 bis 3 SächsBestG ganz überwiegend um Kommunen sowie Kirchen und Religionsgemeinschaften mit der Eigenschaft einer Körperschaft des öffentlichen Rechts. Bezeichnung und Anschrift dieser Träger dürfen durch die Gesundheitsämter bekannt gegeben werden, ohne dass eine Rechtsvorschrift oder Einwilligung dies erlauben müsste. Denn solche juristischen Personen sind keine Grundrechtsträger; und das SächsDSG gilt gemäß dessen § 2 Abs. 1 für solche Vorgänge nicht, da es sich nicht um personenbezogene Daten handelt: Personenbezogene Daten müssen sich auf natürliche Personen beziehen (§ 3 Abs. 1 SächsDSG).

Anderes gilt jedoch für die privaten Bestattungsplätze gemäß § 3 Abs. 3 SächsBestG. Deren Träger können natürliche Personen sein. Dann richtet sich eine Datenübermittlung (an eine private Stelle, wie im vorliegenden Falle) nach § 15 Abs. 1 Nr. 2 SächsDSG. Dieser Vorschrift zufolge ist eine Übermittlung nur erlaubt, wenn derjenige, auf den sich die Angaben beziehen, kein schutzwürdiges Interesse daran hat, dass die Bekanntgabe des Datums unterbleibt. Bei kleineren Bestattungsplätzen besteht vermutlich auf jeden Fall ein schutzwürdiges Interesse am Unterbleiben der Übermittlung.

Darauf kam es im praktischen Ergebnis allerdings nicht an, weil der Fragesteller auf der zweiten Stufe seiner Informationsbeschaffung scheitern musste: Die Daten, um die es in diesem Fall eigentlich ging - nämlich die Anzahl der Bestattungen, die von den benannten Bestattungsunternehmen in bestimmten Jahren jeweils auf dem betreffenden Bestattungsplatz durchgeführt worden waren - durften nämlich ganz überwiegend nicht übermittelt werden:

Bestattungsunternehmen, die als juristische Personen betrieben werden, sind so klein, dass der durch Gesellschafter- bzw. Organstellung vermittelte Bezug auf eine oder mehrere natürliche Personen so eng ist, dass diesbezügliche Angaben durchweg als personenbezogene, grundrechtlich geschützte Daten anzusehen sind. Denn auch Informationen über Geschäftsinhaber bzw. Geschäftsführer sind personenbezogene Daten.

Zumindest soweit Träger der Friedhöfe Kommunen sind - also öffentliche Stellen, für welche das Sächsische Datenschutzgesetz gilt - durften sie demnach Daten der Bestattungsunternehmen an den Fragesteller nur unter den Voraussetzungen des § 15

Abs. 1 Nr. 2 SächsDSG übermitteln. Hier war überhaupt nicht zu erkennen, dass es am *Interesse* der betroffenen Bestattungsunternehmen fehlen könnte: Der Versuch des Fragestellers, die nötigen Zahlen von den - ihm übrigens bekannten - Bestattungsunternehmen selbst zu bekommen, war an deren mangelnder Bereitschaft gescheitert, was den Angaben des Interessenten zufolge auch nicht allein auf Bequemlichkeit zurückzuführen war.

Das Geheimhaltungsinteresse war auch nicht etwa nicht [sic!] schutzwürdig. Denn die Tatsache, dass die gewünschten Daten Auswirkungen auf die rechtlichen Beziehungen unter Dritten haben, lässt die Schutzwürdigkeit nicht entfallen; das galt hier namentlich auch für den Fall, dass die Bestattungsunternehmen Vertragspartner einer der beiden - dritten - Prozessparteien gewesen sein sollten. Und andere Anhaltspunkte für ein Fehlen der Schutzwürdigkeit waren nicht zu erkennen.

Möglicherweise bestehen in solchen Fällen zivilrechtliche Auskunftsansprüche. Diese müssen dann aber, gegebenenfalls nacheinander in einer Kette, durchgesetzt werden. Aus der Beurteilung solcher schwer zu durchschauender zivilrechtlicher Verhältnisse unter Dritten hat sich die öffentliche Stelle, sofern sich ihre sachliche Zuständigkeit nicht mit diesen Verhältnissen gerade berührt - was vorliegend ja nicht der Fall war -, herauszuhalten. Dies gilt erst recht dann, wenn, wie hier, der Auskunftsbegehrende zum Sachverhalt fast nichts mitteilt, so dass der Versuch einer Beurteilung des Interesses und seiner Schutzwürdigkeit schon von vornherein aussichtslos ist. Hier kam hinzu, dass offensichtlich war, dass die Betroffenen (d. h. die Bestattungsunternehmen) dem Interessenten die Daten ja offenbar gerade verweigert hatten. Und außerdem: Was vorstehend mit der doppelten Verneinung vielleicht etwas gekünstelt formuliert gewirkt hat, ist wichtig. Denn prüfen muss die Behörde nicht, ob das Interesse des Betroffenen schutzwürdig ist, sondern sie muss sich Gewissheit verschaffen, dass es an der Schutzwürdigkeit fehlt! Diese negative Tatsache ist Voraussetzung der Erlaubtheit der Übermittlung, nicht etwa ist die Schutzwürdigkeit Voraussetzung der Verbotenheit der Übermittlung! (Auf gut deutsch: Im Zweifel für die Freiheit.)

Anderes galt nur für die nicht von Privaten, sondern von Kommunen betriebenen Bestattungsunternehmen. Es war davon auszugehen, dass deren Marktanteil auch in den neuen Bundesländern nicht so groß ist, dass dem Fragesteller mit einer auf diese Unternehmen beschränkten Auskunft einigermaßen ausreichend gedient gewesen wäre.

Die an mich von Seiten des Interessenten gestellte rhetorische Frage, ob denn *Behörden unter Berufung auf den Datenschutz jemandem die Möglichkeiten der Durchsetzung legitimer Interessen in einem ordentlichen Gerichtsverfahren vorenthalten dürfe*, diese Frage war, insoweit dies aus den vorstehenden Ausführungen hervorgeht, mit *ja* zu beantworten.

10.2 Sozialwesen

10.2.1 Weitergabe von Sozialdaten zu Zwecken der Strafverfolgung und zur Einleitung dienstrechtlicher Maßnahmen

Macht jemand in einem Antrag auf Gewährung von Sozialleistungen bewusst oder auch nur aufs Geratewohl, ins Blaue hinein, falsche Angaben zu Lasten des Sozialleistungsträgers, so erfüllt er den Tatbestand des (versuchten) Betruges. Bemerkt der für die Gewährung der Sozialleistung zuständige Sozialleistungsträger, dass ein solcher Betrug oder Betrugsversuch unternommen wurde, möchte er natürlich entsprechende Schritte einleiten. Wurden zu Unrecht bereits Sozialleistungen gewährt, sind diese nach den Vorschriften der §§ 45, 50 SGB X durch den Begünstigten zu erstatten.

Daneben besteht auch das Interesse, potentielle Täter abzuschrecken, sich auf Kosten der Sozialleistungsträger und damit letztlich der Allgemeinheit durch zu Unrecht gewährte Sozialleistungen zu bereichern. Dies Interesse wird durch die Strafverfolgung gewahrt. Die Staatsanwaltschaft, die die Ermittlungen durchzuführen hat, benötigt zur Aufklärung des Sachverhalts zunächst den Antrag, in dem die Falschangaben gemacht wurden. Der Sozialleistungsträger darf sie an die Staatsanwaltschaft dann übermitteln, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Es liegt auf der Hand, dass der Betroffene seine Einwilligung nicht gibt. Gibt es also eine Rechtsvorschrift, die in solchen Fällen die Übermittlung von Sozialdaten - denn um solche handelt es sich hier - durch den Sozialleistungsträger an die Staatsanwaltschaft zulässt?

In Betracht kommt § 73 Abs. 1 SGB X. Aber Betrug ist kein Verbrechen; ihn als Vergehen von erheblicher Bedeutung einzustufen, wird auf den Einzelfall ankommen. Die leider „normalen“ Betrügereien durch Falschangaben in Anträgen auf Gewährung von Sozialleistungen fallen nicht darunter. Auch bedürfte es gemäß Absatz 3 der Vorschrift der ermittlungsrichterlichen Anordnung der Übermittlung.

Einschlägig für die Übermittlung von Sozialdaten für die Durchführung eines Strafverfahrens ist daneben aber auch § 69 Abs. 1 SGB X.

Dessen *Nr. 2* sieht vor, dass eine Übermittlung von Sozialdaten zulässig ist, soweit sie erforderlich ist für die Durchführung eines mit der Erfüllung einer Aufgabe nach § 69 Abs. 1 Nr. 1 SGB X zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens. Allerdings ist der überwiegende Teil der Kommentarliteratur, richtigerweise vom Wortlaut ausgehend, der Auffassung, dass unter Strafverfahren lediglich das gerichtliche Verfahren, nicht auch das strafrechtliche Ermittlungsverfahren zu verstehen ist. Danach kann die Übermittlung an die Staatsanwaltschaft auch nicht auf § 69 Abs. 1 Nr. 2 SGB X gestützt werden.

Eine Erlaubnis einer Übermittlung von Sozialdaten durch den Sozialleistungsträger an die Staatsanwaltschaft für Zwecke der Strafverfolgung wegen Sozialbetruges ist jedoch § 69 Abs. 1 *Nr. 1* SGB X zu entnehmen.

Anerkanntermaßen gehört es im Sinne dieser Vorschrift zu den gesetzlichen Aufgaben der Sozialleistungsträger, ggf. auch eine Strafanzeige (oder eine Anzeige an die Gewerbeaufsichtsbehörde) zu erstatten, wenn dies „zur Wahrung der Zahlungsdisziplin oder zur Verhütung weiterer Schäden für die Versichertengemeinschaft“ erforderlich ist, so heißt es in der Gesetzesbegründung zu § 69 SGB X a. F. (Fassung ab 1. Januar 1981, der Vorgängerregelung des § 69 SGB X; BT-DS 8/4022 S. 85). Zu den gesetzlichen Aufgaben des Sozialleistungsträgers gehört es demnach, auch dadurch etwas dagegen zu tun, dass Sozialleistungen zu Unrecht in Anspruch genommen werden, dass er von einschlägigen Versuchen den Strafverfolgungsbehörden Mitteilung macht. Dies ist in der Literatur, soweit erkennbar, unbestritten (vgl. Hauck/Haines, Rdnrn. 23, 32 zu § 69 SGB X). Klargestellt wird dies im Übrigen auch dadurch, dass in § 69 Abs. 1 Nr. 2 SGB X, der in die Nr. 1 der Vorschrift ergänzt, ja sich auf sie bezieht (Schroeder-Printzen, Rdnr. 26 zu § 69 SGB X), Strafverfahren ausdrücklich erwähnt werden.

Ich war mit einem Fall befasst, in dem die Sozialbehörde Falschangaben eines Beamten, eines sog. Finanzanwärters, entdeckt hatte. Da die Sozialbehörde der Durchführung eines strafgerichtlichen Verfahrens keine Aussicht auf Erfolg gab, setzte sie auf das Pferd „Disziplinarverfahren“. Die Sozialbehörde übermittelte also an den Dienstvorgesetzten des Beamten den Widerspruchsbescheid, aus dem sich der gesamte Sachverhalt einschließlich der Tatsache, dass Falschangaben gemacht worden waren, ergab. Der Dienstvorgesetzte erteilte daraufhin dem Beamten eine Rüge. Der Beamte hat sich daraufhin an mich gewandt, um prüfen zu lassen, ob die Daten von der Sozialbehörde an seinen Dienstvorgesetzten hatten übermittelt werden dürfen.

Ich neige dazu, die Übermittlung dieser Daten für rechtswidrig zu halten, sicher erscheint mir dies jedoch nicht. Mit anderen Worten: Ich halte es für gut möglich, dass die Gerichte anders entscheiden, also doch eine Rechtsgrundlage für diese Datenübermittlung als gegeben ansehen - zumindest, was den Kern der Angelegenheit betrifft, nämlich diejenigen Daten, die nach Auffassung der Sozialbehörde den Verdacht begründen, dass der Beamte bei seinem Antrag auf Gewährung von Sozialleistungen bewusst oder auch nur ins Blaue hinein, also vorsätzlich, falsche Angaben zulasten des Sozialleistungsträgers gemacht hat.

Als Rechtsgrundlage der Übermittlung kommt auch hier ausschließlich § 69 Abs. 1 Nr. 1 SGB X in Betracht. Die Frage ist, ob diese Vorschriften nicht nur Anzeigen, welche die Einleitung eines Strafverfahrens erwirken sollen, umfasst, sondern auch Anzeigen, welche die Einleitung disziplinarrechtlicher Maßnahmen auslösen sollen. Disziplinarrechtliche Maßnahmen - wie auch die Verhängung von Bußgeldern - unterscheiden sich von Kriminalstrafen. Unbeschadet des Resozialisierungszweckes von Kriminalstrafen wird aber in allen Fällen ein Übel zugefügt. Das Besondere der dienstrechtlichen, insbesondere disziplinarrechtlichen Maßnahmen, die im Rahmen eines Amtsverhältnisses ergriffen werden können (Ähnliches gilt für die Standesaufsicht), besteht darin, dass hier vor allem der Zweck verfolgt wird, dass gerade die Inhaber bestimmter Ämter, also im Wesentlichen die Beamten, davon abgehalten werden sollen, sich über die Rechtsordnung hinwegzusetzen, damit Achtung vor und

Vertrauen in das Amt und damit das Ansehen des öffentlichen Dienstes gewahrt bleibt.
Die Sozialleistungsträger sollen durch Auslösung repressiver Maßnahmen anderer Stellen die Schädigung der Sozialkassen eindämmen, auch wenn die Sanktionen, welche die betreffende dritte Stelle, also der Datenempfänger, zu verhängen hat, zusätzlich eine andere Institution, nämlich das Beamtentum, schützen sollen.

Der Kommentarliteratur lassen sich dazu nur spärliche Andeutungen entnehmen. Immerhin setzt der bereits zitierte Kommentar Hauck/Haines a.a.O. Rdnr. 34, a. E., voraus, dass neben Bußgeldverfahren auch Disziplinarverfahren unter § 69 Abs. 1 Nr. 1 SGB X fallen. Und dasselbe scheinen der auf einen früheren, aber in der Sache nicht überholten Gesetzesstand sich beziehende Gemeinschaftskommentar zum Sozialgesetzbuch - Schutz der Sozialdaten (GK-SGB X 2), 1989, Rdnr. 103 zu § 69, sowie der Kasseler Kommentar Rdnr. 8, a. E., zu § 69 SGB X zu tun.

Eine Staatsanwaltschaft, der gemäß § 69 Abs. 1 Nr. 1 SGB X (wie erwähnt: nur nach einer Mindermeinung auch gemäß § 69 Abs. 1 Nr. 2 SGB X, vgl. Hardtung NJW 1992, 211, zustimmend Schroeder-Printzen Rdnr. 26 zu § 69 SGB X, anders wohl LG Stuttgart NJW 1994, 63) die einen Verdacht auf den Versuch einer betrügerischen Erlangung von Sozialleistungen begründenden Daten übermittelt worden sind, darf ihrerseits Beschuldigtendaten übermitteln, soweit dies nach ihrer Beurteilung erforderlich ist für die Durchführung dienstrechtlicher Maßnahmen im Hinblick auf ein Amtsverhältnis. Setzt der Sozialleistungsträger die Staatsanwaltschaft von einem einschlägigen Sachverhalt in Kenntnis, darf diese unter den Voraussetzungen des § 14 Abs. 1 Nr. 4 Buchstabe a EGGVG ihrerseits dem Dienstvorgesetzten des Beschuldigten die einschlägigen Daten übermitteln.

Um es zusammenzufassen: Die Rechtslage erscheint mir unsicher. Eine verlässliche Grundlage für eine Datenübermittlung wie die im vorliegenden Fall geschehene gibt es meiner Auffassung nach zurzeit nicht. Eine bestimmtere Auskunft konnte ich dem Petenten - und auch der Behörde, einem Regierungspräsidium - nicht geben.

10.2.2 Akteneinsichtsgesuch eines Unterhaltsschuldners zur Überprüfung der Entscheidung des Sozialleistungsträgers, Rückgriff auf der Grundlage von § 91 BSHG zu nehmen

Ein Sozialamt hat gegen den Sohn eines Sozialhilfeempfängers im Rückgriffswege zunächst außergerichtlich einen Unterhaltsanspruch in voller Höhe der geleisteten Aufwendungen geltend gemacht, da den Feststellungen der Behörde zufolge die Tochter des Sozialhilfeempfängers nach ihren Erwerbs- und Vermögensverhältnissen nicht in der Lage war, Unterhalt zu gewähren. (Nur unter dieser Voraussetzung kann die Behörde auf den Sohn in voller Höhe Rückgriff nehmen, weil nämlich gemäß § 1606 Abs. 3 Satz 1 BGB mehrere gleichnahe Verwandte anteilig, d. h. als Teilschuldner, nicht als Gesamtschuldner haften, BGH NJW 1971, 1985.) Der Rechtsanwalt des Sohnes hat vom Sozialamt Akteneinsicht begehrt, um die Feststellungen des Sozialamtes zu überprüfen. (Für solche Datenerhebungen hat eine Sozialhilfebehörde

als Rechtsgrundlage die beiden Auskunftsansprüche des § 116 Abs. 1 Satz 1 BSHG und des § 1605 Abs. 1 Satz 1 BGB i. V. m. § 91 Abs. 1 Satz 1 BSHG.)
Die Gewährung von Akteneinsicht wäre eine Offenbarung personenbezogener Daten und daher (vgl. auch § 35 SGB I) nur aufgrund einer gesetzlichen Erlaubnis zulässig.

(1) Unabhängig davon, inwieweit nach bürgerlichem Recht dem Einsichtsbegehrenden (=Sohn) ein zivilrechtlicher Auskunftsanspruch gegen den anderen möglichen Unterhaltsverpflichteten (=Tochter) zusteht, scheidet § 74 Satz 1 Nr. 2 Buchstabe a SGB X als Datenübermittlungs-Erlaubnis aus. Denn die Vorschrift gibt als nötigen Zweck der Datenübermittlung die Geltendmachung eines Unterhaltsanspruches an. Mit anderen Worten: Die Vorschrift erlaubt Datenübermittlungen, z. B. auch durch Akteneinsicht, nur zugunsten desjenigen, der Unterhaltsansprüche geltend machen kann, also als Unterhaltsgläubiger in Frage kommt (so ausdrücklich der RV-Träger-Kommentar, 6. Auflage [I/1998], Anmerkung 4 zu § 74 SGB X, trotz gelegentlicher darüber hinausgehender Formulierungen unter I; ferner auch die übrige Kommentarliteratur, z. B. Hauck/Haines Rdnr. 10 zu § 74 SGB X). Der Sohn will aber als möglicher Unterhaltsschuldner Ansprüche abwehren! Hinter dieser engen, nicht jede Klärung des Bestehens von Unterhaltsansprüchen einbeziehenden Zweckbestimmung steht die gesetzgeberische Überlegung, dass die privilegierte Zweckänderung, die in § 74 Satz 1 Nr. 2 Buchstabe a SGB X erlaubt wird, nur dazu dienen soll, Sozialleistungsansprüche zu vermeiden und die Erfüllung von Unterhaltsansprüchen sicherzustellen (Hauck/Haines Rdnr. 12 zu § 74 SGB X; ähnlich Kasseler Kommentar Rdnr. 2 zu § 74 SGB X).

(2) Als Übermittlungs-Erlaubnis kommt jedoch § 25 Abs. 1 Satz 1 SGB X in Betracht. Nach dieser Vorschrift haben die Beteiligten des Verwaltungsverfahrens ein Akteneinsichtsrecht, soweit die Aktenkenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.

Zwar fehlt es an dem danach vorausgesetzten Verwaltungsverfahren im Sinne von § 8 SGB X. Denn die Behörde kann auf sie übergegangene Unterhaltsansprüche aus den §§ 1603 ff. BGB nur durch Klage vor dem Zivilgericht geltend machen, weil sich durch den Forderungsübergang an der zivilrechtlichen Natur der Unterhaltsansprüche nichts geändert hat. Mit anderen Worten: Soweit der Sozialhilfeträger auf der Grundlage der übergeleiteten zivilrechtlichen Ansprüche vorgeht, gilt: Sein Auskunfts- und sein Zahlungsbegehren sind nicht auf den Erlass eines Verwaltungsaktes gerichtet und stellen einen solchen auch nicht dar. Insoweit wird Verwaltungsprivatrecht ausgeführt.

Unter den Voraussetzungen des § 25 SGB X gibt es jedoch auch außerhalb eines laufenden Verwaltungsverfahrens eine in das pflichtgemäße Ermessen der Behörde gestellte Befugnis, Akteneinsicht zu gewähren (RV-Träger-Kommentar a.a.O. Anmerkung 2.1 zu § 25 SGB X; vgl. ferner Hauck/Haines Rdnr. 9 a zu § 25 SGB X; ähnlich Kasseler Kommentar Rdnr. 5 zu § 25 SGB X).
Der Grund dafür ist, dass das Recht auf Akteneinsicht ein Teil des Rechts auf rechtliches Gehör ist, es dient der von Verfassungs wegen vorgeschriebenen Sicherung effektiven Rechtsschutzes (vgl. Kasseler Kommentar Rdnr. 2 zu § 25 SGB X).

Der Rechtsstaatsgrundsatz verlangt, dass der Private nicht zum bloßen Objekt einer staatlichen Handlung wird, dass ihm vielmehr vor Vornahme der staatlichen Handlung - soweit ohne Vereitelung von deren Zweck möglich - ein *verfassungsunmittelbarer Anspruch* auf Gewährung rechtlichen Gehörs zusteht (M. Schulte, Schlichtes Verwaltungshandeln, Tübingen 1995, S. 122 f.). Dies sollte meines Erachtens nicht nur für verwaltungsaktähnliche Maßnahmen der schlicht-hoheitlichen Verwaltung gelten (wie vom LG Stuttgart in der von Schulte a.a.O. ausschnittsweise wiedergegeben *Birkel*-Entscheidung ausgesprochen), sondern auch dort gelten, wo die Verwaltung verwaltungsprivatrechtlich, also durch Geltendmachung zivilrechtlicher Forderungen und ggf. Klageerhebung, vorgeht. Es kann nicht der Sinn der Rechtstechnik des Forderungsübergangs gemäß §§ 90 f. BSHG und ähnlicher Vorschriften im Sozialrecht sein, die öffentliche Gewalt von Bindungen, welche für diese spezifisch sind, grundsätzlich freizustellen.

Mit anderen Worten: Verfahrensanforderungen wie z. B. das Recht auf Akteneinsicht sind durch das Rechtsstaatsprinzip verfassungsrechtlich vorgegeben. Sie haben als verfahrensrechtliche Konsequenzen eines Grundrechtsschutzes durch Verfahren für den Bereich des schlichten Verwaltungshandelns (so Schulte a.a.O. S. 118) ihren Sinn auch dort, wo der Adressat des Handelns der öffentlichen Gewalt noch auf die Garantien des rechtsstaatlichen Verfahrens vor den ordentlichen Gerichten zurückgreifen kann.

Die Anerkennung eines solchen an § 25 SGB X angelehnten verfassungsunmittelbaren Akteneinsichtsrechtes und der entsprechenden Übermittlungsbefugnis seitens der Behörde ist auch kein Verstoß gegen den in § 74 Nr. 2 Buchstabe a SGB X zum Ausdruck kommenden Rechtsgedanken. Diese Vorschrift dient, wie schon erwähnt, nur der Förderung der Geltendmachung von Unterhaltsansprüchen unabhängig von bzw. außerhalb aller von der Verwaltung betriebenen Verfahren, sie begründet also insoweit keinen Umkehrschluss.

Die Gestattung von Akteneinsicht nach § 25 SGB X gehört zu den gesetzlichen Aufgaben im Sinne des § 69 Abs. 1 Nr. 1 SGB X (Hauck/Haines Rdnr. 16 zu § 25 SGB X, m.w.N.), hat also eine Übermittlungsbefugnis, wie sie von § 67 d Abs. 1 SGB X gefordert wird, zur Grundlage. Für eine um der Einhaltung des Rechtsstaatsgrundsatzes willen, also zur Erfüllung eines verfassungsunmittelbaren Anspruches geschehene Akteneinsichtsgewährung kann nichts anderes gelten.

(3) Daraus folgt als vorläufiges Zwischenergebnis: Der Einsichtbegehrende hat einen Anspruch auf Akteneinsicht, sei es aus analoger Anwendung des § 25 SGB X, sei es unmittelbar aufgrund des Verfassungsgebotes der Gewährung rechtlichen Gehörs.

(4) Dieses Ergebnis kann man zusätzlich auf folgende Hilfsüberlegung stützen:
Eine Möglichkeit, die gewünschte Akteneinsicht zu erhalten, ließe sich auch auf Umwegen herbeiführen: Der Sohn könnte die Erfüllung der vom Sozialamt gegen ihn geltend gemachten zivilrechtlichen Forderung aus den §§ 1601 BGB i. V. m. 91 Abs. 1 Satz 1 BSHG verweigern. Das Sozialamt müsste dann auf Erfüllung vor den ordentlichen Gerichten klagen. Im Rahmen dieses Prozesses hätte der Betroffene dann als

Partei ein Akteneinsichtsrecht nach § 299 Abs. 1 ZPO. Dieses Akteneinsichtsrecht bezieht sich auf die Prozessakten, die beim Zivilgericht entstanden sind. Im Zivilprozess gilt der Beibringungsgrundsatz. Dies bedeutet, dass die Parteien darüber entscheiden, welcher Tatsachenstoff in den Prozess eingeführt wird. Der Träger der Sozialhilfe, der als Kläger den auf ihn übergegangenen Unterhaltsanspruch vor dem zuständigen Zivilgericht geltend macht, hat die seinen behaupteten Anspruch begründenden Tatsachen darzulegen und gegebenenfalls zu beweisen. Demgegenüber trifft den beklagten Unterhaltspflichtigen die Darlegungslast für die anspruchshindernden und anspruchsvernichtenden Tatsachen. Allerdings hat der Träger der Sozialhilfe gemäß § 20 SGB X bereits im Vorfeld alle entscheidungserheblichen Umstände aufzuklären, unabhängig davon, ob sie vom Unterhaltspflichtigen geltend gemacht worden sind oder nicht. Der für das Verwaltungsverfahren geltende Untersuchungsgrundsatz wird insoweit mit in den Zivilprozess „hineingetragen". Der Träger der Sozialhilfe ist deshalb verpflichtet, im Unterhaltsrechtsstreit sämtliche Tatsachen vorzutragen, aus denen sich für den Unterhaltspflichtigen günstige Rechtsfolgen herleiten lassen. Dies ergibt sich im Übrigen auch aus den während des Prozesses weiter bestehenden öffentlich-rechtlichen Verpflichtungen des Sozialhilfeträgers zur Aufklärung, Beratung und Betreuung. Demnach werden die vom Sozialhilfeträger ermittelten Einkommens- und Vermögensverhältnisse der Schwester des Einsichtbegehrenden auch Gegenstand des Zivilprozesses und somit Akteninhalt (so überzeugend Schellhorn, BSHG, § 91 Rdnr. 135). Nicht zuletzt aus dem Gedanken der Prozessökonomie, welchem zu dienen durchaus auch zu den Zwecken des Grundsatzes rechtzeitigen rechtlichen Gehöres gehört, sollte die Akteneinsicht auch schon vor Beginn eines gerichtlichen Verfahrens möglich sein.

(5) Dies muss jedenfalls dann gelten, wenn, wie vorliegend, der Einsichtbegehrende gegen den Betroffenen, also im vorliegenden Fall die Tochter, einen Anspruch auf Auskunft hat: Einen solchen Anspruch wird man, sei es analog § 1605 BGB, sei es auf der Grundlage von § 242 BGB anzuerkennen haben. Dies hat die Rechtsprechung, namentlich BGH NJW 1988, 1906, im Verhältnis zwischen Eltern zur Feststellung ihrer Unterhaltspflicht gegenüber einem gemeinsamen Kind getan; die Überlegungen gelten aber genauso im Verhältnis zwischen Geschwistern zur Feststellung ihrer Unterhaltspflicht gegenüber den Eltern (so überzeugend Staudinger/Kappe, 12. Aufl. 1993, Rdnr. 6 zu § 1605 BGB mit Nachweisen der Anerkennung einer Auskunftspflicht im Verhältnis von Eltern zueinander). Die ausdrückliche, aber unbegründete Ablehnung der Übertragung dieses Gedankens auf das Verhältnis zwischen Geschwistern im Hinblick auf deren Unterhaltspflicht gegenüber Eltern bei Palandt-Diederichsen Rdnr. 13 zu § 1605 BGB überzeugt nicht. Die Überlegungen des BGH a.a.O. (= FamRZ 1988, 268), gelten auch hier: Der in Anspruch Genommene ist zur Berechnung seines Haftungsanteils nur in der Lage, wenn ihm die Einkommens- und Vermögensverhältnisse des anderen Unterhaltspflichtigen bekannt sind; deswegen reicht das gemäß § 1606 Abs. 3 BGB bestehende besondere Rechtsverhältnis zwischen beiden aus, den Auskunftsanspruch zu begründen (a.a.O. 1906 rSp); es muss vermieden werden, dass Beteiligte in möglicherweise auf dem Prozessweg auszutragende Auseinandersetzungen gedrängt würden (a.a.O. 1907 lSp).

(6) Daraus folgt zugleich, dass die Beschränkung des Akteneinsichtsrechtsanspruches

in Absatz 3 des § 25 SGB X nicht eingreift: Der Schuldner eines zivilrechtlichen Auskunftsanspruchs hat insoweit kein berechtigtes Interesse an Geheimhaltung gegenüber seinem Gläubiger; ein berechtigtes Interesse eines Dritten ist ebenfalls nicht ersichtlich. Im Hinblick auf einen unmittelbar aus der Verfassung (Gebot der Gewährung rechtlichen Gehörs) herzuleitenden Akteneinsichtsanspruch kann nichts anderes gelten.

(7) In einem ganz weiten, nämlich den Rechtsstaatsgrundsatz einbeziehenden Sinne könnte man die Datenübermittlung sogar auf § 74 Satz 1 Nr. 2 Buchstabe a SGB X stützen. Denn die Datenübermittlung (Akteneinsichtsgewährung) diente der Verwirklichung des *übergegangenen* Unterhaltsanspruches insofern, als dessen Durchsetzung durch die Behörde gegen den Unterhaltspflichtigen rechtsstaatlich nur angemessen sein kann, wenn die Behörde ihrerseits, salopp formuliert, ihre Karten auf den Tisch legt, d. h. in einem fairen Verfahren angemessene Gegenwehr ermöglicht und dadurch beiden Seiten ermöglicht wird, unnötige Prozesse zu vermeiden. Dies gilt jedenfalls deswegen, weil ja, wie dargelegt, der Betroffene ohnehin dem Einsichtsbegehrenden gegenüber nach § 242 BGB auskunftspflichtig ist.

(8) Es bleibt also bei dem oben unter 3 genannten Anspruch auf Akteneinsicht. Das SMS hat - wie meine Kollegen in Bund und Ländern - Einwände oder Verbesserungsvorschläge gegenüber meiner Rechtsauffassung nicht geäußert.

10.2.3 Datenabgleich zwischen Sozialamt und Kfz-Zulassungsstelle

Eine Anfrage der Kfz-Zulassungsstelle eines Landratsamtes betraf einen ‘wunden Punkt’ der gegenwärtigen Gesetzeslage:

Gemäß § 117 Abs. 3 Satz 1 BSHG sind *die Träger der Sozialhilfe befugt, zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe Daten von Personen, die Leistungen nach diesem Gesetz beziehen, bei anderen Stellen ihrer Verwaltung, bei ihren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden zu überprüfen, soweit diese für die Erfüllung dieser Aufgaben erforderlich sind.* Gemäß § 117 Abs. 3 Satz 4 Buchstabe f BSHG gehört zu den Daten, die gemäß Satz 1 überprüft werden dürfen, die Eigenschaft als Kraftfahrzeughalter. Gemäß Abs. 3 Satz 5 der Vorschrift ist die Kfz-Zulassungsbehörde verpflichtet, dieses Datum zu übermitteln. Nach Satz 7 unterbleibt eine Übermittlung, „soweit ihr besondere gesetzliche Verwendungsregelungen entgegenstehen“.

Das BSHG tritt dadurch gegenüber den bereichsspezifischen Datenverarbeitungsregelungen zurück, die für die um Übermittlung ersuchte Stelle gelten. Für die Kfz-Zulassungsbehörde ist das das StVG. Es regelt in den §§ 31 bis 47 die Führung des Fahrzeugregisters, d. h., welche Daten dort zu welchen Zwecken gespeichert werden und an wen diese Daten zu welchen Zwecken übermittelt werden dürfen.
Gemäß § 35 Abs. 1 StVG *dürfen die Halterdaten an Behörden zur Erfüllung der Aufgaben des Empfängers nur übermittelt werden, wenn dies für die Zwecke nach § 32 Abs. 2 jeweils erforderlich ist* für eine der dort aufgezählten zehn Aufgaben (z. B. Maßnahmen nach dem Abfallbeseitigungsgesetz, Absatz 2 Nr. 6), wobei die Ausfüh-

rung des Bundessozialhilfegesetzes nicht erwähnt wird. § 32 Abs. 2 StVG bestimmt als einen *Zweck des Fahrzeugregisters die Erteilung von Auskünften, um Personen in ihrer Eigenschaft als Halter von Fahrzeugen festzustellen oder zu bestimmen.* Will das Sozialamt die Eigenschaft des Sozialhilfeempfängers als Kraftfahrzeughalter überprüfen und bittet es die Zulassungsbehörde um Auskunft, hielte sich die Übermittlung dieses Datums durch die Zulassungsbehörde an das Sozialamt zwar im Rahmen der Zweckbestimmung des § 32 Abs. 2 StVG. Hinzukommen muss jedoch die Erforderlichkeit der Übermittlung für eine der in § 35 Abs. 2 Nr. 1 bis 10 genannten Aufgaben. Der in § 117 Abs. 3 Satz 1 BSHG genannte Zweck „Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe“ wird als Aufgabe in § 35 Abs. 1 Nr. 1 bis 10 aber eben nicht aufgeführt. Es erscheint mir als mehr als zweifelhaft, ob man die verdachtsunabhängige Überprüfung von Sozialhilfeempfängern zur Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe als eine Maßnahme *zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung* im Sinne des § 35 Abs. 1 Nr. 4 StVG ansehen kann. Jedenfalls wird man nicht argumentieren dürfen, dass jeder Verstoß gegen die Rechtsordnung ausreiche: Das wäre zu unbestimmt und passte auch nicht zu den ausgesprochen konkreten anderen Aufgaben-Tatbeständen der Vorschrift. (Insofern habe ich dem SMS, das ich um Stellungnahme gebeten habe, widersprechen müssen.)

Mit der Formulierung in § 35 Abs. 1 StVG „dürfen nur übermittelt werden, wenn“ wird ausgedrückt, dass eine Übermittlung zur Erfüllung anderer als der unter Nr. 1 bis 10 genannten Aufgaben unzulässig ist. Da die Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe allem Anschein nach nicht unter die Aufgaben des § 35 Abs. 1 Nr. 1 bis 10 fällt, ist diese Vorschrift eine dem § 117 Abs. 3 Satz 5 BSHG entgegenstehende besondere gesetzliche Verwendungsregelung.
Damit wäre dem Wortlaut des Gesetzes nach eine Übermittlung des Datums „Eigenschaft als Kraftfahrzeughalter“ durch die Kfz-Zulassungsstelle an das Sozialamt zur Überprüfung rechtswidriger Inanspruchnahme von Sozialhilfe durch den Betroffenen nicht zulässig. Zwar hat der Gesetzgeber mit § 117 Abs. 3 Satz 4 i. V. m. Satz 1 BSGH die Überprüfung der Eigenschaft des Sozialhilfeempfängers, Kraftfahrzeughalter zu sein, ermöglichen wollen, er hat aber bei der Einführung der Vorschrift durch Gesetz vom 23. Juli 1996 vergessen, die bereits seit dem 28. Januar 1987 geltende Vorschrift des § 35 Abs. 1 StVG entsprechend zu ändern.

Einen Ausweg aus dem Dilemma, dass der Gesetzgeber zum einen die Überprüfung gewollt hat, zum anderen das Gesetz infolge der versehentlich unterlassenen Änderung des § 35 StVG diese Überprüfung aber durch § 117 Abs. 3 Satz 7 BSHG i. V. m. § 35 Abs. 1 StVG verbietet oder doch jedenfalls zu verbieten scheint, bietet meines Erachtens nur folgende Überlegung:
§ 117 Abs. 3 Satz 4 Buchstabe f BSHG liefe vollständig leer, wenn die Zurücktretens-Anordnung des Satzes 7 dieser Vorschrift auch gegenüber § 35 Abs. 1 StVG gälte. § 117 Abs. 3 Satz 4 Buchstabe f BSHG ist spezieller - ist ein konkreterer Ausdruck des Willens des Gesetzgebers - als die Regel des Satzes 7 i. V. m. der (bei Abfassung des Gesetzes nicht notwendig ganz ‘präsenten’) Regel des § 31 Abs. 1 StVG (numerus clausus der Aufgabenerfüllung). Hinzu kommt: § 117 Abs. 3 Satz 4 Buchstabe f BSHG ist das *spätere* Gesetz.

Wendete man Satz 7 des § 117 Abs. 3 BSHG i. V. m. § 31 Abs. 1 StVG gegenüber Satz 4 Buchstabe f an, entstünde wegen des vollständigen Leerlaufens ein eindeutiger Widerspruch im Gesetz. Dieser lässt sich durch einen Vorrang des späteren Gesetzes lösen. Dieser Vorrang lässt sich aber nur dadurch erreichen, dass Satz 7 so einschränkend ausgelegt wird, dass keiner der Bestandteile des Satzes 4 infolge einer älteren gesetzlichen Regelung leerläuft. (Das schließt nicht aus, dass Satz 7 für ein Zurücktreten gegenüber späteren bereichsspezifischen Regelungen für Behörden, die für eine Übermittlung an die Sozialhilfebehörde in Frage kommen, sorgt.)

Im Ergebnis, sich mit einer derartigen Auslegungsbemühung zu behelfen, sind sich die Datenschutzbeauftragten und die Verwaltungspraxis einig. Diese Auffassung der Praxis lässt sich, wie gezeigt, auch mit einer keineswegs rein „subjektiven", d. h. vor allem auf den Willen des (historischen) Gesetzgebers abstellenden Auslegung begründen. Aber das rechtsstaatliche Postulat der „Normenklarheit" ist dabei auf der Strecke geblieben. Der Gesetzgeber sollte, auch darin besteht Einigkeit, § 35 Abs. 1 StVG sobald wie möglich anpassen.
Das SMWA steht diesem Anliegen positiv gegenüber.

10.2.4 Datenerhebung der LVA bei Rentenantrag nach Unternehmensübertragung auf Ehegatten

Einem Bäckermeister war Rente wegen Berufsunfähigkeit bewilligt, wegen der fortgesetzten Einkünfte aus seinem Betrieb aber eine Rente nicht ausgezahlt worden. Noch bevor seine Ehefrau die beantragte Genehmigung zur Führung eines Bäckereibetriebes erlangt hatte, war daraufhin die Bäckerei auf sie umgemeldet worden und hatte der Ehemann bei der LVA die Zahlung einer Erwerbsunfähigkeitsrente beantragt. Die LVA hatte daraufhin unter anderem von ihm wissen wollen,

- inwieweit aufgrund seines Ausscheidens aus dem Unternehmen weitere, fremde Arbeitskräfte eingestellt worden seien,
- inwieweit seit dem Übergang des Unternehmens auf seine Ehefrau dessen Größe sich verändert habe und
- wodurch die Ehefrau sich die erforderlichen Kenntnisse zur Weiterführung des Unternehmens „in allen Belangen" angeeignet habe.

An mich wandte sich der Bäckermeister, nachdem er mit der Begründung, diese Fragen beträfen nicht ihn, sondern das Unternehmen seiner Frau, die Beantwortung dieser Fragen abgelehnt hatte.

(1) Der Hintergrund, vor dem die Fragen der LVA gesehen werden mussten, war folgender:
Die Bewilligung einer Rente wegen Erwerbsunfähigkeit setzt gemäß § 44 Abs. 2 Satz 2 Nr. 1 SGB VI unter anderem voraus, dass der Versicherte keine selbständige Tätigkeit ausübt.
Der Begriff der selbständigen Tätigkeit ist im Gesetz nicht definiert. In Anlehnung an die steuerrechtlichen Regelungen in §§ 2, 15, 18 EStG wird allgemein als Selbständiger eingestuft, wer in der Absicht, Gewinn zu erzielen, nachhaltig tätig ist und auf den Geschäftsbetrieb ausgerichtete Handlungen im eigenen Namen vornimmt oder vornehmen lässt (U. Köbl, in: Schulin, Handbuch des Sozialversicherungsrechts, Band 3, 1999, § 24 Rdnr. 27 m. w. N.).

Auch wenn der Antragsteller das Geschäft durch andere Personen betreiben lässt, ist er selbständig tätig, wenn er nach wie vor auf den Geschäftsbetrieb Einfluss nehmen kann. Dabei ist unerheblich, in welcher Weise sich der Antragsteller nach außen oder innen am Geschäftsbetrieb beteiligt (ständige Rechtsprechung des Bundessozialgerichts, vgl. BSGE 55, 174, 175; Köbl a.a.O. Rdnr. 28).

Eine solche die selbständige Tätigkeit im Sinne von § 44 Abs. 2 Satz 2 Nr. 1 SGB VI begründende Einflussmöglichkeit kann insbesondere auch in ungefähr gleichgeordneter unternehmerischer Beteiligung an einer zwischen Ehegatten bestehenden Berufsgemeinschaft bestehen. Das gilt selbst dann, wenn das Bestehen einer gesellschaftlichen Beziehung den Ehegatten nicht bewusst ist; nur bei lediglich geringfügiger, familienhafter *und* untergeordneter Mitarbeit eines Ehegatten liegt keine Ehegattengesellschaft (Innengesellschaft unter Ehegatten) vor.

Ist ein Betrieb, wie es hier der Fall war, vom Versicherten auf den Ehegatten übertragen worden, muss die Versicherung prüfen, ob der Versicherte nicht mehr in gemäß § 44 Abs. 2 Satz 2 Nr. 1 SGB VI 'rentenschädlicher' Weise an der Führung des Betriebes beteiligt ist. Darauf, wer in der Handwerksrolle eingetragen ist, kommt es nicht an. Nur wer tatsächlich nicht mehr aktiv, auch nicht durch unternehmerische Entscheidungen oder Mitentscheidungen, am Erwerbsleben teilnimmt, ist nicht mehr selbständig erwerbstätig. Nur wenn der Versicherte keinerlei Einfluss auf die Führung des Geschäftsbetriebes nehmen kann und sein Ehegatte tatsächlich alle unternehmerischen Entscheidungen selbständig trifft (z. B. auch die Anschaffung von Maschinen etc.), kann eine sog. Innengesellschaft zwischen den Ehegatten verneint werden.

(2) Aufgrund dessen handelte es sich bei den von der LVA gestellten drei Fragen um Fragen nach Hilfstatsachen. Die Erhebung dieser Hilfstatsachen war hier zur Aufgabenerfüllung erforderlich und daher gemäß § 67 a Abs. 1 SGB X rechtmäßig. Unmittelbar erforderlich war nur die Erhebung der negativen Tatsache, dass der Petent nicht mehr aktiv in einer gemäß § 44 Abs. 2 Satz 2 Nr. 1 SGB VI rentenschädlichen Weise selbständig tätig war, insbesondere auch nicht in dem von ihm seit langem betriebenen und nun (nach außen) im Namen seiner Ehefrau weiterbetriebenen Bäckereiunternehmen. Durch eine bloße Frage nach der Nichtausübung einer entsprechenden Tätigkeit und dem Nichtvorhandensein unternehmerischer Einflussmöglichkeit wäre die Behörde (LVA) ihrer Verantwortung nicht gerecht geworden. Denn sie hatte in den ihr rechtlich gesetzten Grenzen insoweit den Sachverhalt aufzuklären, wie er tatsächlich ist, sie durfte sich nicht mit der bloßen verneinenden Antwort auf die Frage nach der negativen Tatsache begnügen.

Deswegen war die Frage nach Umständen, denen sich Hinweise darauf entnehmen ließen, ob der Petent als früherer Betriebsinhaber im Betrieb nunmehr nicht mehr tätig war und auch keinen unternehmerischen Einfluss mehr ausüben konnte, gerechtfertigt.

Die drei Fragen waren - und zwar auch für den Petenten erkennbar - geeignet, der LVA Informationen zu verschaffen, die es wahrscheinlich oder aber unwahrschein-

lich machten, dass der Petent noch unternehmerischen Einfluss auf den Bäckereibetrieb ausübt. Der Petent sollte hier Auskunft darüber geben, wer seine Aufgaben im Betrieb übernommen hatte (War z. B. ein Bäckermeister oder ein Geselle eingestellt worden?) und wer letztlich die unternehmerischen Entscheidungen im Betrieb traf. War die Ehefrau ab dem Zeitpunkt der Unternehmensüberschreibung auch tatsächlich die alleinige Betriebsinhaberin, oder war der Petent aktiv Mitunternehmer? Für die LVA sollten die Antworten auf diese Fragen insoweit Indizienfunktion haben. Aufgrund der fehlenden Angaben hatte die LVA bislang nicht ausschließen können, dass der Petent noch selbständig tätig war. Nachweise darüber, dass die Ehefrau jetzt die nötige Qualifikation zur Führung des Betriebes besaß, lagen der LVA noch nicht vor. Damit hing auch die Frage zusammen, wie sich das Ausscheiden des Petenten auf den Betrieb ausgewirkt hatte. Seinen Angaben zufolge hatte die Ehefrau schon früher ständig im Betrieb mitgearbeitet, neben einem angestellten Mitarbeiter, so dass im Betrieb immer drei Personen (ein Bäckermeister und zwei Angestellte) gearbeitet hatten. Das Ausscheiden des Petenten - immerhin des Meisters im Betrieb - musste sich somit ganz erheblich auf die Kapazität des Betriebes ausgewirkt haben, es sei denn, es war ein weiterer Mitarbeiter eingestellt worden.

(3) Aus diesem Grunde konnte dem Argument, die Fragen seien unberechtigt, weil sie das Unternehmen der Ehefrau beträfen, also deren Daten und nicht solche des Antragstellers, nicht gefolgt werden:
Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach dem SGB X erhoben, verarbeitet oder genutzt werden (§ 67 Abs. 1 SGB X). Das Datum weist einen Personenbezug auf, wenn es Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person enthält. Einzelangaben sind hierbei alle denkbaren Informationen über eine Person (vgl. Hauck/Haines, Rdnrn. 13 f. zu § 67 SGB X). Durch die Antworten auf die genannten Fragen hätte die LVA nun aber nicht nur Angaben über den Betrieb der Ehefrau erhalten, sondern sie hätte auch Rückschlüsse darauf ziehen können, inwieweit beim Petenten die Ausübung einer rentenschädlichen Erwerbstätigkeit auszuschließen war. Die Antworten hätten also nicht nur personenbezogene Daten der Ehefrau beinhaltet, sondern auch Daten, die den Antragsteller selbst betrafen. Die verlangten Angaben hatten situationsbedingt, nämlich infolge der engen Beziehung zur Ehefrau sowohl Kraft der bestehenden Ehe als auch durch die betriebsbezogene Verbundenheit (ehemalige Mitarbeit der Frau, spätere Übernahme des früheren Betriebes des Mannes) einen (impliziten) Doppelbezug. Dieser Doppelbezug entstand, anders ausgedrückt, durch die Wahrscheinlichkeit, dass der Petent wegen seiner vielfältigen Beziehungen zu diesem Betrieb - nämlich frühere Unternehmereigenschaft und ehelichen Verbundenheit mit der Person, die jetzt zumindest formell Inhaberin des Betriebes war - doch dort unternehmerisch tätig war. Ein solcher Doppelbezug reicht aus, damit das in § 67 a Abs. 2 Satz 1 SGB X ausgesprochene grundsätzliche Gebot, die Daten beim Betroffenen zu erheben, eingehalten wird: Nicht nur die Ehefrau, sondern auch der Petent selbst war im Hinblick auf die Daten, die mittels der genannten Fragen erhoben werden sollten, Betroffener im Sinne der genannten Vorschrift; und dies eben auch dann, wenn er in den Antworten gar nicht ausdrücklich vorkam.

(4) Für die Zulässigkeit einer derartigen Erhebung kann es meines Erachtens nicht darauf ankommen, ob die Erwerbstätigkeit negative Anspruchsvoraussetzungen mit der Folge ist, dass die Beweislast beim Antragsteller liegt (so die h. M., vgl. Köbl a.a.O. Rdnr. 45 und Niesel, in: Kasseler Kommentar, Rdnr. 23 zu § 44 SGB VI, beide unter nicht ohne Weiteres einleuchtender Berufung auf BSGE 45, 238 [Urteil vom 15. Dezember 1977]), ob man statt dessen die Beweislast beim Rentenversicherungsträger sieht, weil § 44 Abs. 2 Satz 2 einen (rechtshindernden oder rechtsvernichtenden) Ausnahme-Tatbestand (so auch BSGE a.a.O. S. 240) darstellt (so Mayer, in: GK-SGB VI § 44 Rdnr. 46, zit. nach Köbl a.a.O.) oder ob man, was wohl vorzugswürdig ist, die bisherige Rechtsprechung des BSG eher im Sinne einer abgestuften Darlegungs- und Beweislast interpretieren soll (in dieser Richtung Köbl, wenn sie a.a.O. Rdnr. 42 ausführt, der Rentenversicherungsträger dürfe einen Nachweis des Nichtvorliegens einer selbständigen Tätigkeit nicht grundlos vom Versicherten verlangen, sondern nur dann, wenn er einen begründeten Anlass zur Annahme einer selbständigen Tätigkeit habe).

(5) Die eigentliche datenschutzrechtliche Frage, nämlich die, ob die LVA dem Petenten die betreffenden Fragen stellen durfte, war damit positiv zu beantworten.
Darüber hinaus stellte sich die Frage, welche Rechtsfolgen es haben würde, wenn der Petent der Aufforderung nicht nachkam. Insoweit durfte und musste ich mich auf allgemeine Hinweise beschränken die seinem Verständnis der Angelegenheit dienen sollten, aber keine Auskünfte zu den rechtlichen Folgen in seinem konkreten Fall darstellten:
Die LVA war auf seine Mithilfe angewiesen. Die Pflicht, zur Aufklärung des Sachverhaltes beizutragen, ergab sich aus dem SGB. Als Antragsteller hatte er bestimmte Mitwirkungspflichten, die in § 60 Abs. 1 Satz 1 SGB I normiert sind. Danach hat der Versicherte, wenn er Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistungspflichten erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen (§ 60 Abs. 1 Satz 1 Nr. 1 SGB I), Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweis und Urkunden vorzulegen oder ihrer Vorlage zuzustimmen (§ 60 Abs. 1 Satz 1 Nr. 3 SGB I). Der Betroffene muss im Rahmen der Auskunftspflicht auch Erkundigungen einholen, wenn ihm entscheidungserhebliche Tatsachen nicht bekannt sind (Seewald, in: Kasseler Kommentar, Rdnr. 15 zu § 60 SGB I). Der Petent war daher im Rahmen seiner gesetzlichen Mitwirkungspflicht gehalten, die geforderten Angaben bei seiner Ehefrau einzuholen, was ihm im Hinblick auf die räumliche Nähe zum Betrieb und aufgrund seiner engen familienrechtlichen Beziehungen zur Betriebsübernehmerin, seiner Ehefrau, auch ohne weiteres zuzumuten war.

Die Wahrnehmung dieser Mitwirkungspflichten liegt jeweils auch zugleich im eigenen Interesse des Leistungsberechtigten (Seewald a.a.O. Rdnr. 2). Kommt der Leistungsberechtigte diesen Mitwirkungspflichten nicht nach und wird hier durch die Aufklärung des Sachverhaltes erheblich erschwert, kann der Leistungsträger nämlich ohne weitere Ermittlungen die Leistung bis zur Nachholung der Mitwirkung ganz oder teilweise versagen oder entziehen, soweit die Voraussetzungen der Leistung nicht nachgewiesen sind (§ 66 Abs. 1 Satz 1 SGB I).

Das Vorgehen der LVA in diesem Fall war also einwandfrei.

10.2.5 Sog. Plausibilitätsprüfung von Anträgen auf Wohngeld

Zur wirtschaftlichen Sicherung angemessenen und familiengerechten Wohnens wird gemäß den Vorschriften des Wohngeldgesetzes (WoGG) Wohngeld als Zuschuss zu den Aufwendungen für den Wohnraum gewährt. Art und Umfang des Wohngeldanspruches sind abhängig von der Höhe der Miete (oder Belastung) und der Höhe des Familieneinkommens. Dieses besteht aus allen Einnahmen der zum Haushalt rechnenden Familienmitglieder innerhalb eines Jahres abzüglich bestimmter notwendiger Aufwendungen.

Um die Angaben der Antragsteller auf die Plausibilität des Verhältnisses zwischen Einnahmen und Ausgaben zu überprüfen, hat die Stadt Dresden als für die Gewährung von Wohngeld zuständige Stelle einen Fragebogen verwendet, mit dessen datenschutzrechtlicher Überprüfung ich aufgrund einer Eingabe befasst worden bin (und der mit ähnlichem Inhalt wohl allenthalben in Sachsen verwendet worden ist).
In dem Fragebogen wurde zum einen nach der Höhe der Ausgaben gefragt, und zwar aufgeschlüsselt nach den Kosten für Ernährung, Unterkunft, Neuanschaffung von Bekleidung, Reinigung und Reparaturen, Haushaltsgegenstände und Möbel, persönliche Dinge des täglichen Lebens, für Telefon, Rundfunk, Fernsehen, Versicherungen sowie Kosten für ein Kfz und Sonstiges. Zum anderen wurde nach der Höhe und Herkunft der Einnahmen gefragt, wobei Sparguthaben, Sachbezüge, Darlehn und Schenkungen als Beispiele von Einkunftsquellen aufgeführt waren. Der Fragebogen enthielt am Ende dieser Auflistung eine Erklärung des Antragstellers, dass er darüber belehrt worden sei, dass falsche oder unvollständige Angaben den sofortigen und rückwirkenden Entzug des Wohngeldes zur Folge hätten.

Anlass dieser sog. Plausibilitätsprüfungen war und ist nach Auskunft des SMI die auf der praktischen Erfahrung beruhende Erkenntnis, dass viele Antragsteller sich nicht darüber im Klaren sind, über welche Einkünfte sie insgesamt verfügen. In schätzungsweise 10 % der Fälle, mit steigender Tendenz, würden aus diesem Grund die Einkommen zu niedrig angegeben, so dass sich ein Missverhältnis zwischen angegebener Miethöhe und angegebenem vergleichsweise niedrigem Einkommen ergebe, das den Wohngeldantrag als nicht plausibel erscheinen lasse. Um dem wahren Einkommen auf die Spur zu kommen, habe sich dieses Verfahren der sog. Plausibilitätskontrolle bewährt. Liste nämlich der Antragsteller seine Ausgaben auf, ergebe sich oft, dass die Ausgaben das angegebene Einkommen übersteigen. Da nicht davon auszugehen sei, dass der Antragsteller ständig über seine Verhältnisse lebt, sei mit einiger Wahrscheinlichkeit sein Einkommen doch größer als angegeben.

Dieses Verfahren, über Angaben zu Ausgaben die Höhe des wirklichen Einkommens zu ermitteln, ist datenschutzrechtlich nicht zu beanstanden. Es findet seine Rechtsgrundlage in den §§ 9 ff. WoGG, insbesondere § 11 Abs. 1 Satz 1 WoGG (i. V. m. § 67 Abs. 1 SGB X i. V. m. Art. II § 1 Nr. 14 SGB I); unterstellt in diesen Vorschriften ist selbstverständlich die Wahrheitsgemäßheit einschließlich der Vollständigkeit der vom Antragsteller insbesondere zu seinem Einkommen zu machenden Angaben.

(Keine ausreichende Erhebungserlaubnis ist dagegen, und zwar wegen § 37 Satz 3 SGB I, § 21 Abs. 1 Nr. 1 SGB X, und auch § 25 WoGG, der lediglich eine besondere Erlaubnis zur Erhebung bei Dritten darstellt.)

Allerdings musste der Umfang des ursprünglichen Fragebogens auf das Erforderliche beschränkt werden. Darüber konnte in einer Besprechung mit dem SMI Einigkeit erzielt werden, so dass nunmehr folgendes geändertes Verfahren angewandt wird:
Zunächst werden die angegebenen („nachgewiesenen“) Bruttoeinnahmen vermindert um den so genannten sozialhilferechtlichen Bedarf, also einen Betrag, den das Sozialministerium jährlich festlegt, der sehr niedrig ist (zurzeit für den Alleinstehenden bei ca. 540,00 DM) und in dem mit Ausnahme der Wohnungsmiete alle Lebenshaltungskosten enthalten sein sollen. Hierbei handelt es sich um eine stark zugunsten des Antragstellers angesetzte Größe.
Liegen die in dem Antrag auf Wohngeld angegebenen Bruttoeinnahmen nicht über dem sozialhilferechtlichen Bedarf, sind die Angaben des Antragstellers nicht plausibel. Er wird dann, wie bisher, zu einem Gespräch mit dem jeweils zuständigen Mitarbeiter der Wohngeldstelle gebeten. (Man will nicht den wegen des Missverhältnisses zwischen angegebener Miethöhe und angegebenem Einkommen nicht plausiblen Antrag einfach wegen fehlender [nämlich nicht auf die Wahrheit gerichteter] Mitwirkung des Antragstellers ablehnen.)

In diesem Gespräch werden Angaben zu den dem Antragsteller obliegenden festen Verpflichtungen, z. B. Versicherungen, Unterhalt, Kredite, Kfz-Kosten und ähnliches, erfragt. Übersteigt schon der Betrag des sog. Existenzminimums, also des sozialhilferechtlichen Bedarfs, die Einnahmen des Antragstellers, so ist dies erst recht der Fall, wenn man hierzu noch seine festen Kosten addiert. In dem Gespräch wird dem Antragsteller dies vor Augen geführt. Da eben nicht davon auszugehen ist, dass der Antragsteller ständig über seine Verhältnisse lebt, wird ihm in diesem Gespräch in aller Regel nunmehr klar, dass er die Höhe seiner Einnahmen wohl nicht richtig dargestellt hat. Im Gespräch mit dem Antragsteller versucht der Bearbeiter, dessen weitere Einnahmequellen zu ermitteln.

Schriftlich festgehalten wird in einem Vordruck, der die Überschrift „Gesprächsprotokoll über die Plausibilitätsprüfung“ trägt, lediglich die Höhe der Summe der ermittelten Ausgaben. Im Unterschied zu dem früheren Verfahren werden diese Ausgaben also nicht in der Akte aufgeschlüsselt. Festgehalten in dem Protokoll werden weiterhin die in dem Gespräch aufgedecken Einnahmequellen, aufgeschlüsselt nach Sparguthaben, Darlehen, Betriebsentnahmen sowie Unterstützungen (finanzieller Art, in Form von Naturalien oder kostenlosen Mahlzeiten).
Je nach Ergebnis dieses Gespräches ist der Wohngeldantrag nunmehr als schlüssig oder nicht schlüssig anzusehen.

Das SMI hat die Regierungspräsidien als übergeordnete Wohngeldstellen angewiesen, die bisherigen Vordrucke zur sog. Plausibilitätskontrolle nicht weiter verwenden und stattdessen den gemeinsam mit mir erarbeiteten Vordruck „Gesprächsprotokoll über die Plausibilitätsprüfung“ einsetzen zu lassen.

10.2.6 Verarbeitung von Patientendaten durch die Kassenärztliche Vereinigung zur sog. Richtgrößenprüfung

Ärzte haben sich an mich gewandt, weil sie von der KV Sachsen einen mit „Anzeige von Praxisbesonderheiten für Richtgrößenprüfung“ überschriebenen Fragebogen erhalten hatten, in dem zu namentlich aufzuführenden Patienten neben der gesetzlichen Krankenkasse, in der sie versichert waren, die Art und Menge der in dem betreffenden Quartal verordneten Arzneimittel, deren geschätzte Kosten (in Apothekenabgabepreisen) sowie mit Hilfe eines Zahlenschlüssels ein sog. Indikationsgebiet angegeben werden sollten, d. h. eine Kombination aus Diagnose und Therapie (Beispiel: „Insulintherapie bei insulinpflichtigem Diabetes mellitus“).
Die Angaben, so sei von der KV mitgeteilt worden, seien nötig, damit die Ärzte einer Regressgefahr entgingen.

(1) Zu den Versuchen, für *Wirtschaftlichkeit der kassenärztlichen Versorgung* zu sorgen und damit zur Kostendämpfung im öffentlichen Gesundheitswesen beizutragen, gehört im Rahmen des § 106 Abs. 2 Satz 1 SGB V u. a. die sog. Auffälligkeitsprüfung bei Überschreiten von Richtgrößen, die gemäß § 84 Abs. 3 SGB V zwischen KV und Krankenkassenverbänden arztgruppenspezifisch insbesondere für das Volumen der je Arzt verordneten Arzneimittel vereinbart werden.
Wird diese Richtgröße von einem Vertragsarzt (‘Kassenarzt’) um einen als Interventionsgrenze bezeichneten Prozentsatz überschritten, wird das Verschreibungsverhalten wegen Auffälligkeit untersucht: In der schwächeren Form als eine bloße Überprüfung, in der stärkeren in Gestalt des Regresses: Nach § 106 Abs. 5 a Satz 1, 2. Halbsatz SGB V *hat der Vertragsarzt bei einer Überschreitung der maßgeblichen Richtgröße den sich daraus ergebenden Mehraufwand zu erstatten, soweit dieser nicht durch Praxisbesonderheiten begründet ist.* (Richtgröße ist von Gesetzes wegen 25 v. H., in Sachsen ist sie wohl aufgrund § 106 Abs. 5 a Satz 4, Abs. 3 Satz 4 SGB V nunmehr durch Vereinbarung auf 15 v. H. herabgesetzt.)

Die Aufforderung der KV, derentwegen die Ärzte sich an mich gewandt haben, war also die Mitteilung der KV, dass sie die Richtgröße in einem Maße überschritten hätten, das zur Erstattungspflicht führen müsse, wenn sich nicht aus den beizubringenden Daten ergebe, dass sie besonders viele Patienten versorgt haben, die unter ein als *Praxisbesonderheit* berücksichtigungsfähiges „Idikationsgebiet“ fallen (d. h. schlichter ausgedrückt, deren Krankheit eine besonders teure Arzneimittelversorgung notwendig macht).

(2) In der schulmäßigen datenschutzrechtlichen Prüfung stellt sich der Vorgang folgendermaßen dar:
Die KV wollte versichertenbezogene Daten erheben, mithin Sozialdaten im Sinne des § 67 Abs. 1 Satz 1 SGB X. Als eine in § 35 SGB I genannte Stelle darf die KV dies gemäß § 67 a Abs. 1 SGB X nur, soweit die Kenntnis der Daten zur Erfüllung einer ihr nach dem SGB obliegenden Aufgabe *erforderlich* ist. Außerdem sind die für eine *Erhebung ohne Mitwirkung des Betroffenen* geltenden Einschränkungen zu berücksichtigen: Betroffene sind hier - übrigens neben den Ärzten, aber doch gewissermaßen als Hauptbetroffene - die (versicherten) Patienten. § 67 a Abs. 2 Satz 2 Nr. 2

Buchstabe a SGB X erlaubt eine solche Erhebung ohne Mitwirkung des Betroffenen - eigentlich eben wegen des möglichen Mehrfachbezuges der Daten: *sämtlicher Betroffener* - bei jemandem, der wie die Vertragsärzte weder eine Sozialbehörde im Sinne von § 35 SGB I noch eine diesen datenschutzrechtlich gemäß § 69 Abs. 2 SGB X gleichgestellte Stelle ist, nur dann, wenn eine Rechtsvorschrift die Erhebung bei ihm zulässt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt.

Diese Voraussetzungen sind im Falle der geschilderten Abfrage von Praxisbesonderheiten erfüllt: Gemäß § 285 Abs. 2 i. V. m. Abs. 1 Nr. 5 SGB V dürfen die Kassenärztlichen Vereinigungen Einzelangaben über die persönlichen und sachlichen Verhältnisse der Versicherten erheben und speichern, soweit dies zur Durchführung von Wirtschaftlichkeitsprüfungen gemäß § 106 SGB V erforderlich ist. Dies ist der Fall: Daten, die in der oben erläuterten Weise *Praxisbesonderheiten* begründen, können nur von den Ärzten stammen, und sie müssen auf einzelne Patienten in nachvollziehbarer Weise, also unter Namensnennung bezogen sein, damit die Angaben auch überprüft werden können. Die Erhebung der Daten ist also erforderlich, und ihre Erhebung beim Arzt ist durch § 285 Abs. 2 i. V. m. Abs. 1 Nr. 5 i. V. m. § 106 Abs. 5 a Satz 1, 2. Halbsatz SGB V zugelassen.

Dem Arzt ist in § 106 Abs. 5 a Satz 1, 2. Halbsatz SGB V die Darlegungs- und Beweislast für das Vorliegen von die Richtgrößenüberschreitung rechtfertigenden Praxisbesonderheiten auferlegt. Das folgt nach allgemeinen Regeln der Gesetzesauslegung daraus, dass der durch Praxisbesonderheiten begründeten Nichteintritt der Erstattungspflicht als Ausnahmeregelung (*soweit nicht*) formuliert ist. Dem entspricht ferner die ständige Rechtsprechung des Bundessozialgerichtes zur Berücksichtigung von Praxisbesonderheiten aus der Zeit vor Einführung des § 106 Abs. 5 a SGB V (Clemens, in: Schulin, HBdSVR Band 1, 1994, § 35 Rdnr. 89 mit umfangreichen Nachweisen; übereinstimmend, wenn auch weniger deutlich, Krauskopf Rdnr. 35 zu § 106 SGB V und Hess, Kasseler Kommentar Rdnr. 33 zu § 106 SGB V).

(3) Ob der behandelnde Vertragsarzt darüber hinaus sogar *verpflichtet* ist, den Prüfungsinstanzen diejenigen Unterlagen zur Verfügung zu stellen, die diese zur Prüfung des Vorliegens einer Praxisbesonderheit benötigen (so Hess a.a.O. Rdnr. 25 zu § 106 SGB V für den Fall der Durchschnittswerte-Prüfung sowie Rdnr. 3 zu § 298 SGB V unter Berufung auf BT-DS 12/5187 S. 33 zu Art. 4 Nr. 14) ist zweifelhaft, kann datenschutzrechtlich aber dahinstehen. Worauf es vielmehr gerade den Ärzten ankommt, das ist, dass es dem Arzt nicht durch die ärztliche Schweigepflicht (strafbewehrt) verboten ist, Praxisbesonderheiten begründende Umstände - in dem genannten erforderlichen Umfang - auch eben unter Offenbarung von Patientendaten der zuständigen Stelle darzutun. Darüber besteht, soweit ersichtlich, jedoch Einigkeit: § 298 SGB V wird als Klarstellung dieser Übermittlungserlaubnis verstanden (Krauskopf Rdnr. 2 zu § 298 SGB V, Hess a.a.O. Rdnr. 3 zu § 298 SGB V mit zutreffendem Hinweis auf die bereits zitierte Bundestags-Drucksache). Denn schon bevor es den § 298 SGB V gab, hat das Bundessozialgericht in seiner Entscheidung vom 19. November 1985 - 6 RKa 14/83, BSGE 59,172 mit ausführlicher Begründung gegenüber der Kritik an diesem von ihm schon länger eingenommenen Standpunkt bekräftigt, dass die ärztliche Schweigepflicht durch die Erhebungsbefugnisse, die den

die Wirtschaftlichkeitsprüfung durchführenden Stellen im Recht der gesetzlichen Krankenversicherung gegenüber den Ärzten eingeräumt werden, eingeschränkt wird (vgl. auch Hess a.a.O. Rdnr. 25 zu § 106 SGB V a. E.).

(4) Ergebnis war demnach, dass die an die Ärzte ergangene Aufforderung der KV Sachsen datenschutzrechtlich nicht zu beanstanden war, und dass die Ärzte ihr nachkommen konnten, ohne das Arztgeheimnis zu verletzen, da es sich um eine befugte Offenbarung von Patientendaten handelte.
Unterstellt ist dabei allerdings, dass - was ich naturgemäß nicht nachprüfen kann - die Richtgröße regelrecht bestimmt (vereinbart) worden ist, auch mit angemessener Fachgruppenbildung, und dass die Indikationsgebiete (gemäß Anlage 3 der Empfehlung zu Richtgrößen vom 10. Februar 1999; vgl. auch Krauskopf Rdnrn. 28 f. zu § 106 SGB V) fachgerecht im Rahmen des den Beteiligten eingeräumten Beurteilungsspielraumes (vgl. Hess a.a.O. Rdnr. 33 i. V. m. Rdnr. 26 zu § 106 SGB V) bestimmt worden sind; dabei ist zu berücksichtigen, dass nach der Rechtsprechung die Möglichkeiten anerkennungsfähiger Praxisbesonderheiten vielfältig sind (ausführlich Clemens a.a.O. § 35 Rdnr. 92).
Für die Zulässigkeit der Offenbarung von Patientendaten, zu der die Ärzte aufgefordert waren, muss es ausreichen, wenn die von der KV gegebene Begründung nicht für sie offensichtlich abwegig, d. h. für jeden Fachkundigen erkennbar unsinnig ist.

Ärzte und KV haben gegen meine Auffassungen keine Einwände erhoben.

10.2.7 Vermittlung von Arbeitswilligen zur Aufbauarbeit in Bosnien

In 7/10.2.1 habe ich aus Gründen des Sozialdatenschutzes vorgeschlagen, die bei der SK eingegangenen Bewerbungen für die Aufbauarbeit in Bosnien komplett an die Arbeitsverwaltung abzugeben, damit das Arbeitsamt (als Fachbehörde für die Arbeitsvermittlung) die weiteren Maßnahmen ergreifen kann. Außerdem bat ich, die betroffenen Bewerber über die Abgabe ihrer Bewerbungsunterlagen an die Arbeitsverwaltung schriftlich zu informieren.

Die SK hat mir Mitte Juni 1999 bestätigt, dass meinen Vorschlägen vollständig gefolgt worden sei.

10.2.8 „Diabetes-Vereinbarung Sachsen“

Das SGB appelliert zwar an Ärzte und Kassen, sich um Qualitätssteigerungen zu bemühen, regelt aber die Einzelheiten der damit verbundenen Datenverarbeitung nicht. Das ist besonders heikel, weil es um Gesundheitsinformationen, besser: Krankheitsdaten, geht und jede Übermittlung solcher Daten als Bruch der Schweigepflicht strafbar sein kann. Die KV Sachsen hat mit den gesetzlichen Krankenkassen im Jahr 1999 eine Vereinbarung getroffen, die dafür sorgen soll, dass die Qualität der vertragsärztlichen Versorgung von Zuckerkranken verbessert wird. Dies soll dadurch geschehen, dass bestimmte aussagekräftige Befunde erhoben werden. Wenn dabei bestimmte Werte erreicht werden, soll der Patient in bestimmter Weise behandelt oder zum Spezialisten überwiesen werden. Um das sicherzustellen, braucht man

patientenbezogene Daten und außerdem Anreize: Die - freiwillig - am Qualitätssicherungs-Programm teilnehmenden Ärzte müssen Erhebungsbögen mit patientenbezogenen Befunden abgeben. Für die Übermittlung dieser Daten und ein entsprechendes Behandlungs- und Überweisungsverhalten werden besondere Gebühren/Honorare gezahlt.

Die Vertragsparteien haben mich nicht zu Rate gezogen, obwohl sie bei Vertragsschluss wussten, dass in Thüringen der Landesdatenschutzbeauftragte bereits dafür gesorgt hatte, dass das Verfahren nur noch mit Einwilligung der Patienten betrieben wurde. Es waren Ärzte, die mich auf die Angelegenheit aufmerksam gemacht haben - und in der Tat: Die Übermittlung der Befunde unter Bezug auf Versicherungsnummer und Versichertennummer des Patienten an die KV war rechtswidrig. Von dem halben Dutzend Ermächtigungsgrundlagen aus dem SGB, die man mir dann nannte, passte, wie sich bei genauerem Hinsehen herausstellte, keine Einzige. Die KV konnte aus den Abrechnungsunterlagen die Klarnamen und Anschriften der Patienten entnehmen, dass der Personenbezug der Daten auf den Dokumentationsbögen unzweifelhaft war. Damit war das Patientengeheimnis verletzt.

Es blieb zunächst bei dem auf meine Aufforderung hin von der KV verfügten Stopp des Verfahrens. Den Ärzten, die die Bögen mühsam ausgefüllt hatten, musste die KV erklären, sie vorerst nicht zu wollen.

Die Lösung, die schließlich einvernehmlich gefunden worden ist, sieht folgendermaßen aus: Die Angaben zum Befund bzw. zur Behandlung erhebt die KV nicht mehr, weil sie entweder maschinell verschlüsselt also für sie unverständlich sind oder ihr nur im verschlossenen Umschlag zur Weiterbeförderung übersandt werden. Die Daten gehen nämlich zur Auswertung an ein Universitätsinstitut. Diesem sind die Befund- und Behandlungsangaben verständlich, aber die den Patienten individualisierende Angabe - nämlich unverändert Versicherungsnummer und Versichertennummer - ist ihm unverständlich. Diesen Grad an Pseudonymisierung halte ich im Hinblick auf die Wahrung des Patientengeheimnisses (§ 203 StGB) zumindest für eine Übergangszeit für ausreichend sicher; bei der - zeitgemäßen - Umstellung auf eine arbeitssparende maschinelle Bearbeitung der Daten schon bei den Ärzten, über die noch nachgedacht wird, sollte die Verschlüsselung (Pseudonymisierung) verstärkt werden, wobei Fachleute eher dazu raten, die Versichertennummer noch einmal zu verschlüsseln statt in der Praxis fortlaufende Nummern zu vergeben, weil dies Verfahren doch verhältnismäßig fehleranfällig sei. Zu einer solchen Verbesserung habe ich die Beteiligten ebenso ermuntert wie zur bisher noch unterbliebenen, die neue Verfahrensweise widerspiegelnden Änderung des Vertragstextes und vor allem auch zur sorgfältigen Unterrichtung der Ärzte: Verständlicherweise sind gerade Ärzte, die ihr Berufsgeheimnis besonders ernst nehmen und denen an dieser Qualitätssicherung besonders viel liegt, verunsichert, wenn sie befürchten müssen, dass aus den Reihen der Ärzte lautgewordene Warnungen vor der Verletzung des Arztgeheimnisses beim ‘Basteln’ der Diabetes-Vereinbarung zunächst in den Wind geschlagen worden sind.

Ich freue mich aber, dass am Ende eine Lösung entwickelt werden konnte, die die grundlegenden Verschwiegenheitspflichten des SGB einhält: Die Krankenkassen er-

fahren keine patientenbezogenen Daten; die KV erhält nur Daten zum Zweck der Abrechnung. Soweit sie Daten über den Arzt und seine Tätigkeit erfährt, liegt dem eine aufgeklärte und freiwillige Einwilligung des Arztes zugrunde. Die qualitätssichernde Datenverarbeitung selbst liegt in den Händen eines neutralen (Universitäts-) Instituts, dort liegen die Daten der Patienten strikt anonymisiert vor.

10.3 Lebensmittelüberwachung und Veterinärwesen

Übermittlungen an eine private Datenbank für „Tierschutzfälle“

Ein Tierschutzverein wollte in Zusammenarbeit mit der Tierärztlichen Hochschule in Hannover eine Datenbank aufbauen, in der Fälle von Zuwiderhandlungen gegen das Tierschutzrecht erfasst werden sollten. Hierzu sollten die für Tierschutzrecht zuständigen Stellen, insbesondere die für die Ahndung von Ordnungswidrigkeiten nach § 18 TierSchG (Tierschutzgesetz) zuständigen Länderbehörden, Erhebungsbögen ausfüllen, und damit Auskünfte zum Tierhalter, zum Sachverhalt und zum Verfahren erteilen. Unter anderem sollte neben dem Tag der Tat das behördliche, staatsanwaltschaftliche und gerichtliche Aktenzeichen angegeben werden, der Beruf des Tierhalters, sein Tatmotiv sowie Art und Höhe der gegen ihn verhängten Sanktionen. Gegebenenfalls sollten weitere Unterlagen an den Verein bzw. die Hochschule gesandt werden; Zweck dieser Datensammlung sollte, so hieß es weiter, die Erleichterung der Bearbeitung von Tierschutzfällen sein sowie die Vereinheitlichung der Ahndung gleichgelagerter Fälle. Die Behörden sollten die Datenbank dazu - bundesweit - nutzen.

Das Vorhaben ist, wie beim SMS und mir, ganz überwiegend bei den zuständigen Länderministerien und den Landesdatenschutzbeauftragten auf Ablehnung gestoßen: Weder das TierSchG - ein Bundesgesetz -, namentlich auch nicht sein § 16 f Abs. 3, noch sächsisches Recht bieten die nötige Rechtsgrundlage für die Übermittlung solcher - personenbezogener - Daten an den Verein bzw. die Hochschule.
Es ist nicht nachzuvollziehen, aus welchem Grund die ordnungsgemäße, insbesondere gesetzesgemäße Ausführung des Tierschutzrechtes, einschließlich dazugehörender Bußgeld- und Strafvorschriften, auf eine solche Datensammlung angewiesen sein soll. Es fehlt daher an der sowohl für § 16 f Abs. 3 TierSchG wie auch für eine Übermittlung nach § 13 Abs. 1, § 15 Abs. 1 Nr. 1, 1. Tatbestands-Voraussetzung, SächsDSG nötigen Erforderlichkeit der Übermittlung für die Aufgabenerfüllung der übermittelnden Stelle. Im Hinblick auf § 15 Abs. 1 Nr. 2 SächsDSG ist von einem schutzwürdigen Interesse der Betroffenen auszugehen, dass nicht private Stellen oder Hochschulen ohne ihre Einwilligung personenbezogene Daten über ihre Rechtsverstöße von den zuständigen Behörden übermittelt bekommen. (Der Verhältnismäßigkeitsgrundsatz gilt eben auch zugunsten von Tierquälern!)

11 Landwirtschaft, Ernährung und Forsten

In diesem Jahr nicht belegt.

12 Umwelt

12.1 Deckung des Datenbedarfs im Vorfeld einer geplanten Änderung des Bemessungsmaßstabs einer Gebühr

Ein Wasserversorgungs- und Abwasserzweckverband wollte den Bemessungsmaßstab für die Grundgebühr umstellen und sich dafür, vor Verabschiedung der Satzungsänderung, für die (ihm bekannten) angeschlossenen Grundstücke jeweils das künftig maßgebliche Datum, nämlich die Anzahl der Wohnungseinheiten auf dem Grundstück, besorgen. Diese Daten wollte sich der Zweckverband von den Abfallämtern der Landkreise übermitteln lassen.

Das Datum „Anzahl der Wohnungseinheiten eines Grundstückes" ist ein personenbezogenes Datum, da eine Angabe über sachliche Verhältnisse einer zumindest bestimmbaren natürlichen Person gemacht wird (§ 3 Abs. 1 SächsDSG). Beide Verarbeitungsschritte bedurften einer Grundlage: Sowohl die Erhebung durch den Zweckverband als auch die Übermittlung durch die Abfallämter.

(1) Nach In-Kraft-Treten der Satzungsänderung würde die Rechtsgrundlage für beides vergleichsweise unproblematisch sein:
(1.1) Der Zweckverband würde gemäß § 11 Abs. 1 SächsDSG das Datum erheben dürfen, weil er es zur Erfüllung seiner Aufgaben benötigen würde, die satzungsgemäßen (vgl. § 2 Satz 1 SächsKAG) Gebühren für die Benutzung seiner Anlagen zu erheben.
Zusätzlich würde es aber einer Erlaubnis dafür bedürfen, dass der Zweckverband die Daten nicht bei den Betroffenen, den (gebührenpflichtigen) Grundstückseigentümern, sondern ohne deren Mitwirkung bei einem Dritten, eben den Abfallämtern, erheben würde. Hierfür findet sich unter den einschlägigen Erlaubnistatbeständen des § 11 Abs. 4 SächsDSG auch eine Grundlage: Nummer 8 der Vorschrift wägt mit den natürlich ebenfalls grundrechtsrelevanten Belastungen ab, die der Abgabenzahler zu tragen hätte, und spricht eine Erlaubnis für den Fall aus, dass *die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür vorliegen, dass überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.*
Dem Aufwand, alle Grundstückseigentümer anzuschreiben, stünden keine, zumindest keine überwiegenden, schutzwürdigen Interessen der Grundstückseigentümer entgegen.
Die geplante Erhebung würde demnach erlaubt sein. Allerdings würde es ratsam sein, dass der Zweckverband bei der ersten Nutzung der Daten gegenüber den Betroffenen, also wohl bei der ersten Abrechnung, erläuterte, dass er die Daten (nach datenschutzrechtlicher Überprüfung) von der Abfallbehörde des Landkreises bekommen habe, und zugleich Gelegenheit gäbe, unzutreffende (veraltete u. ä.) Daten zu berichtigen.

(1.2) Die Abfallämter würden auch die Daten an den Zweckverband übermitteln dürfen, und zwar gemäß § 13 Abs. 1 SächsDSG:
Der Zweckverband würde die Daten zur Aufgabenerfüllung, wie dargelegt, benötigen (§ 13 Abs. 1 Nr. 1 SächsDSG). Zusätzlich wäre auch die Voraussetzung des § 13 Abs.

1 Nr. 2 erfüllt, weil diese Vorschrift, vermittelt über § 12 Abs. 2 Nr. 1 SächsDSG, auf die Erlaubnistatbestände des § 11 Abs. 4 SächsDSG verweist, dessen Nummer 8, wie ebenfalls vorstehend dargelegt, hier erfüllt sein würde.

(2) Vor In-Kraft-Treten der Satzungsänderung ist es anders: Die bloße Existenz eines Satzungsentwurfes, der einen Wechsel zu einem anderen als dem bisherigen Bemessungsmaßstab vorsieht, hat keine datenschutzrechtliche Vor-Wirkung, d. h. begründet noch nicht mit rechtlicher Wirkung die Aufgabe, für die einzelnen (angeschlossenen) Abgabenschuldner, die auf der Grundlage des geplanten künftigen Bemessungsmaßstabes sich ergebenden Bemessungseinheiten zu erheben.
Soll der Gebühren- oder Beitragsmaßstab geändert werden, gibt es meiner Auffassung nach folgende zwei Möglichkeiten:

(2.1) Der Zweckverband könnte eine Erhebung durchführen, die der Gewinnung eines Überblickes, d. h. von Erkenntnissen über die tatsächlichen Verhältnisse in ihrer Gesamtheit, diente, aus der dann auf die Wirkungen möglicher Gebühren- bzw. Beitragsfaktoren gefolgert werden könnte. Juristisch wäre dies eine amtliche Statistik (vgl. §§ 1 Abs. 1 Satz 1, 2 Abs. 1 Nr. 4, 8 Abs. 4 und 9 Abs. 7 SächsStatG). Dazu müsste der Zweckverband vorübergehend eine den Anforderungen des § 9 SächsStatG entsprechende gesonderte Statistikstelle einrichten. Die Erhebung könnte vermutlich auf eine Stichprobe beschränkt werden.
In diesem Fall wäre dann die Abgabensatzung des Zweckverbandes auf der Grundlage der durch die Statistik gewonnenen Erkenntnisse auszugestalten. Dabei wäre allerdings dreierlei zu beachten:

(2.1.1) Eine solche Kommunalstatistik wäre gemäß § 8 Abs. 2 SächsStatG nicht zulässig, wenn dem Zweckverband die für eine hinsichtlich des Beitragsmaßstabes rechtmäßige Gestaltung der Abgabensatzung benötigten Daten vom Statistischen Landesamt zur Verfügung gestellt werden könnten. Solche Daten könnten im vorliegenden Falle die Gesamtanzahl der angeschlossenen Wohnungen (oder Wohnungsanschlüsse), vielleicht auch die Durchschnittszahl je Hausanschluss sein.
Dieses der Vermeidung unnötiger Doppelerhebungen dienende Subsidiaritätsgebot des § 8 Abs. 2 SächsStatG wird dadurch gesichert, dass gemäß § 3 der Vorschrift der Vorbereitung einer Satzung für eine Kommunalstatistik - neben dem Sächsischen Datenschutzbeauftragten - auch das Statistische Landesamt zu beteiligen ist.

(2.1.2) Sollten diese Zahlen nicht vom Statistischen Landesamt zu bekommen sein, müsste der Zweckverband die Statistik selbst durchführen, was für ihn einige Kosten verursachte. Denn der Ausweg, dass die Abfallämter, welche über die betreffenden Daten verfügen, die statistischen Werte lieferten, steht nicht offen. Es handelte sich nämlich um eine Datennutzung durch die Abfallämter, für die als Rechtsgrundlage nur § 7 Abs. 1 SächsStatG (der den insoweit engeren § 12 Abs. 3 Satz 1 SächsDSG verdrängt) in Frage käme. Diese Erlaubnis von *Statistiken im Verwaltungsvollzug* gilt jedoch nur für die Datennutzung für die Erfüllung der eigenen Aufgaben und ergänzend derjenigen der jeweils übergeordneten öffentlichen Stelle. Diese Voraussetzungen wären im vorliegenden Falle nicht erfüllt. Namentlich ist Amtshilfe nicht eine der in § 7 Abs. 1 SächsStatG gemeinten Aufgaben.

Da für Wasser und Abwasser die Gemeinden, für Abfall jedoch die Landkreise zuständig sind, ist auch der Ausweg über eine gemeinsame kommunale Statistikstelle, den § 9 Abs. 6 Satz 1 SächsStatG vorsieht, verbaut.

(2.1.3) Schließlich fragte es sich, ob eine auf der Grundlage einer solchen statistischen Erhebung - statt auf der Grundlage einer im Rahmen des Verwaltungsvollzuges stattfindenden Totalerhebung - durchgeführte Globalberechnung (im Sinne des § 18 Abs. 2 SächsKAG) bzw. Gebührenbemessung (gemäß § 14 SächsKAG) den Anforderungen der Rechtsprechung des Sächsischen Oberverwaltungsgerichtes an die Beitrags- bzw. Gebührenkalkulation genügte. Dagegen spricht, dass das SächsOVG verlangt, dass „dem Satzungsgeber bei der Beschlussfassung über die Festsetzung der Gebühren eine Kalkulation vorgelegen hat, die auf fehlerfrei ermittelten [...] Bemessungsfaktoren beruht“ (SächsOVG Urteil vom 9. September 1998 - 2 S. 617/95, LKV 1999, 275 rSp. unten). Bedenkt man jedoch, dass in dem vom SächsOVG entschiedenen Fall dem satzungsgebenden Gemeinderat bei seiner Beschlussfassung eine Kalkulation überhaupt nicht vorgelegen hat, erscheint gegenüber einer zu strengen Auslegung der zitierten Passage der Begründung Vorsicht geboten. Vermutlich werden die Anforderungen, die an die Ermittlung der Kostenfaktoren zu stellen sind, strenger sein als diejenigen, die an die Ermittlung der Bemessungsfaktoren zu stellen sind.
Auch die vergleichsweise weniger strengen Formulierungen in der Entscheidung vom 24.10.1996 (2 S 175/96 SächsVBl. 1997, 34, 35 lSp.), die an eine Entscheidung des Baden-Württembergischen Verwaltungsgerichtshofes vom 12. Oktober 1989 anknüpfen, sind keineswegs ohne weiteres so zu verstehen, dass eine Festsetzung des Beitragssatzes durch den Satzungsgeber auf der Grundlage einer ordnungsgemäß durchgeführten Statistik wegen der wahrscheinlichen Abweichung der Statistik von den tatsächlichen Verhältnissen als Ermessensfehler anzusehen sein müsste.
Immerhin dürfte es kein Einzelfall sein, dass der (materielle) Gesetzgeber Entscheidungen auf der Grundlage amtlicher Statistiken treffen muss; gerade auch der Informationsbedarf der normsetzenden Beschlusskörperschaften ist bei der gesetzlichen Aufgabenbestimmung der amtlichen Statistik (vgl. § 1 Abs. 1 SächsStatG) gemeint.

(2.2) Daneben sehe ich die Möglichkeit einer zeitlichen Staffelung in der Abgabensatzung, ohne Durchführung einer Statistik:
Der Zweckverband kann sich zunächst in Satzungs-Form für einen bestimmten Bemessungsmaßstab entscheiden, also etwa die Zahl der Wohnungsanschlüsse je Grundstück. Auf der Grundlage einer dahingehend verabschiedeten Satzung kann er dann die Daten erheben, aus denen hervorgeht, in welchem Maße das betreffende Kriterium jeweils erfüllt wird, also wie viele Bemessungseinheiten je angeschlossenen Benutzer jeweils vorhanden sind. Auf dieser Grundlage kann der Zweckverband sodann die angemessenen kostendeckenden Tarife (Gebühren- oder Beitragssatz je Bemessungseinheit) berechnen und durch ergänzende Satzung festsetzen und danach dann die Abgaben dementsprechend erheben.

Auch hier stellt sich allerdings die Frage, ob eine solche Lösung den Anforderungen des SächsOVG an ein rechtmäßiges Zustandekommen einer Gebühren- oder Beitragssatzung entspricht. Das Gericht legt § 2 Satz 1 SächsKAG dahingehend aus,

dass die Festsetzung des Gebührensatzes zum notwendigen Mindestinhalt der Gebührensatzung gehört (LKV 1999, 275, 276 lSp. oben; ähnlich schon SächsVBl. a.a.O. S. 35, lSp. Mitte). Auf den ersten Blick erscheint die vorgeschlagene zeitliche Staffelung damit als unzureichendes Verfahren zur Beschaffung der benötigten Daten. Bei näherer Betrachtung erweist sich allerdings das gegenteilige Ergebnis als durchaus wahrscheinlich:
Zunächst ist zu berücksichtigen, dass diese Rechtsprechung strenger ist als in anderen Bundesländern (vgl. LKV 1999 S. 275/276). Auch vom Zweck der vom SächsOVG in Auslegung des § 2 Satz 1 und 2 SächsKAG aufgestellten strengen Regel her ist es nicht erforderlich, die genannte Staffelung für ein unzureichendes Verfahren der Beschaffung der Daten auf der Bemessungsfaktorenseite der Kalkulation zu halten. Denn verhindert werden soll ja eine ermessensfehlerhafte Berechnung des Gebühren- oder Beitragssatzes und die auf seiner Grundlage stattfindende tatsächliche wirtschaftliche Belastung der Abgabenpflichtigen. Eine solche Belastung wäre jedoch bei der vorgeschlagenen zeitlichen Staffelung vermieden, und die Voraussetzungen einer fehlerfreien Bestimmungen des Abgabensatzes durch den Satzungsgeber wären, was die Bemessungsseite der Abgabenkalkulation betrifft, gewährleistet.

(2.3) Eine dieser beiden Möglichkeiten muss das Abgabenrecht eröffnen, zumal bei einer bloßen - verbrauchsunabhängigen - Grundgebühr (§ 14 Abs. 1 Satz 3 SächsKAG). Denn die, soweit ich zu erkennen vermag, einzig übrig bleibenden dritte Möglichkeit scheint mir auf jeden Fall ausgeschlossen:
Die Rechtsprechung des SächsOVG mit ihren strengen Anforderungen an die zum Zeitpunkt der Beschlussfassung erforderliche Kenntnis des Satzungsgebers von den Bemessungsfaktoren (in der Entscheidung von 1996 „Flächenfaktoren“ genannt) kann, auch i. V. m. § 2 Satz 1 und 2 SächsKAG, nicht als hinreichend bestimmte Aufgabenzuweisung angesehen werden, die i. V. m. § 11 Abs. 1 SächsDSG vor der Beschlussfassung über die Satzung die nötige Rechtsgrundlage dafür darstellte, dass die kommunale Körperschaft die personenbezogenen Daten erhebt, die *zugleich* die Globalberechnung auf der Bemessungsfaktor-Seite und die Abgabenerhebung im Einzelfall ermöglichen. Dies liefe nämlich darauf hinaus, § 2 Satz 1 und 2 SächsKAG als Ermächtigung der Verwaltung dafür anzusehen, das Vorhandensein von der Verwaltungsspitze frei gewählter Bemessungsfaktoren bei sämtlichen in Frage kommenden Abgabeschuldnern zu erheben, ohne dass durch den Satzungsgeber vorher festgelegt worden wäre, dass der betreffende Bemessungsfaktor auch tatsächlich für die Abgabenbemessung einmal maßgeblich sein soll. Möglich wäre dann ja sogar auch, dass die Verwaltungsspitze zur gleichen Zeit die jeweilige Ausprägung mehrerer verschiedener, einander ausschließender Bemessungsmaßstäbe bei den möglichen Abgabenschuldnern erhöbe und danach im günstigen Falle einer dieser Bemessungsmaßstäbe durch den Satzungsgeber maßgeblich gemacht würde.
Durch Anwendung des Verhältnismäßigkeitsgrundsatzes wäre einem solchen Vorgehen kein Riegel vorzuschieben, da es ja der Verwaltungsspitze der kommunalen Körperschaft überlassen wäre, sich nach Belieben - innerhalb der Grenzen des KAG - den am ehesten genehmen Bemessungsfaktor herauszusuchen und dafür jeweils eine Totalerhebung durchzuführen (oder eben sogar dasselbe gleich mehrfach zur gleichen Zeit). Eine solche Auslegung von § 2 Satz 1 und 2 SächsKAG i. V. m. § 11 Abs. 1 SächsDSG verstieße gegen die Bestimmtheitsanforderungen, die an Rechtsvorschrif-

ten zu stellen sind, welche zum Eingriff in das Grundrecht auf informationelle Selbstbestimmung ermächtigen.

Ich habe die aus Anlass der Anfrage des Zweckverbandes angestellten vorstehenden Überlegungen dem SächsOVG, SMUL und SMI sowie dem SSG unterbreitet; Einwände sind mir bisher nicht bekannt geworden.

12.2 Bezugnahmen auf Rechtsstreitigkeiten wildfremder Leute

Bei jemandem, der gegen den Abwassergebührenbescheid einer Großen Kreisstadt geklagt hatte, hatte es erhebliches Unbehagen ausgelöst, als er in der vom Oberbürgermeister persönlich unterzeichneten Klageerwiderung der Behörde Passagen wie diese fand:

Bezüglich der Sachverhaltsdarstellung nimmt die Beklagte wie folgt Bezug:

1. *Entscheidung des Verwaltungsgerichtes Dresden, Stadt X gegen Herrn [vollständiger Name], [vollständiges Aktenzeichen]*
2 *Ausführungen des Landratsamtes Y in seinem ablehnenden Widerspruchsbescheid vom [genaues Datum] zum Widerspruch der Frau [vollständiger Name und vollständige Anschrift] gegen Abwassergebührenbescheide*

...

Auf diese Weise waren durch die Große Kreisstadt personenbezogene Daten Dritter an den Kläger übermittelt worden, der sich daraufhin mit der Befürchtung, dass die Stadtverwaltung Bürger, die ihre Rechte zu vertreten suchen, mit solchem Vorgehen als Störenfriede an den Pranger stellen wolle, an mich gewandt hat.

Mittelbar ging diese Datenübermittlung darüber sogar noch beträchtlich hinaus, da sie die gesamten Angaben erfasste, die in den genannten Schriftstücken zu Privatpersonen enthalten sind. Denn die in den Rechtsstreit eingeführten Schriftstücke müssen vollständig den Parteien, also auch dem (privaten) Kläger des Verwaltungsrechtsstreites, eben dem Petenten, zur Verfügung stehen.
Es hatte auch keinen Grund gegeben, der es erforderlich gemacht hätte, die betreffenden Schriftstücke unter Namensnennung, also ohne hinreichende Anonymisierung ihres Wortlautes, in das Verfahren einzuführen. Ein dem § 13 Abs. 2 VwVfG entsprechender Zusammenhang zwischen dem Rechtsstreit des Petenten und denjenigen Verfahren, aus denen die genannten Schriftstücke stammten, bestand nicht: Vom konkreten Streitgegenstand der anderen Verfahren war der Petent in seinen rechtlichen Interessen nicht berührt; Übereinstimmungen gab es lediglich hinsichtlich bestimmter Rechtsfragen, welche den Verfahren gemeinsam waren.

Der Oberbürgermeister hat den Datenschutzrechtsverstoß ohne Weiteres eingesehen, sein Bedauern darüber erklärt (und den Fehler darauf zurückgeführt, dass anstelle des in der Stadtverwaltung für solche Verfahren zuständigen Juristen in dessen Abwesenheit ein insoweit nicht zuständiger Bediensteter den Text formuliert habe); es handele sich um einen Ausnahmefall, gegen dessen Wiederholung man inzwischen Vorkehrungen getroffen habe.
Damit konnte die Angelegenheit ohne Beanstandung abgeschlossen werden.

13 Wissenschaft und Kunst

13.1 Forschungsauftrag des BMJ zum neuen Kindschaftsrecht

Seit dem 1. Juli 1998 gelten, aufgrund des Gesetzes zur Reform des Kindschaftsrechts vom 16. Dezember 1997 (Kindschaftsrechtsreformgesetz - KindRG, BGBl. I S. 2942), für den Fall einer Ehescheidung Neuregelungen zur elterlichen Sorge, zum Recht der Eltern auf Umgang mit dem Kind und zu anderen die Kinder betreffenden Fragen. Das BMJ hat ein privates Forschungsinstitut damit beauftragt, eine rechtstatsächliche Untersuchung zur Bewertung dieser gesetzlichen Neuregelung durchzuführen. Diese von Bundesministerien als Vorarbeit für gesetzgeberische Tätigkeit immer häufiger angewandte Vorgehensweise geht in der Regel mit der Verarbeitung personenbezogener Daten einher. Im vorliegenden Fall war es freilich nicht mit der Auswertung von Akten der Justiz getan. Vielmehr sollten - neben sogenannten Expertenbefragungen, also Umfragen bei Richtern, Anwälten sowie Bediensteten von Jugendämtern - Betroffene selbst befragt werden; genauer gesagt sollten und sollen alle Eltern um Angaben gebeten werden, deren Ehescheidungsverfahren im ersten Quartal 1999 im ersten Rechtszug abgeschlossen worden sind.

In dem dabei zu verwendenden Fragebogen geht es natürlich um sehr persönliche Dinge. Aber darum hatte ich mich, als sich das Forschungsinstitut und das SMJus in der Angelegenheit an mich wandten, nicht zu kümmern - schon deswegen nicht, weil die, natürlich auf freiwilliger Grundlage, zu beantwortenden Fragen eben von einer privaten, zudem außerhalb Sachsens angesiedelten Stelle gestellt wurden. Zuständig war ich aber insoweit, als das Forschungsinstitut auf die Mithilfe der sächsischen Justizbehörden (§ 24 Abs. 2 SächsDSG!) angewiesen war, um an die zu befragenden Geschiedenen gezielt herantreten zu können.

Gewünscht hatte das - datenschutzrechtlich kundige - Forschungsinstitut von vornherein nicht die Überlassung der Namen und Anschriften der betreffenden Eltern, sondern nur die so genannte Adressmittlung: Die Familiengerichte in Sachsen sollten die bei ihnen in den Scheidungsverfahrensakten enthaltenen Daten *Namen und Anschriften der im ersten Quartal 1999 im ersten Rechtszug geschiedenen Eheleute, die Eltern gemeinschaftlicher minderjähriger Kinder sind*, verwenden, um an die Betreffenden den Fragebogen des Forschungsinstitutes mitsamt dessen Anschreiben zu versenden, in dem es um Beteiligung an der Untersuchung bitten wollte.

Rechtlich handelte es sich dabei um eine zweckändernde Nutzung personenbezogener Daten durch die Familiengerichte, die mangels bereichsspezifischer Regelungen nach § 12 Abs. 2 Nr. 4 SächsDSG zu beurteilen war.
Die danach nötige *Erforderlichkeit* war gegeben: Die mit der gewünschten Adressmittlung verbundene Datennutzung durch die Familiengerichte war, soweit erkennbar, die einzige Art und Weise, es der forschungtreibenden Stelle zu ermöglichen, mit Aussicht auf Erfolg und vertretbarem Aufwand an die betreffenden Eltern - und damit den für die Untersuchung in erster Linie als Auskunftspersonen benötigten Personenkreis - heranzutreten und die erforderliche Menge an Auskunftsbereiten zu gewinnen.

Es fehlte auch nicht an einem - ja auch praktischen, rechtspolitisch bedeutungsvollen - wissenschaftlichen Interesse an der Durchführung des Forschungsvorhabens. Die Gestaltung der Erhebungsbögen ließ beim Laien keine Zweifel an der wissenschaftlichen Qualität der Studie entstehen, zumal man im BMJ den nötigen Sachverstand vermuten durfte, nur eine wissenschaftlich geeignete Studie in Auftrag zu geben, auch wenn bei solcher Auftragserteilung die Gefahr eines Gefälligkeitsgutachtens, also einer Einschränkung der Unabhängigkeit der Forschung, nie ganz auszuschließen ist.
Bei der nötigen Abwägung zwischen dem wissenschaftlichen Interesse an der Durchführung des Forschungsvorhabens und dem durch die zweckändernde Datennutzung erfolgenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung war davon auszugehen, dass der Grundrechtseingriff durch die Adressmittlung sehr geringfügig sein würde, da eine Datenübermittlung ja vermieden werden sollte. Bei dieser Abwägung, zumindest jedoch im Rahmen der Ermessensausübung, welche der Entscheidung über die tatsächliche Durchführung des Adressmittlungsverfahrens, also der Datennutzung, zugrunde liegen würde, waren aber meiner Auffassung nach Anforderungen an die Art und Weise zu stellen, in welcher das Institut - eben unter Nutzung der Adressmittlung durch die Justizverwaltung - die Daten von den Eltern sich zu beschaffen versuchen wollte. Dabei habe ich es als unbedenklich angesehen, dass das Forschungsinstitut in dem Anschreiben die Verlosung von 200 für Kinder geeigneten Geschenken unter den Einsendern ankündigen wollte. Die Gewährung eines derartigen finanziellen - „aleatorischen“ - Anreizes (durch Private!) für die Hingabe von Daten ist nicht schon an und für sich sittenwidrig oder sonst bedenklich (auch nicht wettbewerbswidrig, vgl. OLG Stuttgart, Urteil vom 27. November 1998, Az.: 2 U 111/98, RDV 1999, 77). Es ist vielmehr ein normaler Vorgang in der Tausch-Gesellschaft, die zugleich gerne als „Informationsgesellschaft“ bezeichnet wird, in der also Informationen ein wichtiges Gut sind. Informationen sind kein Gut extra commercium.
Hinzunehmen war meines Erachtens auch, dass in den Fragebögen Daten über Dritte erhoben werden sollten, nämlich über den Scheidungspartner und die gemeinsamen Kinder. In den Sozial- und Humanwissenschaften, in denen Sachverhalte untersucht werden, an denen notwendig mehrere Personen beteiligt sind (Beziehungs-Sachverhalte), wird man ohne das nicht auskommen können, wird man also solche Datenerhebungen bei Dritten nicht als unredlich ansehen können. Denn ohne die Untersuchung der wechselseitigen Sicht innerhalb der Beziehungen lassen sich diese Beziehungen nicht hinreichend erforschen. Daher stand die meiner Auffassung nach bei dieser Studie bestehende Möglichkeit, auch ohne Verwendung der Namen und Anschriften der Einsender jeweils zueinandergehörende Fragebögen herauszufinden, der Datennutzung nicht entgegen.

Nachdem mein Verlangen, Teile des Anschreibens des Forschungsinstitutes an die Eltern so zu verbessern, dass die Entstehung irriger Annahmen über das Vorgehen des Forschungsinstituts vermieden wurde, erfolgreich gewesen war, musste ich nur noch gegenüber der Justiz darauf dringen, dass die Angeschriebenen zusätzlich auch von der adressmittelnden Stelle selbst, also dem jeweiligen Familiengericht, ein Anschreiben erhielten, aus dem hervorging, dass

- keine Datenübermittlung, sondern eine bloße Nutzung stattgefunden habe, dass ferner
- keinerlei Pflicht zur Teilnahme bestehe und dass
- insbesondere das Familiengericht sich nicht darum kümmere und gar nichts davon erfahre, wer teilnimmt, sowie dass
- die Teilnahme an der Studie jederzeit abgebrochen werden könne.

Dabei musste ich verlangen, dass das Anschreiben der Familiengerichte den jeweiligen üblichen Briefkopf des Gerichtes trug - damit nicht bei den Adressaten der Eindruck erweckt werden konnte, es handele sich nicht um eine nicht uneingeschränkt amtliche, ordnungsgemäße Verfahrensweise des Absenders.
Der geringfügige Mehraufwand scheint sich, wie ich vorhergesagt habe, gelohnt zu haben. Zumindest in meiner Dienststelle ist keine Anfrage von einer der geschätzt immerhin 4.800 betroffenen Scheidungsparteien eingegangen.

Vgl. zu diesem Vorgang auch oben unter 5.7.2.

13.2 Datenübermittlung zu Forschungszwecken an Hochschulen oder an Hochschulen Tätige nach allgemeinem Datenschutzrecht

Richtet sich die Datenübermittlung nach dem Sächsischen Datenschutzgesetz statt nach bereichsspezifischen Vorschriften, sind, namentlich im Falle von Dissertationsvorhaben, Voraussetzungen zu prüfen, auf die man leider auch Juristen aufmerksam machen muss.

Zunächst ist, wie schon 7/5.8.4 ausgeführt, entscheidend, ob der Übermittlungsempfänger eine bestimmte Person (z. B. der Doktorand) oder aber die Hochschul-Institution sein soll. In der Regel haben sich die Beteiligten allerdings darüber noch keine Gedanken gemacht, wenn sie sich an mich oder an die Behörde wenden, von der sie personenbezogene Daten wollen (und die sich dann an mich wendet) - jedenfalls äußern sie sich dazu nicht näher.
Sollen die Daten an den Interessenten als Privatperson (Individuum) gehen, bestimmt sich die Erlaubtheit einer Datenübermittlung nach § 15 SächsDSG, mit allen damit verbundenen Hindernissen (vgl. dazu 3/10.3.2).
Im anderen Fall, der sich nach § 13 SächsDSG richtet, muss, über die einschlägigen Ausführungen von 7/5.8.4 hinaus, auf Folgendes geachtet werden:

Zum einen muss gemäß Nr. 1 der genannten Vorschrift die Übermittlung (richtiger: die Kenntnis der zu übermittelnden Daten) *erforderlich* sein für die Aufgabenerfüllung auf Empfängerseite. Übermittlungsempfänger ist die betreffende forschungbetreibende Organisationseinheit, z. B. der „Lehrstuhl“. Dort müssen die Daten zur Aufgabenerfüllung benötigt werden. Wegen § 13 Abs. 1 Nr. 2 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG kommt von den verschiedenen gesetzlich vorgegebenen Aufgaben der Hochschule und ihrer Organisationseinheiten nur die Aufgabe „Durchführung von Forschungsaufgaben“ in Frage. Gemeint ist dabei die sozusagen ‘eigenhändige’ Durchführung von Forschungsaufgaben: Die datenempfangende Hochschulein-

richtung muss, ggf. im Verbund mit anderen Stellen, die Forschung in eigener Regie betreiben; ihr dürfen personenbezogene Daten nicht als bloßer Daten-Durchgangs-Station, also zugunsten anderer Hochschuleinrichtungen oder sonstiger Forschungseinrichtungen, übermittelt werden; sie darf also nicht Daten für einen von vornherein ausschließlich fremden Forschungsbedarf übermittelt bekommen. Denn dies widerspräche dem im Wortlaut der Vorschrift zum Ausdruck kommenden Verhältnismäßigkeitsgrundsatz: Die Daten würden jemandem übermittelt, der sie selbst gar nicht benötigt.
Besteht die Datenübermittlung von der Behörde an die Hochschul-Einrichtung darin, dass die Behörde Einsicht in bei ihr vorhandene Unterlagen gewährt, muss die Behörde sich die nötige Gewissheit (vgl. § 13 Abs. 2 Satz 3 SächsDSG) verschaffen, dass die betreffende forschungstreibende Organisationseinheit der Hochschule die Daten für ein *von ihr durchgeführtes Forschungsvorhaben* benötigt und dass während der gesamten Zeit der Einsichtnahme in Behörden-Unterlagen das Dienstverhältnis der einsichtnehmenden Personen innerhalb der betreffenden datenempfangenden (und forschungstreibenden) Organisationseinheit der Hochschule fortbesteht. Das Dienstverhältnis ist vom Doktoranden-Status zu unterscheiden. Dieser ersetzt das Dienstverhältnis nicht, d. h. ist keine hinreichende Grundlage dafür, dass der Doktorand die Daten lediglich in einer der sachenrechtlichen Stellung des Besitzdieners oder des Besitzmittlers entsprechenden Funktion für die forschungtreibende Organisationseinheit verarbeitet.

Hinsichtlich dieser Voraussetzungen (Eigenbedarf und Dienstverhältnis) muss sich die Behörde, welche die personenbezogenen Daten zur Verfügung stellen soll, die nötige Gewissheit verschaffen, und zwar unabhängig von der Frage, inwieweit die Erleichterung des § 13 Abs. 2 Satz 2 SächsDSG gerade für diese Fallgruppe passt (vgl. dazu 6/5.8.4, zum 5. Spiegelstrich).

Die *weitere*, oft zunächst übersehene Voraussetzung ist, dass hochschulseits zu verantwortende Angaben gemacht werden, die es ermöglichen, zu beurteilen, ob die Bedeutung des wissenschaftlichen Vorhabens ein Allgemeininteresse begründet, welches den mit der Datenübermittlung verbundenen Eingriff in das Grundrecht auf informationelle Selbstbestimmung mit der nach dem Gesetz nötigen Eindeutigkeit überwiegt. Dies Überwiegen zu beurteilen ist dann, zumindest im Rahmen des § 13 Abs. 2 Satz 3 SächsDSG, Sache der betreffenden Behörde.
Bei Doktoranden ist manchmal schon die Themenangabe zu unbestimmt, um auch nur eine Vorstellung von den Fragestellungen der Arbeit zu bekommen (handelt es sich um juristische Themen, fällt dies auch den für die Beurteilung zuständigen Juristen auf; vgl. 7/13.2). Auch auf eine Angabe darüber, welche Arten von Unterlagen - wenn man so will: welche Datensätze genau - ausgewertet werden sollen, muss oft erst noch gedrungen werden. Und pauschale Angaben über einen „Zusammenhang“ mit einem mit beträchtlichen öffentlichen Geldmitteln geförderten Forschungsvorhaben bieten die notwendige Beurteilungsgrundlage noch nicht.

Solche hinreichenden Darlegungen zum Forschungsvorhaben, die seitens der datenempfangenden forschungtreibenden Stelle zu verantworten sind, sind im Übrigen auch dann Voraussetzung, wenn die erforderliche Abwägung nicht nach § 13 Abs. 1

Nr. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG, sondern nach bereichsspezifischen Übermittlungsvoraussetzungen (einschließlich Archivrecht: § 10 Abs. 4 Satz 2, 1. Halbsatz SächsArchivG) stattfindet.

13.3 Forschungsvorhaben zum Wandel der kommunalen Eliten in Sachsen 1990 bis 2000

Unter der vollständigen Bezeichnung „Kommunales Führungspersonal in Thüringen und Sachsen: Rekrutierung, Austausch, Orientierungen 1990-2000“ führt die TU Dresden, zusammen mit der Universität Jena für Thüringen, bezogen auf 107 repräsentativ ausgewählte Städte und Gemeinden Sachsens eine Untersuchung durch. Aufmerksame Kommunalverwaltungen, große wie kleine, haben deshalb bei mir angefragt. Ich war frühzeitig seitens der Forscher um Beratung gebeten worden. Diese konnten sich zu Recht darauf berufen, dass ihre Datenwünsche an die Verwaltung mit mir abgestimmt seien.
Im Einzelnen geht es vor allem um folgende Übermittlung personenbezogener Daten von Kommunalpolitikern durch sächsische Gemeindeverwaltungen:

(1) Die gewünschte Übermittlung der Namen, Amtsbezeichnungen und Zuständigkeitsbereiche sowie Amtszeiten der Bürgermeister, Beigeordneten sowie der Ratsmitglieder ist gemäß § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 2 SächsDSG zulässig: Diese Daten lassen sich allgemein zugänglichen Quellen entnehmen, es handelt sich um amtsausübungsbezogene Daten.
(2) Die Übermittlung der zugelassenen Wahlvorschläge ist wegen deren öffentlicher Bekanntmachung (§ 6 Abs. 8, § 41 Abs. 9 KomWG, § 21 KomWO) gemäß § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 2 SächsDSG zulässig. Zum Datensatz gehört auch die Anschrift der Bewerber (§ 16 Abs. 1 Satz 2 Nr. 2 KomWO).
Insoweit die Wahlvorschläge zwar eingereicht, jedoch nicht zugelassen worden sind und damit auch nicht veröffentlicht wurden, sind die Voraussetzungen des § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 4 SächsDSG erfüllt: Die Betreffenden haben sich auf die öffentliche politische Bühne begeben; das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens überwiegt deshalb dasjenige des Betroffenen am Unterbleiben der Zweckänderung erheblich. (Das müssten notfalls die Gerichte entscheiden; für die von mir zu treffende Beurteilung war ausschlaggebend: Die wissenschaftliche Wichtigkeit des Themas leuchtete ein; die Darstellung der Untersuchung in einem an die Deutsche Forschungsgemeinschaft gerichteten Antrag war für den mit dem Wissenschaftsbetrieb nicht unvertrauten politologischen Laien ausgesprochen eindrucksvoll, vgl. zu dieser Problematik 7/13.2.)
(3) Die Kommunalwahlergebnisse sind ebenso wie die zugelassenen Wahlvorschläge personenbezogen „öffentlich bekanntzumachen“ (gewesen), § 24 Abs. 2 Satz 1 KomWG, § 51 Abs. 1 und 2 KomWO; folglich ist die Datenübermittlung insoweit wiederum auf § 13 Abs. 1 i. V. m. § 12 Abs. 2 Nr. 2 SächsDSG zu stützen.
Auch hier gehört zum Datensatz die Anschrift.
(4) Das Übermittlungsersuchen ist jeweils an die Gemeinde in ihrer Eigenschaft als Kommunalwahlbehörde gerichtet, also als diejenige Stelle, die das Kommunalwahlgesetz ausführt. Aus den in diesem Amt vorhandenen Unterlagen darf die Gemeinde die Anfrage beantworten.

Etwas anderes wäre es, wenn sich später die TU Dresden wegen veränderter Anschriften an dieselbe Gemeinde in deren Eigenschaft als Meldebehörde wenden sollte. Dann bestimmte ausschließlich das Sächsische Meldegesetz, unter welchen Voraussetzungen eine Melderegisterauskunft zu erteilen ist.
(5) Zur Studie im Übrigen: Die einzusetzenden studentischen Hilfskräfte werden förmlich nach dem strafrechtlichen Verpflichtungsgesetz verpflichtet. Bei einer über die oben genannten Listen hinausgehenden Datenerhebung sind gemäß § 30 Abs. 3 SächsDSG die unmittelbar identifizierenden Merkmale (Name, Anschrift) getrennt zu speichern.
Es wird nicht personenbezogen veröffentlicht.
Es sollte weder der Eindruck erweckt noch die Meinung ausgenutzt werden, dass die ehemaligen oder jetzigen Amtsträger etwa Kraft ihres Amtes verpflichtet sein könnten, den Forschern in einem Interview Auskunft zu erteilen.

13.4 Gedenkstätte eines Bergbaumuseums

Der Förderverein des Knappenroder Bergbaumuseums hat wissen wollen, ob das Museum in einer Gedenkstätte die Namen von Bergleuten, die seit 1920 im Lausitzer Bergbaugebiet tödliche Arbeitsunfälle erlitten haben, mitsamt dem Geburts- und Todesjahr sowie dem Namen der Grube (Betriebsstätte) anbringen dürfe. Es handelt sich um rund 740 Männer.

Zuständig für die Beantwortung, also für die Beratung des Vereins, war ich deswegen, weil Träger des Museums die Stadt Knappenrode war, die dem Verein zum Teil den Betrieb des Museums übertragen hatte. Es handelt sich also beim Betreiben des Museums um eine Tätigkeit eines Trägers öffentlicher Gewalt auf dem Gebiet der Kulturpflege, mit der Folge, dass der Verein insoweit Aufgaben der öffentlichen Verwaltung wahrnimmt und somit öffentliche Stelle im Sinne von § 2 Abs. 2 Satz 1 SächsDSG ist.

Zulässig war das Vorhaben, weil in das Grundrecht auf informationelle Selbstbestimmung nicht eingegriffen wurde. Und das verfassungsrechtliche Persönlichkeitsrecht, insoweit es nach dem Tode datenschutzähnliche Wirkung hat, war nicht berührt.

Denn der Datenschutz endet - von gesetzlichen Ausnahmen abgesehen - grundsätzlich mit dem Tode des betroffenen Menschen. Ein Verstorbener wird allerdings durch das verfassungsrechtliche Persönlichkeitsrecht *insoweit* geschützt, als es sich aus Art. 1 Abs. 1 GG (Unantastbarkeit der Würde des Menschen) herleiten lässt. Hält man sich hinsichtlich der dabei zu beachtenden zeitlichen Grenzen, mangels zuverlässigerer Anhaltspunkte, an die Schutzfristen des sächsischen Archivrechtes, so kommt ein Persönlichkeitsrechtsschutz ohnehin nur für die in den letzten zehn Jahren tödlich Verunglückten in Frage. Deren Daten werden dem Besucher ohnehin häufig bekannt oder noch in Erinnerung sein.

Aus der Lektüre der Gedenkstätten-Daten zu einer Person, von der er - wenn überhaupt - eine konkrete, identifizierende Vorstellung hat, erfährt der Besucher der Gedenkstätte, dass der Träger eines bestimmten Namens in einem bestimmten Jahr

und in einem bestimmten Alter als Beschäftigter in einer Grube tödlich verunglückt ist. Diese Daten sind nicht geeignet, das Persönlichkeitsrecht zu stören oder sonst zu tangieren, vielmehr stärken sie die Würde des Betroffenen. Denn das ehrende Andenken auf Ehrenmalen, Grabsteinen, Krieger-Gedächtnisstätten und anderen Denkmalen ist eine herkömmliche und würdevolle Form der Daten-Veröffentlichung, die das Persönlichkeitsrecht immer dann wahrt und stärkt, wenn nach allgemeiner Auffassung mit der Veröffentlichung kein Makel verbunden ist. Diese Mahnungen zur Erinnerung, zum Innehalten oder auch zum Gebet geben Zeugnis vom persönlichen Schicksal der Verstorbenen. Von einem Eingriff in deren Persönlichkeitsrecht kann vorliegend keine Rede sein.

Anders wäre ein Fall zu beurteilen, in dem solche Informationen über Verstorbene veröffentlicht werden, die ihnen abträglich wirken oder wirken können, z. B. über „Aktivisten der ersten Stunde“ oder über „nationalsozialistische Helden“, vielleicht aber auch über „Wirtschaftskapitäne“, die später als Umweltsünder gelten. Es kommt also auf den konkreten Inhalt der Gedenk-Nachricht an; wirkt sie negativ, darf die Veröffentlichung nur mit Einwilligung der Hinterbliebenen stattfinden.

14 Technischer und organisatorischer Datenschutz

14.1 Telemedizin

Bereits im letzten Jahr berichtete ich über das vom SMS initiierte Modellprogramm zur „Digitalisierung bildgebender Verfahren und Bildkommunikation der Krankenhäuser im Freistaat Sachsen“. Es geht um den Aufbau einer funktionierenden internen und externen Bildkommunikation. Aspekte sind dabei die Erprobung von Hard- und Software u. a. zur internen und externen Vernetzung bzw. Bildkommunikation, zur Nutzung digitaler Archivierung, zur Befundung, die Erstellung und Anwendung von Standards für die digitale Bildübertragung sowie die Einbeziehung der Aufnahmeplätze und Funktionsstellen in die digitale Bildkommunikation und Archivierung.

Im Berichtszeitraum wurden die Konzeption und die Vertragspartner der Modellprojekte im wissenschaftlichen Beirat des Projektes, dem ich angehöre, vorgestellt, intensiv begutachtet und bewertet. Von ursprünglich acht regionalen Modellprojekten wurden sieben in die Förderung aufgenommen: Sie erhalten insgesamt 26 Mio. DM Fördermittel. Derzeit laufen die Vertragsabschlüsse mit den Generalunternehmern für die einzelnen Projekte.

Hat der wissenschaftliche Beirat in seiner ersten Phase stark gestaltend in die Projekte eingegriffen, wird sich seine Arbeit jetzt stärker auf die Begleitung und Evaluierung der Projekte - u. a. auch bei den beiden folgenden Schwerpunkten - verlagern.

Datenschutzkonzept
In der telemedizinischen Zusammenarbeit werden z. T. hochsensible Gesundheits- und Behandlungsdaten übermittelt. Deshalb gehört zu den Aufgaben des wissen-

schaftlichen Beirates - neben der Erstellung eines Evaluierungskonzeptes - die Erarbeitung eines Datenschutz- und Datensicherheitskonzeptes unter meiner Begleitung. Ziel dieser Arbeit ist es, den Projekten bei der Vertragsgestaltung mit den Generalunternehmern Hilfestellung zu geben, damit Aspekte der Datensicherheit und des Datenschutzes angemessen berücksichtigt werden. Darüber hinaus könnte mit Hilfe der Erfahrungen im Modellprogramm ein allgemeiner Leitfaden zu dieser Thematik entstehen. Die „Empfehlungen für ein Sicherheits- und Datenschutzkonzept“ wurden in dieser Form am 24. März 2000 vom wissenschaftlichen Beirat akzeptiert.

Die Empfehlungen gehen ausführlich auf die rechtliche Situation im Rahmen des Modellprogramms ein (Rahmenbedingungen durch Datenschutzrecht, Zivilrecht und Schadensersatzrisiken, Rechtmäßigkeit digitaler Verfahren, Beweisqualität digitaler Dokumente). In einem zweiten Teil werden Vorschläge für Maßnahmen anhand der Kriterien *Vertraulichkeit* (u. a. Datenzugriff, Zugriff im Notfall, Datenübertragung und Fernwartung), *Integrität* (u. a. Integrität der Patientendaten, Einheit von Bild und Befund, Datenübertragung), *Verfügbarkeit* (u. a. Zuverlässigkeit und Ausfallsicherheit), *Authentizität*, *Revisionsfähigkeit* (u. a. Dokumentationspflicht und Protokollierung) sowie *Transparenz* gemacht. Ergänzungen hinsichtlich der externen Archivierung und der Einführung der Health Professional Card (HPC als „Zugangsschlüssel“) werden noch erarbeitet.

Elektronischer Arztausweis – Health Professional Card (HPC)
Bei der Verwirklichung des Modellprogramms spielen Kommunikation und elektronischer Austausch von Patientendaten eine wichtige Rolle. Von daher stellt sich sofort die Frage nach der technischen Realisierung der hohen Datenschutzanforderungen. Wie gewährleiste ich u. a. die Identitätsfeststellung der Kommunikationspartner, die Vertraulichkeit der Kommunikation über Netze, den sicheren Austausch von Patienten- und Befunddaten zwischen verschiedenen Anwendungssystemen und - was besonders schwierig ist - die Beweissicherheit, z. B. durch eine digitale Signatur?

Bundesweit ist dafür die Einführung eines elektronischen Arztausweises (als erste Stufe einer HPC und modellhaft für alle Teilnehmer im Gesundheitswesen) im Gespräch. Er soll als Kombination von Sichtausweis und Chipkarte folgende Funktionen erfüllen:
- Identifikation/Authentifikation (mit Angaben zur Person, zur Rolle als Arzt und zur Kammerzugehörigkeit)
- Verschlüsselung von Transportdaten (asymmetrisch/symmetrisch)
- Digitale Signatur (Signatur-Gesetz konform)
- Zusatzfunktionen (z. B. Weiterbildungszertifikate, Zusatzqualifikationen, Pseudonym, etc.)

Seit Juli 1999 liegt die erste Version der Spezifikationen für die deutsche HPC vor. Auf der Basis dieser Spezifikationen sollen nun sowohl erste Prototypen von elektronischen Arztausweisen erstellt werden als auch in den Bereichen einiger Landesärztekammern im Laufe des Jahres 2000 erste Pilotanwendungen gestartet werden. Genaue Angaben zu Inhalten und Anwendungen liegen von den Pilotprojekten allerdings

derzeit nicht vor. Mit Ergebnissen aus diesen Projekten ist während der Laufzeit des sächsischen Modellprogramms nicht zu rechnen.

Neben den technischen und inhaltlichen Spezifikationen stehen derzeit die infrastrukturellen Fragen im Vordergrund. Die Vorbereitungen zur Einrichtung einer anerkannten Zertifizierungsinstanz bzw. zum Einkauf entsprechender Dienstleistungen sind aufgenommen worden. Grundsätzlich ist klar, dass die Landesärztekammern (wie bisher bei Führung des Berufsregisters und Ausgabe des konventionellen Arztausweises) die Anlaufstelle zur Antragstellung, Identifizierung, Prüfung der Berechtigung, Registrierung und Ausgabe des elektronischen Arztausweises sein werden. Zur Erfüllung aller weiteren Aufgaben wie technische Prüfung, Schlüsselgenerierung, Personalisierung, Zertifizierung und Herstellung des Ausweises werden sich die Kammern dann eines oder mehrerer technischer Dienstleister (Trusted Third Party Services) bedienen.

Bei den sächsischen zuständigen Stellen (u.a. auch der Landesärztekammer) besteht ein hohes Interesse an der Einbeziehung der HPC in das Modellprogramm. Eine Nachfrage hinsichtlich des elektronischen Arztausweises ist in Sachsen vorhanden. Ich unterstütze dies und sähe bei einem frühzeitigen Einsatz der HPC innerhalb des Modellprogramms positive Auswirkungen (Nutzung einer standardisierten Verschlüsselung, Innovation und Schaffung von De-facto-Standards, Sammeln von Erfahrungen usw.). Allerdings steht dem der hohe organisatorische und finanzielle Aufwand, eine in der gegebenen Zeit des Modellprogramms fragwürdige technische Realisierung und die schwierige praktische Umsetzbarkeit der derzeitig hohen Anforderungen des Signaturgesetzes entgegen. Ich habe deshalb nicht auf einen generellen Einsatz der HPC im Modellprogramm bestanden, fände es allerdings begrüßenswert, wenn innerhalb einzelner Projekte Lösungen zum Einsatz kämen, die in die Richtung der HPC gingen. Ich halte vor allem die Erfahrungen bei den oft unterschätzten organisatorischen Problemen für interessant. Um sich die Dimension klar zu machen, stelle man sich vor, man sei innerhalb eines Krankenhaus mit mehreren hundert Ärzten und medizinischen Mitarbeitern mit unterschiedlichen Tätigkeitsbereichen, Versetzungen, Personalfluktuation und zusätzlich noch verschiedener Technik und Anwendungen verantwortlich für die Ausgabe und Aktualisierung einer Health Professional Card.

Mehrere Generalunternehmer haben ihre grundsätzliche Bereitschaft erklärt, an einer Einführung der HPC mitzuwirken; in einigen Modellprojekten werden von den Verantwortlichen zumindest Lösungen in dieser Richtung erwogen. Ich werde dies mit besonderem Interesse beobachten und begleiten.

14.2 Verarbeitung und Übermittlung personenbezogener Daten bei IT-Sicherheitskontrollen

IT-Sicherheit wird neben der Berücksichtigung sicherheitstechnischer und –organisatorischer Aspekte in der Verfahrensvorbereitung auch durch die Kontrolle laufender Verfahren gewährleistet. Dabei werden regelmäßig personenbezogene Daten zur

Kenntnis genommen, so dass in diesen Fällen Datenschutzrecht berücksichtigt werden muss.

1. Erheben und Verarbeiten personenbezogener Daten

Bei der Kontrolle von DV-Verfahren und -einrichtungen können drei Fallkonstellationen mit unterschiedlicher rechtlicher Bewertung auftreten, bei den personenbezogene Daten zur Kenntnis genommen werden:

- das DV-System protokolliert Nutzerdaten. Diese werden im Rahmen der Kontrolle ausgewertet;
- der Kontrolleur muss im Rahmen seiner Kontrolle inhaltliche personenbezogene Daten zur Kenntnis nehmen (z. B. bei der Kontrolle eventueller Veränderungen von Daten in Personalinformationssystemen);
- der Kontrolleur stößt im Rahmen der Kontrolle zufällig auf personenbezogene inhaltliche Daten (z. B. Personalschreiben des Betroffenen auf seiner lokalen Festplatte).

1.1 Auswertung von Protokolldaten

DV-Systeme protokollieren in der Regel Nutzeraktivitäten. Diese Protokolldaten sind personenbeziehbar, in der Regel automatisiert erstellt und auswertbar. Der Umgang mit ihnen unterliegt damit dem Datenschutzrecht. Hinzu kommt, sofern die Nutzer Bedienstete sind, dass Personalrecht ebenfalls einschlägig ist.

Das Erheben von Protokolldaten bei DV-Systemen ist nach § 11 Abs. 1 SächsDSG zulässig, da es zur Erfüllung der Aufgaben der speichernden Stelle dient, in diesem Falle der Gewährleistung des Funktionierens der zur Aufgabenerfüllung notwendigen DV-Systeme. Allerdings gibt § 12 Abs. 4 eine klare Zweckbindung vor: „Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diesen Zweck und hiermit im Zusammenhang stehende Maßnahmen gegenüber Bediensteten genutzt werden."

Spezialregeln existieren im Telekommunikationsbereich. Für Telekommunikationsdienste ist das Telekommunikationsgesetz (TKG) sowie die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) einschlägig, für Teledienste (z. B. die Bereitstellung von Internetzugängen) gilt das Teledienstedatenschutzgesetz (TDDSG), für Mediendienste (öffentlich zugängliche, an die Allgemeinheit gerichtete Angebote) der Mediendienste-Staatsvertrag, für Angebote mit redaktionellem Gehalt der Dritte Rundfunkänderungsstaatsvertrag. Hier gelten dem Sächsischen Datenschutzgesetz vergleichbare strenge Zweckbindungsregelungen, allerdings mit spezifizierten Speicherfristen. Für IT-Sicherheitskontrollen in der öffentlichen Verwaltung sind diese Regelungen in der Regel nicht relevant, solange die Internet- oder E-Mail-Nutzung nicht in den Kontrollbereich einbezogen ist.

Nach § 80 Abs. 3 Nr. 16 SächsPersVG hat die Personalvertretung mitzubestimmen bei „Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen". Nach der Recht-

sprechung des Bundesverwaltungsgerichts bezieht sich das Mitbestimmungsrecht auch auf technische Einrichtungen, die zur Überwachung „geeignet“ sind, selbst wenn ihr Einsatz dazu nicht vorgesehen ist. Die Erhebung von Protokolldaten in DV-Systemen fällt unter diesen Passus.

1.2 beabsichtigte Kenntnisnahme personenbezogener inhaltlicher Daten
Bei einer IT-Sicherheitskontrolle kann es notwendig sein, dass der Kontrolleur z. B. bei Veränderungen in personalverarbeitenden Systemen auch personenbezogene Daten überprüfen muss. Dies ist kein Erheben im Sinne des Sächsischen Datenschutzgesetzes, da die personenbezogenen Daten bereits in anderem Zusammenhang erhoben worden sind.

Auch eine Speicherung, Veränderung oder Nutzung für andere Zwecke, die nach § 12 Abs. 2 SächsDSG an enge Bestimmungen gebunden ist, liegt nicht vor, denn § 12 Abs. 3 SächsDSG stellt ausdrücklich fest:

„Eine Speicherung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung sowie statistischen Zwecken der speichernden Stelle dient.“

Damit ist für diese Daten § 12 Abs. 1 SächsDSG einschlägig, der die Nutzung von personenbezogenen Daten erlaubt, wenn ihre Verarbeitung „zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist“. Dies ist bei einer IT-Sicherheitskontrolle der Fall.

1.3 Zufällige Kenntnisnahme personenbezogener inhaltlicher Daten
Sollte es im Rahmen der Kontrolle vorkommen, dass der Kontrolleur zufällig auf personenbezogene Daten stößt, die nicht originär mit dem Kontrollzweck zu tun haben, so ist dies ebenfalls keine Erhebung, da die Erhebung einen bewussten Entschluss voraussetzt. Allerdings fällt der weitere Umgang mit diesen Daten unter das Sächsische Datenschutzgesetz. Sind diese Daten für die Aufgabenerfüllung des Kontrolleurs von Bedeutung (Gewährleistung der IT-Sicherheit), so kann er sie nach § 11 Abs. 1 SächsDSG i. V. m. § 9 SächsDSG nutzen. Das unter 1.2 Geschriebene gilt in diesem Fall. Sollten die personenbezogenen Daten nicht mit seiner Aufgabenerfüllung zu tun haben, ist eine weitere Nutzung der Daten für andere Zwecke untersagt, sofern nicht bestimmte, eng begrenzte Voraussetzungen vorliegen (siehe unten Nr. 2).

2. Nutzung für andere Zwecke und Übermittlung
Eine Nutzung für andere Zwecke im Sinne des Sächsischen Datenschutzgesetzes liegt vor, wenn personenbezogene Daten für andere Zwecke innerhalb der Dienststelle genutzt werden; bei der Übermittlung werden die Daten an eine andere öffentliche oder nicht-öffentliche Stelle für gleiche oder andere Zwecke weitergegeben.

Die Übermittlung von personenbezogenen Daten, die im Rahmen einer Sicherheitskontrolle verarbeitet worden sind, an eine *andere* öffentliche Stelle ist zulässig, wenn

sie immer noch mit dieser Sicherheitskontrolle verbunden ist (z. B. die Übermittlung von Protokolldaten im Abschlussbericht an die vorgesetzte Dienststelle). Die Zweckbindung der Daten besteht weiter und ist auch von der anderen Dienststelle zu beachten.

Die Nutzung bzw. die Übermittlung an andere öffentliche Dienststellen für andere Zwecke ist zu differenzieren. Personenbezogene Daten, die unter § 12 Abs. 4 SächsDSG fallen (in der Regel Protokolldaten) dürfen nicht für andere Zwecke genutzt werden, es sei denn, es gäbe eine spezialgesetzliche Grundlage (z. B. § 43 Abs. 1 a SächsPolG). Andere personenbezogene Daten, die zufällig bekannt werden, dürfen nur unter eng begrenzten Voraussetzungen gespeichert und für andere Zwecke genutzt werden. § 12 Abs. 2 SächsDSG nennt einen Katalog von Tatbeständen. Für IT-Sicherheitskontrollen dürfte in der Regel nur die Nr. 3 in Betracht kommen: Wenn

„es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist ...“.

Hat der Kontrolleur Anhaltspunkte für solche Fälle, sollte er stets mit dem Dienstvorgesetzten bzw. dem behördlichen Datenschutzbeauftragten Kontakt aufnehmen und die Voraussetzungen für die Übermittlung prüfen lassen.

14.3 Digitale Signaturen

Behörden und öffentliche Stellen setzen beim elektronischen Schriftverkehr zunehmend digitale Signaturen ein. Deshalb möchte ich mit diesem Beitrag zukünftige Anwender über digitale Signaturen informieren und sie zugleich für einen sicheren Umgang mit der neuen Technologie sensibilisieren.

Eine digitale Signatur soll die Integrität (Unversehrtheit) und Authentizität (Nichtabstreitbarkeit) elektronischer Daten nachweisen. Mit Hilfe der digitalen Signatur soll eindeutig festgestellt und überprüft werden können, ob eine Datei (Dokument, Nachricht) zweifelsfrei vom angegebenen Absender stammt und ob die Daten unverfälscht den Empfänger erreicht haben. Die digitale Signatur soll der eigenhändigen Unterschrift beim Papierdokument gleichwertig sein.

Digitale Signaturen werden auf der Basis kryptographischer Verfahren erstellt. Dabei werden Hashfunktionen mit asymmetrischen Verschlüsselungsverfahren (s. 6/14.2) kombiniert, um den Nachweis von Integrität und Authentizität zu erbringen.
Eine *Hashfunktion* ist ein Algorithmus, der eine Datei beliebiger Länge auf einen *Hashwert* (Quer-, Prüfsumme) fester kurzer Länge abbildet. Dazu werden ausschließlich Einweg-Hashfunktionen genutzt. Sie gewährleisten, dass es mit vertretbarem Aufwand nicht möglich ist, zu einem vorgegebenen Hashwert die dazugehörige Datei zu finden. Außerdem soll es nicht möglich sein, zwei Dateien mit demselben Hashwert zu finden.

1. Rechtliche Voraussetzungen für digitale Signaturen

Vor einem Einsatz kryptographischer Verfahren für digitale Signaturen sind zunächst die gesetzlichen Rahmenbedingungen zu prüfen. In Art. 3 Signaturgesetz (SigG) werden grundsätzliche technische und organisatorische Anforderungen für eine Sicherheitsinfrastruktur für digitale Signaturen geregelt. Zusätzlich sind Details in der Signaturverordnung (SigV).

Die Anwendung anderer Verfahren für digitale Signaturen ist gemäß § 1 Abs. 2 SigG freigestellt, soweit nicht digitale Signaturen nach diesem Gesetz durch Rechtsvorschrift vorgeschrieben sind.

2. Technische Realisierung digitaler Signierung

Damit eine Datei mit einer digitalen Signatur versehen werden kann, müssen folgende technische Voraussetzungen erfüllt sein:

- Die Infrastruktur der Anwender muss spezielle Hard- und Software für digitale Signaturen bereitstellen.
- Erzeugung und Prüfung digitaler Signaturen dürfen nur auf Veranlassung und ausdrückliche Einwilligung der Anwender durchgeführt werden.
- Es darf nicht möglich sein, dass ein Anwender durch Täuschung oder technische Manipulation eine andere Datei signieren oder prüfen könnte, als er signieren oder prüfen wollte oder zu signieren oder zu prüfen glaubte.
- Für die Nutzung asymmetrischer Verschlüsselungsverfahren müssen öffentliche und geheime Schlüssel in einer „sicheren Umgebung“ erzeugt werden. Außerdem sollen die technischen Komponenten so beschaffen sein, dass der geheime Schlüssel (Signaturschlüssel) mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommt und aus dem öffentlichen Schlüssel nicht der geheime Schlüssel errechnet werden kann. Überdies ist der Signaturschlüssel besonders gesichert (z. B. in einer Chipkarte) zu speichern. Der öffentliche Schlüssel (Verifizierschlüssel) ist mit Angaben des Inhabers fälschungssicher von einer Zertifizierungsstelle zu veröffentlichen.
- Die Zertifizierungsstelle bearbeitet Anträge für Zertifikate und bescheinigt die Zuordnung öffentlicher Schlüssel zu einer natürlichen Person mit einer digitalen Signatur. Das Zertifikat enthält auch Angaben über seine Gültigkeit, d. h. Beginn und Ende.

Die digitale Signatur wird wie folgt realisiert:

Von der Datei wird beim Absender ein „Hashwert“ gebildet.

- Der Hashwert wird mit dem Signaturschlüssel des Absenders verschlüsselt und im Auftrag zusammen mit dem Zertifikat an die Datei angefügt.
- Die Datei wird mit diesem Anhang an den Empfänger übermittelt.
- Der Empfänger überprüft die Gültigkeit des Zertifikates.
- Der Empfänger berechnet aus der empfangenen Datei einen „eigenen“ Hashwert.
- Der verschlüsselten Hashwert im Anhang der Datei wird mit dem Verifizierschlüssel des Absenders entschlüsselt.
- Der entschlüsselte und der eigene Hashwert werden verglichen. Sind beide Hashwerte identisch, so ist sichergestellt, dass die Datei während der Übermittlung nicht verändert wurde und vom angegebenen Absender stammt. Jede noch so kleine

Änderung der digitalen Signatur oder der Datei würde eine Differenz zwischen den Hashwerten ergeben und die Datei als gefälscht ablehnen.

3. Zur Sicherheit digitaler Signaturen

Die Sicherheit digitaler Signaturen ist in erster Line von den Eigenschaften der eingesetzten Kryptoalgorithmen und von der Geheimhaltung des Signaturschlüssels abhängig. Ohne Kenntnis des geheimen Signaturschlüssels des Absenders ist keine Fälschung der Datei oder der Signatur möglich. Deshalb muss unbedingt durch technische und organisatorische Maßnahmen Diebstahl, Verlust und Preisgabe des Signaturschlüssels verhindert werden.

Um kryptographischer Algorithmen einschließlich ihrer Parameter bewerten zu können, prüfen jährlich Experten aus Wissenschaft, Wirtschaft und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) deren Eignung.
Gemäß § 17 Abs. 2 SigV veröffentlicht die Regulierungsbehörde für Telekommunikation und Post eine Zusammenstellung über Algorithmen und dazugehörige Parameter, die zur Erzeugung von Signaturschlüsseln, zum „Hashen“ zu signierender Daten oder zur Erzeugung und Prüfung digitaler Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt.
Im Bundesanzeiger (vom 11. November 1999 Nr. 213 S. 18.638) veröffentlichte die Regulierungsbehörde folgende Kryptoalgorithmen für die nächsten sechs Jahre, d. h. hier bis Ende 2004:

Vorschläge für geeignete Hashfunktionen sind:
160 Bit Hashfunktionen der MD4- Familie
SHA-1 und
RIPEMD-160.

Vorschläge für geeignete Signaturalgorithmen sind:
RSA mit einer Schlüssellänge von mindestens 1024 Bit (bis Ende 2000 reicht eine Minimallänge von 768 Bit aus),
DSA (Digital Signature Algorithm) mit einer Schlüssellänge von mindestens 1024 Bit
oder auf elliptischen Kurven basierende *DSA-Varianten*, die festgelegte Standards der Veröffentlichung realisieren.

Die Zertifizierungsstellen können abweichend von den hier vorgeschlagenen Algorithmen auch andere Verfahren einsetzen, wenn deren Eignung vom BSI festgestellt wird.

Nachfolgend sind die wichtigsten Sicherheitsanforderungen beim Einsatz digitaler Signaturen zusammen gefasst:

- Installation und Betrieb des Signatur-Verfahrens dürfen nicht manipulierbar sein.
- Es sind sichere kryptographische Algorithmen und ausreichende Schlüssellängen einzusetzen.
- Das Schlüsselmanagement muss folgenden Anforderungen genügen:
  - Die zentrale oder dezentrale Schlüsselerzeugung muss durch geeignete Schlüsselgeneratoren in besonders gesichertem Bereich erfolgen.

- Die Preisgabe von Signaturschlüssel und Identifikationsdaten muss ausgeschlossen werden.
- Der Signaturschlüssel ist auf einem sicheren Speichermedium mit Schutz vor Auslesen, Kopieren, Modifizieren oder Ersetzen zu speichern.
- Der Datenträger mit dem Signaturschlüssel ist persönlich zu übergeben und zu quittieren, es sei denn, eine andere Übergabe wird schriftlich verlangt.
- Der Signaturschlüsseldatenträger (z. B. Chipkarte, Diskette) ist sicher aufzubewahren. Zur Berechtigungsprüfung sind PIN-, Passwort- oder biometrische Verfahren einzusetzen. Der Signaturschlüssel ist geheim zu halten.
- Nach Verlust oder bekannt werden des Signaturschlüssels vor Ablauf der Gültigkeit ist sofort eine Sperrung des Zertifikates zu veranlassen.
- Der Datenträger mit dem Signaturschlüssel ist unbrauchbar zu machen, wenn er nicht mehr benötigt wird. Außerdem ist die Sperrung des Zertifikates zu veranlassen, falls es nicht abgelaufen ist.

· Die Registrierung und Zertifizierung des öffentlichen Schlüssels sowie die Pflege von Zertifikaten und Sperrlisten muss in sicherer Umgebung erfolgen.
· Das Personal muss die erforderliche berufliche Qualifikation besitzen.
· Durch Schulung und Benutzerfreundlichkeit ist eine Fehlbedienung auszuschließen.

Obwohl eine digitale Signatur Integrität und Authentizität einer Datei nachweist, bietet sie keinen Schutz davor, dass eine Datei von Unbefugten gelesen wird. Deshalb sollte - falls erforderlich - eine Datei zur Gewährleistung von Vertraulichkeit möglichst vor ihrer digitalen Signierung verschlüsselt werden.

Wenn digital signierte Daten über einen längeren Zeitraum benötigt werden, könnte infolge des technischen Fortschritts (z. B. schnellerer Rechner) oder neuer wissenschaftlicher Erkenntnisse, evtl. die gesetzlich geforderte Sicherheit nicht mehr gewährleistet werden. Deshalb muss gemäß § 18 SigV von Zeit zu Zeit eine neue digitale Signatur mit neuen technischen Komponenten generiert werden. Man spricht dann von Mehrfachsignatur oder erneuter digitalen Signatur. Eine erneute digitale Signatur muss:
- mit neuen Algorithmen oder zugehörigen Parametern erfolgen,
- vor Ablauf des Zeitpunktes der Eignung der Algorithmen und Parameter die Daten mit einer neuen digitalen Signatur versehen,
- die früheren Daten und die frühere Signatur einschließen und
- einen Zeitstempel haben. Er bescheinigt digital, dass bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben.

4. Pilotversuch SPHINX zum Einsatz digitaler Signaturen

Seit April 1998 führt die „Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt)“ in Zusammenarbeit mit dem BSI einen Pilotversuch SPHINX zur Ende-zu-Ende-Sicherheit für E-Mail in den öffentlichen Verwaltungen durch. Den Teilnehmern des Pilotprojektes werden kryptographische Sicherheitsprodukte von zehn verschiedenen Firmen zur Verschlüsselung und digitalen Signatur für die Kommunikation per E-Mail zur Verfügung gestellt. Durch den Einsatz der Sicherheitsprodukte sollen sowohl Integrität und Authentizität als auch Vertraulichkeit für E-Mails gewährleistet werden.

Die eingesetzten Sicherheitsprodukte unterschiedlicher Hersteller müssen auf herstellerübergreifenden Standards (MailTrusT-Spezifikation) beruhen, Konformität zum Signaturgesetz anstreben und außerdem ohne Verzicht auf Sicherheitsfunktionalitäten miteinander verträglich, d. h. interoperabel sein.

Die Arbeitsplätze der Teilnehmer wurden mit Chipkartenlesern und Sicherheitssoftware ausgestattet. Die benötigten Schlüssel können sowohl zentral als auch dezentral erzeugt und auf Disketten oder Chipkarten gespeichert werden. Zur Erzeugung digitaler Signaturen werden RSA-Verfahren mit einer Schlüssellänge von 1024 Bit und die Hashfunktion SHA-1 mit 160 Bit Länge verwendet. Zertifizierungsstellen unterschiedlicher Betreiber veröffentlichen auf einem über das Internet erreichbaren Verzeichnisserver Zertifikate und Sperrlisten.

Die Teilnehmer testen hauptsächlich E-Mail-Sicherheitsprodukte für Microsoft Outlook 97/98 und LotusNotes für die Betriebssysteme Windows 95/98.

Die ersten beiden Phasen des Pilotprojektes (bis Spätsommer 1999) wurden erfolgreich abgeschlossen. Der Pilotversuch wird mit angepassten bzw. neuen Zielen (z. B. Sicherheitsprodukte für Betriebssystem LINUX) fortgesetzt.
Die Erfahrungen können nun von den öffentlichen Verwaltungen genutzt werden, um die Einführung digitaler Signaturen zu erleichtern.

14.4 Verschlüsselung mobiler Datenträger

Elektronisch gespeicherte personenbezogene Daten auf mobilen Datenträgern (z. B. Wechselplatten, Disketten, CDs, Magnetbänder, Kassetten) könnten beim Transport, während der Aufbewahrung oder nach einem Diebstahl von Unbefugten gelesen, kopiert, verändert oder gelöscht werden. Mit Hilfe kryptographischer Verfahren kann auch bei mobilen Datenträgern durch Verschlüsselung ein unberechtigter Zugriff auf personenbezogene Daten verhindert werden.

1. Nutzung kryptographischer Verfahren

Zur Verschlüsselung von Daten mit kryptographischen Verfahren kann ein Anwender spezielle Hard- und Software einsetzen. Diese handelsüblichen Sicherheitsprodukte unterstützen übliche Betriebssysteme (MS-DOS, Windows 3.x, Windows 95, Windows 98, Windows NT, OS/2 und UNIX) und unterschiedliche Arten von Datenträgern (CD, ZIP-Medium, Disketten).
Zum Verschlüsseln von Daten bieten die meisten Sicherheitsprodukte symmetrische Chiffrieralgorithmen an, die sehr schnell arbeiten und wenig Rechenzeit benötigen. Symmetrische Verfahren benutzen nur einen geheimen Schlüssel zum Ver- und Entschlüsseln. Dieser muss sowohl beim Absender als auch beim Empfänger vorliegen. Der Absender muss den Schlüssel dem Empfänger auf sicherem Weg (Kurier, per Brief, persönlich, telefonisch oder noch besser als Liste von „Einmalschlüsseln“) zustellen. Das sollte zeitlich und räumlich getrennt von den verschlüsselten Datenträgern erfolgen.
Der geheime Schlüssel ist nach Maßgabe der erforderlichen Sicherheit auszuwählen und sicher aufzubewahren. Als besonders zuverlässig haben sich zufällig erzeugte

Schlüssel erwiesen. Vor jeder neuen Chiffrierung sollte auch ein neuer Schlüssel vereinbart werden. Wenn ein Schlüssel wie ein Passwort gewählt werden kann, sind die Regeln des Passwortgebrauchs zu beachten.
Dem Anwender stehen häufig unterschiedliche symmetrische Verschlüsselungsalgorithmen (z. B. Triple-DES, IDEA, DES, Blowfish, XOR, STEALTH) zur Verfügung, die sich sowohl in der Sicherheit als auch in der Verarbeitungsgeschwindigkeit unterscheiden. Eine Verschlüsselung mobiler Datenträger kann auf Datei- oder Blockebene erfolgen. Während eine Dateiverschlüsselung nur die Dateien auf dem Datenträger chiffriert, verschlüsselt eine Blockchiffrierung auch noch die Verzeichnisinformationen.
Zum Ver- und Entschlüsseln eines mobilen Datenträgers können unterschiedliche Sicherheitsprodukte eingesetzt werden, wenn diese

- gleiche symmetrische Algorithmen mit der erforderlichen Mechanismenstärke nutzen,
- gleiche geheime Schlüssel verwenden und
- die Sicherheitsprodukte interoperabel, d. h. miteinander verträglich sind.

  Zu beachten ist ferner, dass verschlüsselte Datenträger erst dann auf Viren geprüft werden können, wenn sie vorher entschlüsselt wurden.

2. Zur Sicherheit symmetrischer kryptographischer Verfahren

Die Sicherheit kryptographischer Verfahren ist in erster Linie von der Güte der Algorithmen und der zugehörigen Schlüssellängen, von der Vertraulichkeit der geheimen Schlüssel und dem Schlüsselmanagement abhängig. Darüber hinaus hängt die Sicherheit auch davon ab, ob zur Chiffrierung nur Software oder Hardwarekomponenten (z. B. Einsteckkarten) genutzt werden. Softwarelösungen sind vergleichsweise langsam, bieten weniger physikalische Sicherheit und sind aber leichter anpassbar. Hardwarelösungen sind relativ schnell und weisen eine höhere physikalische Sicherheit auf, da die Verschlüsselung direkt in der Hardware stattfindet. Allerdings kann in der Hardware meist nur ein einziger kryptographischer Algorithmus implementiert werden. Außerdem beeinflusst die technische Entwicklung (schnellere, billigere Systeme) und neue mathematischer Erkenntnisse die Sicherheit kryptographischer Verfahren.

Im Verschlüsseln unerfahrene Anwender sollten zur qualifizierten Bewertung der Nutzbarkeit kommerzieller Kryptoalgorithmen für konkrete Aufgaben das Wissen von Experten oder die Empfehlungen des IT-Grundschutzhandbuches 1999 (Bundesanzeiger-Verlag) im Baustein Kryptokonzept nutzen.
Gegenwärtig wird für einen mittleren Schutzbedarf nur der Einsatz anerkannter symmetrischen Verfahren mit einer Schlüssellänge von mindestens 80 Bit empfohlen.

14.5 Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet, erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (überarbeitete Fassung)

I. Einleitung

Das Internet ist ein weltweites Computernetz, in dem hunderttausende größere Rechnerverbünde und somit Millionen einzelner Computer zusammengeschlossen

sind. Das Internet hat sich zum weltgrößten und mächtigsten globalen Informations- und Kommunikationsmedium entwickelt. Der Internet-Boom hat auch vor den öffentlichen Verwaltungen nicht Halt gemacht. Seit geraumer Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen (zur Beschreibung des Internet und der wichtigsten Internet-Dienste, vgl. Anhang).

Dabei ist der Anschluss an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Denn das Internet wurde ursprünglich nur unter Verfügbarkeitsaspekten entwickelt – auch wenn neuere Entwicklungen versuchen, weiteren Sicherheitsbedürfnissen Rechnung zu tragen. Deshalb wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von bereits weit mehr als 100 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Die vorliegende Orientierungshilfe wurde vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt. Sie soll den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der „internen“ Netze bei einem Anschluss an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, in welchen Fällen und unter welchen Bedingungen es zulässig ist, dass Verwaltungen personenbezogene Daten mit Hilfe des Internet übertragen oder veröffentlichen, ist nicht Gegenstand der Orientierungshilfe und muss jeweils konkret untersucht werden. Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der „Entdeckung“ neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluss an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen hinreichend beherrscht werden können.

II. Vorbereitung und Planung

Grundlage für eine datenschutzgerechte Nutzung des Internet ist eine genaue Planung der Internet-Aktivitäten einer Verwaltung. Je nach dem Informations- und Komm-

unikations-Bedarf ist eine der möglichen Nutzungsarten unter Berücksichtigung einer der Anschlussmöglichkeiten vorzusehen. Es bedarf einer genauen Analyse sowohl dieses Bedarfs als auch der mit der jeweiligen Anschlussart verbundenen Risiken.

1. Nutzungs- und Anschlussmöglichkeiten

1.1 Nutzungsarten

Grundsätzlich sind drei Konstellationen der Internet-Nutzung einer Behörde zu unterscheiden:

1. Eine Behörde nutzt einen Internet-Zugang nur, um Informationen im Internet suchen zu können, und/oder
2. eine Behörde stellt eigene Informationen im Internet zum (potentiell weltweiten) Abruf zur Verfügung (wobei im Internet von Informationsanbietern erwartet wird, dass sie auch per E-Mail erreichbar sind) oder
3. eine Behörde stellt eigene Informationen im Internet zum Abruf zur Verfügung und bietet zusätzlich die Interaktion mit Bürgerinnen und Bürgern, z. B. per E-Mail, an.

Diese drei Konstellationen können auf verschiedene Art und Weise technisch umgesetzt werden und verlangen unterschiedliche Maßnahmen, um den Datenschutz und die Datensicherheit zu gewährleisten.

1.2 Anschlussarten

Die Anschlussarten an das Internet können in drei verschiedene Szenarien unterteilt werden, die unterschiedliche Sicherheitsrisiken mit sich bringen:

1.2.1 Direktanschluss eines Rechners an das Internet

Hier wird ein einzelner, nicht lokal vernetzter Rechner per Modem und Telefonleitung über einen Provider (dies kann ein verwaltungsinterner oder ein externer sein) an das Internet angeschlossen. Diese Variante spielt besonders bei kleinen Behörden und im privaten Bereich eine große Rolle. Bei eventuellen Angriffen besteht ein Sicherheitsrisiko nur für den einzelnen Rechner. Es lässt sich durch entsprechende Maßnahmen reduzieren (z. B. ausschließliche Verwendung des Rechners für den Zugang zum Internet; sicherstellen, dass Ressourcen des Rechners - wie etwa Festplattenverzeichnisse - nicht für den Zugriff über das Netz freigegeben sind).

1.2.2 Zentrale Kopplung eines lokalen Netzes an das Internet

Hier hat der Rechner (evtl. über ein LAN oder aber direkt per Modem oder ISDN) einen Zugang zum Intranet der Verwaltung. Von dort besteht ein einziger zentraler Zugang zum Internet. Eventuelle Angriffe aus dem Internet können bereits an der zentralen Übergangsstelle vom Internet zum Intranet zum großen Teil abgefangen werden. Der Rechner bzw. das LAN ist zusätzlich aus dem Intranet heraus angreifbar.

1.2.3 Dezentrale Zugänge zum Internet

Neben einem direkten Internet-Anschluss über einen Provider verfügt der Rechner gleichzeitig über eine Verbindung zu einem Intranet. Bei eventuellen Angriffen besteht nicht nur ein Sicherheitsrisiko für den an das Internet angeschlossenen Rechner, sondern auch für das LAN, in dem sich der Rechner befindet, und das Intranet. *Daher ist von dieser Konstellation generell abzuraten.*

2. Kommunikations- und Risikoanalyse

Vor einem Anschluss an das Internet ist eine Analyse des Kommunikationsbedarfs durchzuführen. Bei der Beurteilung der Erforderlichkeit eines Internet-Anschlusses ist ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluss eines isolierten Rechners erreicht werden kann.

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden müssen. Bei der Beurteilung der Erforderlichkeit ist ebenfalls ein strenger Maßstab anzulegen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen aufgrund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden.

Ausgangspunkte einer derartigen Analyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle sowie die Risiken der unterschiedlichen Dienste.

In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuchs sind im Rahmen einer Risikoanalyse zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z. B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzer-spezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (z. B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert.)
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, dass nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen.

Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und so weit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muss und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann. Bei einem unvertretbaren Restrisiko muss auf einen Anschluss des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste kann in diesem Fall nur über solche Systeme erfolgen, die nicht mit dem Verwaltungsnetz verbunden sind und auf denen ansonsten keine sensiblen Daten verarbeitet werden.

3. Sicherheitsrisiken und Schutzmaßnahmen

Mit dem Zugang zum Internet sind Risiken verbunden, die großenteils daraus resultieren, dass das Datennetz nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So stellt das zugrunde liegende Protokoll beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung bereit.
Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluss wider. Selbst wenn Maßnahmen gegen die bekannten Gefährdungen getroffen werden, lässt sich ein hundertprozentiger Schutz ohne Verzicht auf die Internet-Anbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

3.1 Protokollimmanente Sicherheitsrisiken

Bei vielen gängigen Diensten werden die Inhaltsdaten im Klartext über das lokale Netz (z.B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter der Bezeichnung LAN-Analyzer bekannt sind (z. B. Packet Sniffer), kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden.

Gegenmaßnahmen: Verschlüsselung der Daten

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden z.B. lassen sich die IP-Adressen von Sender und Empfänger fälschen, die TCP Sequence Number von Paketen kann häufig vorhergesagt werden, und der Übertragungsweg ist bei dynamischem Routing modifizierbar. Pakete können abgefangen werden, so dass sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin lässt sich die Kommunikation eines autorisierten Nutzers mitschneiden und später wiedereinspielen (Replay Attack), wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z. B. beim Festplattenzugriff über NFS [Network File System]).

Gegenmaßnahmen:
Gegen eine unerkannte Manipulation von Nachrichteninhalten können digitale Signaturen eingesetzt werden. Für starke Authentisierung eignen sich Einmalpasswörter oder Challenge-Response-Systeme gegen Replay Attacks. Für Router sollte nach Möglichkeit statisches Routing konfiguriert werden. Außerdem sollte das „Source Routing" abgestellt sein.

Bei vielen Internet-Diensten erfolgt die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers. Dies kann sich ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen (IP-Spoofing) ans fremde Rechnersystem schickt. Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit unbeschränkter Administratorberechtigung, gewährt.

Gegenmaßnahmen:
Konfiguration eines Packet Filters, so dass alle Pakete mit ungültigen IP-Adressen (definiert im RFC 1597) und mit offensichtlich gefälschten IP-Adressen (z. B. IP-Pakete von außen mit internen Adressen) verworfen werden und nicht ins System gelangen können. Hierbei sollte man ebenfalls verhindern, dass IP-Pakete mit ungültigen Adressen das eigene System verlassen können (weitere Hinweise: RFC 2267 (Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing).

Angriffe mit gefälschten Paketen von ARP (Address Resolution Protocol) oder ICMP (Internet Control Message Protocols) basieren ebenfalls darauf, dass sich Rechner allein durch ihre IP-Adresse als legitimer Absender ausgeben können. So kann ein Angreifer bei einem Missbrauch von ARP die IP-Adresse eines anderen Benutzers in einem lokalen Netz übernehmen und damit selbst Verbindungen herstellen oder die Erreichbarkeit des anderen Rechners vollständig verhindern. Auch Firewalls, die aufgrund von IP-Adressen entscheiden, ob eine Verbindung zulässig ist, lassen sich dadurch täuschen. Bei ICMP-Angriffen werden gefälschte Statusmeldungen verschickt, die beispielsweise eine Umleitung der Pakete über einen Router des Angreifers bewirken oder die gesamte Kommunikation eines Rechners nach außen verhindern (Denial of Service Attack). Der „Ping of Death" ist ein besonderer ICMP-Angriff, bei dem zu große Pakete beim Empfänger einen Überlauf des Empfangspuffers verursachen und den Rechner zum Absturz bringen. Ein ähnlicher Effekt wird bei vielen Windows-Rechnern durch das Senden spezieller Pakete (Out-of-Band [OOB]) bevorzugt auf den Port 139 erreicht. Gegen diesen Winnuke-Angriff können einige Windows-Versionen durch Patches geschützt werden.

Gegenmaßnahmen: Installation von Patches, starke Authentisierung

Durch den „TCP Syn Flood"-Angriff können ebenfalls Rechner blockiert werden. Dabei wird ein WWW-Server mit einer großen Anzahl von IP-Paketen mit ungültigen Absenderadressen bombardiert, auf die das System vergeblich zu antworten versucht. Dadurch kann der ganze Server über einen längeren Zeitraum lahm gelegt werden.

Gegenmaßnahmen: Installation von Patches

3.2 Dienstespezifische Sicherheitsrisiken

3.2.1 E-Mail und Usenet-News

Elektronische Post (E-Mail) kann mitgelesen werden, sofern sie nicht verschlüsselt ist. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können - wie bei einem Transfer per Diskette - Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.

Gegenmaßnahmen: Verschlüsselung und digitale Signatur, Virenschutzsysteme

Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, weist eine ganze Reihe von Sicherheitslücken auf, die zu einer Zugangsmöglichkeit mit Administratorrechten führen können.

Gegenmaßnahmen:
Installation von Patches, Verfolgen der Meldungen über neue sicherheitsrelevante Fehler

3.2.2 Telnet

Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Selbst wenn sich ein Angreifer keinen Zugang mit Administratorrechten verschaffen kann, gelingt es ihm häufig, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

Gegenmaßnahmen:
Einschränkung der Telnet- und verwandten Dienste auf die notwendigen Adressen und Ports an einer Firewall

Mit Hilfe verschiedener Programme (z. B. das Cracker-Tool „Juggernaut“) können mittlerweile Telnet-Verbindungen „entführt“ werden, d. h. der Angreifer kann damit nicht nur Passwörter mitlesen, sondern auch in die Verbindung eingreifen, den ursprünglichen Benutzer abhängen und stattdessen sich selbst einklinken. Ähnliche Sicherheitsrisiken bestehen für „R-Utilities“ wie rlogin.

Gegenmaßnahmen:
Vollständiger Verzicht auf den Telnet-Dienst sowie auf rlogin, rsh und rcp, stattdessen Verwendung von SSH (Secure Shell), einem Software-Paket, mit dem man durch anerkannte kryptographische Verfahren eine zuverlässige gegenseitige Authentisierung und eine transparente Verschlüsselung des gesamten Datenstroms erreichen kann. Dabei werden statt rlogin, rsh und rcp neue Programme ssh und scp eingesetzt. Das SSH-Paket steht für alle gängigen Betriebssysteme zur Verfügung (z. B. für UNIX: ftp://ftp.cs.hut.fi/pub/ssh/ oder ftp://ftp.cert.dfn.de/pub/tools/net/ssh;

für Windows (kommerziell): http://www.europe.datafellows.com/f-secure/fssh-reg.htm).

3.2.3 FTP

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen bestimmter FTP-Server (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsrelevante Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Passwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Lässt man zu, dass Benutzer eines FTP-Servers anonym eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

Gegenmaßnahmen:
Ersatz des FTP-Dienstes (incl. rcp) durch Programme aus dem SSH-Paket (scp) oder Konfiguration eines SSH-Kanals mit Verschlüsselung und Authentisierung, Beschränkung durch Vergabe von entsprechenden Zugriffsrechten

3.2.4 WWW

Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) oder anderen Verschlüsselungen lässt sich die Kommunikation abhören. Außerdem können Skripte zur dynamischen Generierung von Dokumenten Sicherheitslücken aufweisen.
Ende 1996 wurde die Angriffsmethode *Web-Spoofing* bekannt, bei dem ein Angreifer seinen Server zwischen das eigentliche Zielsystem und den Rechner des Benutzers schaltet. Der Angreifer erstellt auf seinem System eine täuschend echte Kopie der Daten, die er komplett kontrollieren und für seine Belange modifizieren kann. Danach hat er nach Belieben die Möglichkeit, vom Benutzer verschickte Informationen abzufangen oder zu manipulieren.

Gegenmaßnahmen:
Verschlüsselung und digitale Signatur für die Kommunikation, Zertifikate für Web-Server, gegenseitige Authentisierung von Nutzer und Web-Server

3.2.5 DNS

Mit Hilfe des Domain Name Service (*DNS*) lassen sich Rechnernamen in IP-Adressen umsetzen und umgekehrt. Dabei besteht die Gefahr, dass Informationen über die Struktur des internen Netzes nach außen gelangen. Auch beim DNS gibt es mittlerweile die Angriffsmethode des *Spoofing*. Mit gefälschten Informationen im DNS können Datenströme in beliebige Bahnen gelenkt werden, wenn der Benutzer statt der numerischen IP-Adresse den leichter zu merkenden Rechnernamen angibt.

Gegenmaßnahmen:
Verbergen der Struktur des internen Netzes durch geeignete Anordnung von DNS-Servern, Adressierung durch die numerische IP-Adresse, soweit praktikabel, Einsatz eigener Domain Name Server

3.2.6 Finger

Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen Angriff genutzt werden können. Berühmt geworden ist dieser Dienst 1988 durch den so genannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, dass die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten, die nicht mehr in den Puffer passten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden (*Buffer Overflow Bug*). Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen. Ähnliche Programmierfehler finden sich auch heute noch in vielen anderen Serverprogrammen.

Gegenmaßnahmen:
Abschalten der Dienste, über die sich Angreifer sicherheitsrelevante Informationen aus dem System beschaffen können: finger, rup, rusers, rwho, SMTP EXPN, SMTP VRFY, Installation von Patches gegen den Buffer Overflow Bug

3.2.7 SNMP

Mit Hilfe des Simple Network Management Protocol-Dienstes können Netzwerkkomponenten von zentraler Stelle aus verwaltet werden. Dazu können Informationen über die Konfiguration und den Betriebszustand der Komponenten abgefragt und verändert werden. Dies bietet dem Angreifer u. U. wertvolle Hinweise über die eingesetzte Hard- und Software, die für weitergehende Attacken ausgenutzt werden können.
Besondere Bedeutung kommt dabei den sog. Community Strings zu, die eine einfache Form der Authentisierung bei SNMP darstellen. Häufig ist bei Auslieferung der Community String „public“ eingestellt, der einen unberechtigten Zugriff auf den Dienst sehr erleichtert.

Gegenmaßnahmen:
Verwendung schwer zu erratender Community Strings, jedenfalls nicht „public“, Begrenzung der von SNMP zur Verfügung gestellten Informationen auf das Erforderliche

3.3 Aktive Inhalte/Aktive Elemente

3.3.1 ActiveX

ActiveX ist eine *Entwicklung der Firma Microsoft*. Es steht für eine Reihe von Technologien, die dafür sorgen, dass Windows-Anwendungen mit dem Internet oder Intranet zusammenarbeiten. WWWSeiten können mit dieser Technologie um eine Vielzahl von multimedialen Effekten, unterschiedlichen Layouts und ausführbaren Applikationen, die über das Internet geladen werden, erweitert werden. Die Technologie besteht im Wesentlichen aus folgenden Elementen: ActiveX-Controls, Active Documents und Active Scripting.
ActiveX-Controls sind Programme, die auf einer WWW-Seite dargestellt oder als eigene Programme aufgerufen werden können. Active Documents ermöglicht die Anzeige und Betrachtung von Nicht-HTML-Dokumenten (z. B. Word oder Excel) innerhalb eines Browsers. ActiveX Scripting ermöglicht das Verwalten und die Kom-

munikation von ActiveX-Controls, beinhaltet einen Java-Compiler und ist eine Umgebung zur serverseitigen Nutzung von ActiveX-Controls. Eine ActiveX-Sicherheitsarchitektur gibt es nicht. Die vorhandenen Sicherheitsmechanismen bieten kein in sich konsistentes Sicherheitssystem. Microsoft setzt auf die Nachvollziehbarkeit der Herkunft der heruntergeladenen Codes durch Codesignierung. Für die Codesignierung setzt Microsoft die selbstentwickelte *Authenticode Technologie* ein. Sie beruht auf einer digitalen Signatur und erlaubt neben der sicheren Identifikation des Absenders den Nachweis der Echtheit der übertragenen Codes. Dieses Verfahren macht aber keine Aussage über die Funktionsweise der Software selbst und ob sie gewollt oder ungewollt (Programmierfehler) schadensstiftende Wirkung entfalten kann. Microsoft arbeitet mit der Firma Verisign als Zertifizierungsstelle zusammen und vergibt zwei unterschiedliche Zertifikate: Individualzertifikate und kommerzielle Zertifikate. Es existiert ein mehrstufiges Sicherheitssystem im Zusammenspiel von ActiveX und den unterschiedlichen Browsern. Neben der Möglichkeit, die ActiveX-Funktionalität (gilt für alle Browser) abzuschalten, besteht auch die Option, im Internet-Explorer einen Sicherheitslevel (hoch, mittel und niedrig) vorzugeben. Bei einem hohen Sicherheitslevel werden nur zertifizierte ActiveX-Controls akzeptiert. Bei einem mittleren Level müssen nicht zertifizierte ActiveX-Controls explizit freigegeben werden. Ein niedriger Level bietet gar keinen Schutz. Eine weitere Möglichkeit, sich zu schützen, bieten *ActiveX-Filter*, die Listen mit Servern definieren, von denen ActiveX-Komponenten akzeptiert werden. Der Einsatz des *Internet-Explorer-Administration-Kit* (IEAK) ermöglicht die Erstellung von spezifisch angepassten Internet-Explorern.
ActiveX-Komponenten stellen, da sie keinerlei Einschränkungen bzgl. der Windows- und System-Funktionalität unterliegen, ein immenses Sicherheitsrisiko dar. Folgende Sicherheitsrisiken sind bisher bekannt: *Ausforschung von Nutzern und Computersystemen, Installieren und Ausführen von Viren und Trojanischen Pferden, Beschädigung von Systemressourcen und Überlasten des Systems*. Aus Sicherheitsgründen empfiehlt es sich daher, die ActiveX-Unterstützung gänzlich abzuschalten.

Gegenmaßnahmen:
Abschalten der ActiveXUnterstützung, Verwendung des Microsoft-Authenticodes, Aktivieren einer hohen Sicherheitsstufe im Internet-Explorer, Einsatz von ActiveX-Filtern und des Internet-Explorer-Administration-Kits in Netzwerken

Abschließend sei noch auf die *unzureichenden Sicherheitsmechanismen der Betriebssystemplattformen* hingewiesen. Die Plattform Windows 95 verfügt über keinerlei eingebaute Sicherheitsmechanismen zur Abwehr von Angriffen, und unter Windows NT laufen ActiveX-Controls im Rechteraum (mit den Zugriffsrechten) des gerade angemeldeten Benutzers.

3.3.2 Java

Java ist eine *objektorientierte Programmiersprache*, die unabhängig von der jeweiligen Systemplattform nutzbar ist. Sie wurde von *SUN Microsystems* entwickelt. Java bietet die Möglichkeit, Stand-Alone-Anwendungen (Java-Applikations) sowie Anwendungen für das WWW (Java-Applets) zu schreiben. Java-Applets können in HTML-Seiten integriert, über das Internet angefordert und auf beliebigen Rechnern

ausgeführt werden, ohne dass der Entwickler die lokale Umgebung des Anwenders kennen muss. Einzige Bedingung für die Lauffähigkeit ist die Verfügbarkeit der JVM (virtuelle Java Maschine) auf der Plattform. Java verfügt über ein integriertes Sicherheitssystem. Das *Sandbox-System* ist mehrstufig, bezogen auf die vier Softwareebenen, die bei der Herstellung und Ausführung von Java-Funktionen beteiligt sind:

1. Programmiersprache Java,
2. Virtuelle Java Maschine,
3. Lader für Java-Klassen und
4. Java-Bibliotheken.

Ist JVM Bestandteil des HTML-Viewers, werden Applets ausgeführt, die sehr strengen Sicherheitskontrollen unterliegen. Applets, die über das Netz geladen werden, haben auf dem Client keine Lese- und Schreibrechte, können keine fremden Programme starten, keine Systemfunktionen aufrufen, keine Netzwerkverbindung zu anderen Rechnern aufbauen, keine zusätzlichen Bibliotheken laden und kennzeichnen Fenster besonders, die durch Applets gestartet wurden.
Applets können im Standardfall auch nur definierte Systemeigenschaften (z. B. Betriebssystem NT) lesen. SUN bietet in neueren Versionen die Möglichkeit, mit *signierten Applets* zu arbeiten. Die Applets werden zertifiziert und mit einer digitalen Signatur versehen, bevor sie im Netz zur Verfügung gestellt werden. Somit kann der Client die Authentifikation und die Herkunft prüfen. Die Signierung sagt nichts über die Funktionalität des Programmes. Die Java-Spezifikation bietet mit ihren durchdachten Mechanismen eine ausreichende Sicherheit, aber durch Implementierungsfehler wurden Angriffe durch Java-Applets möglich. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen modifizieren (durch Programmier- und Implementationsfehler in den Ablaufumgebungen), die eine weitere Nutzung des Systems verhindern (*Überlasten des Systems*) oder die Nutzer ausforschen oder belästigen.
Um sich vor Angriffen zu schützen, bieten sich mehrere Optionen an. Zusätzlich zu dem eigenen Sicherheitssystem können noch folgende Maßnahmen ergriffen werden. Man kann z. B. im Browser *die Java-Funktionalität abschalten*. Einen weiteren Schutz bieten *Java-Filter*, die Listen mit Servern definieren, von denen Java-Applets akzeptiert werden. In neueren Browser-Versionen ist das *Arbeiten mit signierten Applets* möglich.

Gegenmaßnahmen:
Abschalten der Java-Funktionalität, Einsatz von Java-Filtern, Arbeiten mit signierten Applets, Verwendung von Browsern, bei denen JVM sauber implementiert ist

3.3.3 JavaScript

JavaScript ist eine von der *Firma Netscape Communication* entwickelte *Skriptsprache*, die plattformunabhängig ist. Sie wird direkt in die HTML-Seiten eingebettet und über einen Interpreter interpretiert und ausgeführt. Die Motivation für die Entwicklung von JavaScript waren die Unzulänglichkeiten der vorhandenen Techniken (HTML und CGI) für Benutzer-Interaktivitäten. Jede Interaktion musste an den Server gesendet werden, um mit Hilfe des CGI-Programmes Plausibilitätsprüfungen durchzuführen. Durch den Einsatz von JavaScript wurde die Anzahl der notwendigen Verbindungen zum Server drastisch verringert. Dynamisch zur Laufzeit können mit

JavaScript beispielsweise Eingaben überprüft oder auch Berechnungen durchgeführt werden. Außerdem lassen sich wichtige Funktionen des Browsers, wie Öffnen und Schließen von Fenstern, Manipulieren von Formularelementen oder das Anpassen von Browser-Einstellungen verwirklichen. Ein Zugriff auf Dateisysteme auf anderen Rechnern ist nicht möglich. Netscape bietet die Möglichkeit, mit *zertifizierten JavaScript-Codes* zu arbeiten. Es wurden jedoch Sicherheitsprobleme in zwei Bereichen bekannt, zum einen in der *Ausforschung von Nutzern und Computersystemen* und zum anderen in der *Überlastung von Rechnern*. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen durch Programmierfehler und Implementierungsfehler in den Ablaufumgebungen modifizieren oder eine weitere Nutzung des Systems - vorsätzlich erzeugt oder ungewollt durch Programmierfehler - verhindern, und Angriffen die das Lesen von fremden Nachrichten, Ändern von Nachrichten und Verschicken von Texten ermöglichen. Die meisten Sicherheitslöcher sind implementierungsabhängig.

Gegenmaßnahmen:
Arbeiten mit zertifizierten JavaScript-Codes oder das Abschalten der JavaScript-Funktionalität, Verwendung von Browsern, bei denen die Anwendung sauber implementiert ist

3.3.4 Plug Ins

Browser Plug Ins sind auf dem Client laufende Software-Module, die den Funktionsumfang des Browsers erweitern und beispielsweise die Darstellung von Audio- und Videodaten erlauben. Plug Ins sind plattformabhängig, belegen lokalen Plattenspeicher und müssen vom Benutzer beschafft und installiert werden.

Gegenmaßnahmen:
Schulung der Benutzer, um unbeabsichtigtes Installieren der Software zu verhindern

3.3.5 Cookies

Cookies (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar. Die Anwendungsmöglichkeiten gehen jedoch weit darüber hinaus.
Typischerweise werden Cookies eingesetzt, damit der Nutzer das Angebot des angewählten Webservers auf seine persönlichen Belange hin abstimmen kann, bzw. um dem Webserver zu ermöglichen, sich selbsttätig auf die (vermuteten) Bedürfnisse des Nutzers einzustellen. Ein Betreiber von WWW-Diensten kann jedoch aus geeignet gewählten und eingerichteten Cookies ein Nutzungsprofil erstellen, das vielfältige Auskunft über den Benutzer gibt, und ihn so als geeignete Zielperson (z. B. für Werbebotschaften) identifiziert. Eine Manipulation des Computers über die Speicherung und Abfrage der Cookie-Daten hinaus ist mit dem Cookie-Mechanismus selbst nicht möglich. Da die Cookie-Informationen, die auch benutzerbezogene Passwörter für Web-Seiten umfassen können, jedoch in einer Datei im Dateisystem auf dem

Rechner gespeichert werden, kann ein Unberechtigter beispielsweise mit Hilfe von ActiveX-Controls (siehe Abschnitt 3.3.1) darauf zugreifen.
Problematisch sind Cookies trotzt dieses vergleichsweise geringen Gefährdungspotentials für die Computersicherheit aufgrund ihrer geringen Transparenz für den Benutzer. Der Datenaustausch mittels Cookies erfolgt zwischen den beteiligten Computern vollkommen im Hintergrund, ohne dass der Benutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Daten informiert wird, sofern er keine besonderen Maßnahmen ergreift. Diese Parameter sind innerhalb der Cookies selbst festgelegt und werden somit allein vom Betreiber des WWW-Servers bestimmt; der Internet-Nutzer hat hierauf im normalen Betrieb keinen Einfluss. Es hängt wesentlich von der Initiative des Nutzers und seiner technischen Kenntnis und Ausrüstung ab, ob er Cookies bemerkt und sich ggf. vor ihnen schützen kann.

Gegenmaßnahmen:
Konfiguration des Browsers, so dass Cookies nicht oder wenigstens nicht automatisch akzeptiert werden und Cookies, die gespeichert werden sollen, angezeigt werden, Löschen bereits gespeicherter Cookies (z. B. Datei cookies.txt bei Netscape-Browsern), Einsatz von Cookie-Filtern

III. Firewall-Systeme

1. Grundlagen

Soll ein Verwaltungsnetz an das Internet angeschlossen werden, so kann dies entweder durch einen zentralen oder durch mehrere dezentrale Zugänge erfolgen. Aus Sicherheitsgründen ist für ein (Teil-) Netz mit einheitlichem Schutzbedarf ein zentraler Zugang vorzuziehen. Die durch die Anbindung hervorgerufenen Sicherheitsrisiken lassen sich durch Einsatz einer Firewall reduzieren.
Unter einer *Firewall* („Brandschutzmauer“) wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin, zu erreichen, dass jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und dass Missbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, dass die Teilnehmer des internen Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: des Internets). Gleichwohl sind Firewall-Lösungen auch geeignet, die „grenzüberschreitenden“ Aktivitäten der internen Nutzer, d. h. den Übergang zwischen verschiedenen Teilnetzen (z. B. Ressortnetze) innerhalb eines Verwaltungsnetzes, zu begrenzen. Mit Hilfe von Firewall-Systemen lassen sich die vorher in der Kommunikationsanalyse definierten Anforderungen weitgehend technisch erzwingen (Policy-Enforcer).

1.1 Charakteristika von Firewall-Systemen

Firewalls weisen die folgenden Charakteristika auf:

- Die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz.
- Im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau. Eine weitere Differenzierung nach Sicherheitsstufen geschieht - zumindest auf der Ebene des Netzes - nicht.

- Die Firewall setzt eine definierte Sicherheitspolitik (*Security Policy*) für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen.
- Es besteht die Notwendigkeit die Benutzerprofile der internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen, auf die Firewall abzubilden.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung von Firewalls in die EDV-Infrastruktur.

1.2 Schutzniveau

Von besonderer Relevanz ist es, für den von einer Firewall geschützten Bereich das erforderliche Schutzniveau zu definieren. Diese Anforderung kann mit drei Lösungsvarianten erfüllt werden:

1. einheitlich hohes Schutzniveau im internen Netz, d. h. Orientierung am höchsten vorhandenen Schutzbedarf;
2. einheitlich niedriges Schutzniveau, d. h. Orientierung am niedrigsten vorhandenen oder an einem insgesamt geringen oder mittleren Schutzbedarf;
3. einheitlich niedriges Schutzniveau sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netzkomponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen, wobei angesichts der Sensibilität der in der Verwaltung verarbeiteten Daten Variante 2 indiskutabel und mit den Anforderungen des Datenschutzrechts unvereinbar sein dürfte. Variante 3 führt zur Lösung gestaffelter Firewalls, d. h. zu einer Konstellation, bei der neben einer zentralen, den mittleren Schutzbedarf abdeckenden Firewall (die u. a. die interne Netzstruktur nach außen sichert) bereichsbezogen und bedarfsorientiert Firewall-Anschlüsse mit unterschiedlichem Sicherheitsniveau implementiert werden können. Allerdings können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz gestaffelte Firewalls sinnvoll sein, um den möglichen Schaden, der mit Sicherheitsverletzungen verbunden ist, auf ein Netzsegment zu begrenzen. Dies gilt insbesondere auch für die Abwehr von internem Missbrauch.

2. Firewall-Technologien

Eine Firewall kann durch verschiedene Konzepte realisiert werden. Im Wesentlichen unterscheidet man folgende Grundkonzepte:

- Packet Filter (Packet Screen, Screening Router)
- Application Level Gateway (Dual-homed Gateway)
- Stateful Inspection (Stateful Packet Filter, Dynamic Packet Filter)

Ein *Packet Filter* (auch *Packet Screen* oder *Screening Router*) ist ein Router, der IP-Pakete zur Unterscheidung zwischen der erlaubten und unerlaubten Nutzung von Kommunikationsdiensten filtert. Packet Filter können nach Quell- und Zieladresse sowie nach Quell- und Zielport filtern. Damit ist sowohl einschränkbar, welche Rechner im zu schützenden und welche im unsicheren Netz an der Kommunikation beteiligt sein dürfen, als auch, welche Kommunikationsdienste erlaubt sind. Die Filterregeln sind an die Netzschnittstellen gebunden. Sie werden vom Packet Filter in der Reihenfolge abgearbeitet, in der sie angegeben sind.

Ein *Application Level Gateway* ist ein speziell konfigurierbarer Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Ein Application Level Gateway arbeitet im Gegensatz zum Packet Filter auf der Anwendungsschicht, d. h. die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt. Für jeden Dienst (Telnet, FTP usw.) werden *Security Proxys* eingeführt, die den direkten Zugriff auf den Dienst verhindern. Hierbei bestehen z. B. die Möglichkeiten einer ausführlichen Protokollierung (Audit) und einer benutzerbezogenen Authentisierung für die unterschiedlichen Dienste. Die meisten Application Level Gateways sind nicht in der Lage zu unterscheiden, über welche Netzschnittstelle ein Paket hereinkommt. Ein Application Level Gateway mit zwei Netzschnittstellen wird *Dual-homed Gateway* genannt.
Die Kombination von Packet Filter und Application Level Gateway wird als *Screened Gateway*, *Transparent Application Gateway* oder *Sandwich-System* bezeichnet und erhöht die Sicherheit der Firewall gegenüber den beiden Einzelkomponenten erheblich. Die Anordnung der beteiligten Komponenten kann variieren und erlaubt die individuelle Realisierung eines Firewall-Konzeptes.
Stateful Inspection (auch *Stateful Packet Filter* oder *Dynamic Packet Filter*) ist eine recht neue Firewall-Technologie und arbeitet sowohl auf der Netz- als auch auf der Anwendungsschicht. Die IP-Pakete werden auf der Netzschicht entgegengenommen, von einem Analysemodul, das dynamisch im Betriebssystemkern geladen ist, zustandsabhängig inspiziert und gegenüber einer Zustandstabelle abgeglichen. Die Regeln, nach denen das Modul agiert, können sehr differenziert vorgegeben werden. Für die Kommunikationspartner stellt sich eine Firewall mit Stateful Inspection als eine direkte Leitung dar, die nur für eine den Regeln entsprechende Kommunikation durchlässig ist. Im Out-Of-Band-Betrieb erfolgt die Wartung und Konfiguration nicht über TCP/IP. Die Firewall besitzt dann keine eigene IP-Adresse, so dass keine Möglichkeit besteht, sie über TCP/IP direkt aus den angeschlossenen Netzen anzusprechen oder auf diesem Wege anzugreifen. Optional führt die Firewall ein Rewriting durch, d. h. Pakete werden vor dem Weitersenden nach vorgegebenen Regeln transformiert.
Stateful Inspection vereinigt bereits konzeptuell die Schutzmöglichkeiten von Packet Filter und Application Level Gateway, so dass diese beiden Funktionen nicht in getrennten Komponenten realisiert werden müssen. Experten streiten sich darüber, welches Konzept in welcher Realisierung mehr Sicherheit mit sich bringt. Inzwischen werden auch hybride Firewalls angeboten, die zusätzlich zur Stateful Inspection Proxys wie beim Application Gateway zur Verfügung stellen.

	Vorteile	Nachteile
Packet Filter (Router oder Rechner mit spezieller Software)	leicht realisierbar, da von vielen Routern angeboten; leicht erweiterbar für neue Dienste; Router auf dem Markt verfügbar; Transparenz für den Benutzer; Arbeitsgeschwindigkeit	Übernahme des Packet Filter durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit; es ist bei den meisten Produkten nicht möglich, Dienste nur für bestimmte Benutzer zuzulassen; alle

	Vorteile	Nachteile
		Dienste, die erlaubt sind und erreicht werden können, müssen sicher sein; Protokollierung nur auf unteren Netzschichten möglich; keine Authentisierung möglich
Dual-homed Gateway (Application Level Gateway mit zwei Netzschnittstellen)	kein Paket kann ungefiltert passieren; aussagekräftige Protokollierung auf höheren Schichten möglich; interne Netzstruktur wird verborgen durch den Einsatz von Network Address Translation (NAT)	Übernahme des Gateways durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit; keine Transparenz für den Benutzer; Probleme bei neuen Diensten, schlechte Skalierbarkeit;
Screened Gateway (Anordnung aus Application Level Gateway mit einem oder zwei Packet Filtern (Teilnetz-Bildung))	kein direkter Zugang zum Gateway möglich; interne Netzstruktur wird verborgen; Network Address Translation (NAT); vereinfachte Regeln durch 2. Filter; durch Einsatz mehrerer Gateways lässt sich die Verfügbarkeit steigern; aussagekräftige Protokollierung möglich	keine Transparenz für den Benutzer; bei Realisation mit mehreren Rechnern und Routern: erhöhter Platzbedarf; Probleme bei neuen Diensten, schlechte Skalierbarkeit
Stateful Inspection (Firewall-Rechner mit zustandsabhängiger Analyse und Reaktion)	gute Skalierbarkeit; arbeitet auf Netz- und Anwendungsschicht; Out-Of-Band-Betrieb: keine Angriffsmöglichkeit über TCP/IP; interne Netzstruktur wird verborgen; Rewriting möglich (über NAT hinaus); umfangreiche Authentisierungsvarianten	Übernahme des Gateways durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit; keine Zwischenspeicherung, daher nicht volle Gateway-Funktionalität und kein Caching; schneller Rechner erforderlich, da wegen der umfangreichen Analyse und Aktionsmöglichkeiten sonst Performance-Einbußen

3. Firewall-Architekturen

Neben den im Folgenden dargestellten Architekturen von Firewalls sind auch Abwandlungen oder Kombinationen der Anordnungen möglich.

3.1 Zentrale Firewalls

Rein zentrale Firewall-Lösungen sind durch folgende Aspekte charakterisiert:

- Die zentrale Firewall bildet die einzige Schnittstelle (Choke Point) zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet.

- Innerhalb des gesamten Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht.
- Eine Kontrolle der internen Verbindungen durch die Firewall ist nicht möglich.
- Die zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus. Abweichende Sicherheitspolitiken für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar.
- Es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muss sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden.

Da eine zentrale Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muss sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, dass gerade von diesen Stellen zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird.

Ein weiterer Nachteil zentraler Firewalls besteht in dem - auch aus dem Großrechnerbereich bekannten - Problem, dass eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.
Da eine Firewall Zugriffe innerhalb des internen Netzes nicht kontrolliert, besteht bei rein zentralen Lösungen die Gefahr, dass das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas “Internet-Anbindung”, muss bei einer Gesamtbetrachtung von Netzsicherheit jedoch unbedingt einbezogen werden.
Der Einsatz einer alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Missbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

3.2 Gestaffelte Firewalls

Gestaffelte Firewall-Lösungen sind durch folgende Aspekte charakterisiert:

- Es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch eine zentrale Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen.
- Innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau.
- Eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich über schreitet.

- Auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitspolitik für das Gesamtnetz voraus. Bei ihrer Definition müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz einfließen. Darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren.
- Die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über die zentrale Firewall mit Systemen im Internet in Verbindung zu treten.
- Auch die dezentralen Firewalls müssen qualifiziert administriert werden.

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Technologien wie bei einer zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn die zentrale Firewall durch einen Eindringling überwunden wurde.
Mit gestaffelten Firewalls kann – anders als bei zentralen Lösungen – das datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze können sowohl gegen Angriffe von außen – aus dem Internet – als auch untereinander abgeschottet werden.
Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung "wilder" Internet-Zugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.
Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentrale Firewall und die dezentralen Firewalls verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im Wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden.

3.3 Entmilitarisierte Zone

Server, die Dienste für Internet-Nutzer zur Verfügung stellen (z. B. WWW oder Mail), werden häufig hinter einer Firewall in der so genannten *entmilitarisierten Zone (DMZ, Demilitarized Zone*, auch *Screened Subnet*) eingerichtet, von der das interne Netz durch eine (weitere) Firewall abgeschottet ist. Dies hat den Vorteil, dass das lokale Netz auch dann noch geschützt ist, wenn ein Angreifer bis zum WWW-Server gelangt.
Die entmilitarisierte Zone kann beispielsweise zwischen zwei Firewalls realisiert werden. Durch Verwendung unterschiedlicher Firewall-Produkte lässt sich dabei eine höhere Sicherheit erreichen, da mögliche Fehlfunktionen bei unabhängiger Entwicklung der Produkte wahrscheinlich nicht gleichzeitig auftreten.

Die Aufgaben der beiden Firewalls können auch von nur einer Firewall mit mehreren Schnittstellen übernommen werden, mit denen sich mehrere Netze mit unterschiedlicher Sicherheit bilden lassen. So können auch eine oder mehrere entmilitarisierte Zonen eingerichtet werden. Diese Lösung ist kostengünstiger, verzichtet aber auf die erhöhte Sicherheit.

3.4 Screened Gateway

Zumeist werden neben der Firewall Router eingesetzt, die oft die Funktion von Packet-Filtern übernehmen können. Damit lässt sich eine „Sandwich-Lösung“ realisieren, die durch Verwendung unterschiedlicher Systeme eine erhöhte Sicherheit gewährleisten kann. Auch hier ist die Einrichtung einer entmilitarisierten Zone möglich.

IV. Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall

1. Allgemeines

Firewalls sind selbst keine eigenständigen Telekommunikations-, Tele- oder Mediendienste, sondern als unselbständiger Bestandteil eines solchen Dienstes zu betrachten. Daher kommt für den Betrieb einer Firewall das Datenschutzrecht zur Anwendung, das auch für den zu Grunde liegenden Dienst gilt.

Soweit öffentliche Stellen sich eines Providers bedienen, kommen aufgrund der Regelungen zur Datenverarbeitung im Auftrag ebenfalls die folgenden Grundsätze zur Anwendung.

Betroffen von einer Protokollierung durch Firewalls sind in erster Linie die Bediensteten oder Arbeitnehmer der Stelle, deren Datenverarbeitungsanlage von der Firewall geschützt werden soll, im Fall der E-mail-Kommunikation aber auch die Kommunikationspartner. Im Übrigen könnten personenbezogene Daten von externen Nutzern wie auch von Angreifern auf diese Weise verarbeitet werden.

Hinsichtlich des Umfangs und der Zulässigkeit der Protokollierung von Zugriffen, die über eine Firewall erfolgen, und der Kontrolle von Inhaltsdaten lassen sich folgende Fallkonstellationen unterscheiden:

2. Kontrolle von Inhaltsdaten bei E-mail-Kommunikation

Die Frage nach der Zulässigkeit der Kontrolle von Inhaltsdaten wird insbesondere relevant bei eingehenden E-Mails, die nicht an die Mail-Adresse einer zentralen Poststelle, sondern an die Mail-Accounts einzelner Arbeitnehmer der betreffenden Dienststelle gerichtet sind. Hierbei können folgende Fallkonstellationen unterschieden werden:

2.1 Kontrolle auf Virenbefall mittels automatischem Virencheck

Sowohl bei dienstlicher als auch bei privater Nutzung bestehen grundsätzlich gegen eine Kontrolle auf Virenbefall mittels automatischem Virencheck keine Bedenken, soweit die Kontrolle ausschließlich automatisch erfolgt und die Kenntnisnahme von den Inhalten privater E-Mails durch Vertreter der Dienststelle (z. B. den Systemadministrator) nicht ohne Einwilligung des Benutzers erfolgt.

Dadurch kann allerdings eine dezentrale Überprüfung der Dateien auf Viren nicht bzw. nicht vollständig ersetzt werden, da Virencheckprogramme Viren, die in verschlüsselten E-Mails enthalten sind, nicht erkennen können. Mindestens für diese E-Mails muss daher nach der Entschlüsselung eine Virenüberprüfung beim Benutzer selbst erfolgen.

2.2 Kontrolle eingehender dienstlicher E-Mails

Wie bei herkömmlicher Post können Vorgesetzte sich auch eingegangene dienstliche

E-Mails von den betreffenden Mitarbeitern vorlegen lassen. Der Arbeitnehmer hat auf Verlangen dem Arbeitgeber Ausdrucke der E-Mails auszuhändigen bzw. diesen den Zugang zu den E-Mails zu ermöglichen.

2.3 Kontrolle eingehender privater E-Mails

Soweit die private Nutzung des E-Mail-Dienstes gestattet ist, ist der Arbeitgeber insoweit als Anbieter von Telediensten einzuordnen und unterliegt damit in Bezug auf die Protokollierung den Vorschriften des Teledienstedatenschutzgesetzes über die Verarbeitung personenbezogener Daten. Im Hinblick auf den Inhalt der privaten E-Mails der Beschäftigten hat er auch das Fernmeldegeheimnis nach § 85 Telekommunikationsgesetz (TKG) zu wahren. Daraus folgt insbesondere, dass es ihm untersagt ist, sich oder anderen über das für die Erbringung des Dienstes erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Die Weitergabe von Informationen, die dem Fernmeldegeheimnis unterliegen, ist strafbewehrt.

Wenn die private Nutzung von E-Mail zugelassen wird, ergibt sich die Notwendigkeit, dienstliche und private E-Mails zu trennen. Hat der Mitarbeiter eine personalisierte E-Mail-Adresse nach dem Muster „Vorname.Name@Behörde.de“, so kann nicht ausgeschlossen werden, dass eingehende Mails nicht an die Behörde, sondern an den Mitarbeiter privat gerichtet sind. Dieses Problem kann dadurch gelöst werden, dass den Beschäftigten für die dienstliche und die private Benutzung von E-Mail verschiedene E-Mail-Adressen zugewiesen werden.

Unabhängig vom Aufbau und der Differenzierung der E-Mail-Adressen einer Behörde gilt, dass private E-Mails, die beim Posteingang fälschlich zunächst als dienstliche E-Mails angesehen wurden, so zu behandeln sind, wie bei der Behörde eingegangene, für einen Mitarbeiter bestimmte private Schreiben, deren privater Charakter nicht besonders, etwa durch den Zusatz „persönlich“ gekennzeichnet ist. Sobald der private Charakter dieser E-Mails erkannt wurde, sind sie unverzüglich dem betreffenden Mitarbeiter zur alleinigen Kenntnis zu geben.

2.4 Kontrolle ausgehender E-Mails

Auch bei ausgehenden E-Mails kann die automatische Kontrolle auf Virenbefall sinnvoll sein. Zwar träfe der Schaden hier den Empfänger, dies kann allerdings eine Rufschädigung der absendenden Stelle zur Folge haben. Ausgehende private E-Mails sind genauso vom Fernmeldegeheimnis geschützt wie die eingehenden, so dass die inhaltliche Überprüfung ausscheidet.

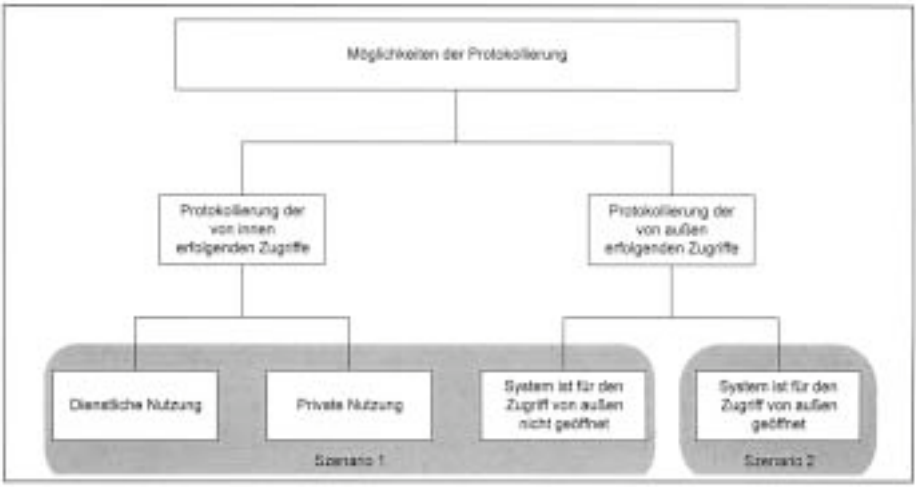
Hinsichtlich ausgehender dienstlicher E-Mails gilt grundsätzlich das oben zu den eingehenden dienstlichen E-Mails Gesagte entsprechend. Die Vertreter der Dienststelle müssen feststellen können, welche Inhalte in dienstlichen E-Mails nach außen gelangt sind. Die Kontrolle der Inhalte durch die Vorgesetzten ist daher ohne weiteres zulässig. Darüber hinausgehend wäre es technisch durch den Einsatz entsprechender Auswertungsprogramme auch möglich, z. B. anhand der Absendezeiten und Länge der E-Mails oder mit der gezielten automatischen Suche nach darin verwendeten Begriffen eine umfassende Leistungs- und Verhaltenskontrolle zu bewirken. Der Einsatz derartiger Programme stellt allerdings einen weitgehenden Eingriff in das Persönlichkeitsrecht der Beschäftigten dar und ist daher lediglich in Ausnahmefällen und auch dann nur aufgrund einer Dienstvereinbarung zulässig.

3. Protokollierung von Internet-Zugriffen mittels einer Firewall

Für Art und Umfang der Protokollierung lassen sich vor allem zwei Szenarien unterscheiden:

- Die Firewall dient lediglich der Abschottung des internen Netzes gegen das Internet, Zugriffe von außen sind grundsätzlich nicht zugelassen. In diesem Szenario kommt die Protokollierung der zulässigerweise von innen erfolgen den Zugriffe der Mitarbeiter auf das Internet in Betracht. Dabei ist zwischen den Zugriffen bei dienstlicher und bei privater Nutzung zu unterscheiden. Außerdem kann die Protokollierung dazu dienen, den Versuch eines unzulässigen Zugriffs von außen rechtzeitig zu erkennen.
- In einem anderen Szenario geht es um Zugriffe von außen auf Komponenten des internen Netzes, die dafür grundsätzlich vorgesehen sind (z. B. Web-Server). Die selbstverständlich möglichen Mischformen bleiben der Einfach heit halber außer Betracht.

Ordnet man die Maßnahmen nach ihrer Zielrichtung, ergibt sich daraus folgendes Schema:



Soweit zur Aufrechterhaltung der Datensicherheit die Protokollierung erforderlich ist, stellt sich die Frage, wie lange die dabei erzeugten Logfiles aufbewahrt werden dürfen. Dies muss für den Einzelfall entschieden werden. Die Daten sind zu löschen, sobald sie für Zwecke der Datensicherheit nicht mehr erforderlich sind.

3.1 Protokollierung der von innen erfolgenden Zugriffe (Protokollierung von Mitarbeiterdaten)

Sämtliche Maßnahmen der Inhaltskontrolle und Protokollierung sind geeignet, die Beschäftigten einer Organisation zu überwachen und ihre Leistung und ihr Verhalten zu kontrollieren. In jedem Fall muss für die Betroffenen transparent sein, welche potenziell zur Überwachung ihres Verhaltens geeigneten Maßnahmen aktiviert sind. Derartige Maßnahmen unterliegen außerdem ohne Ausnahme der Mitbestimmung der gewählten Mitarbeitervertretungen (Personalrat bzw. Betriebsrat). Da - wie im Fol-

genden dargelegt wird - eine Reihe von Einzelfragen zu klären sind, bietet es sich an, zu diesen Themen eine Dienst- bzw. Betriebsvereinbarung abzuschließen.
Vorab ist festzuhalten, dass die Protokolldaten in allen Fällen den besonderen Zweckbindungsvorschriften des § 14 Abs. 4 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG) unterliegen, soweit die Protokollierung der Aufrechterhaltung der Datensicherheit dient.
Grundsätzlich ist eine pauschale, flächendeckende und „vorbeugende" Protokollierung aller Internet-Zugriffe der Mitarbeiter zur Verhaltens- und Leistungskontrolle nicht erforderlich und damit unzulässig. Gleiches gilt auch bei der Nutzung eines Intranet. Hier sollte regelmäßig der Sperrung unerwünschter Angebote bzw. der Beschränkung des Zugriffs auf dienstlich erforderliche Angebote der Vorzug gegeben werden.
Für alle Kontrollmaßnahmen ergibt sich eine grundsätzliche Weichenstellung bei der Frage, ob den Nutzern die private Verwendung des dienstlichen Internetanschlusses erlaubt ist. Für den Dienstherrn bzw. Arbeitgeber besteht keine Pflicht, die private Nutzung zuzulassen. Ist die private Nutzung gestattet, so greift das Fernmeldegeheimnis nach § 85 TKG. Dieses umfasst den Inhalt der Telekommunikation und deren nähere Umstände (wer hat wann mit wem kommuniziert oder dies versucht?). Sämtliche Kontrollmaßnahmen sind dann nur noch unter sehr engen Voraussetzungen zulässig.

3.1.1 Dienstliche Nutzung

Beim Bereitstellen eines Internet-Zugangs für die ausschließlich dienstliche Nutzung handelt es sich nicht um einen Teledienst im Sinne des Teledienstegesetzes (TDG). Der Arbeitgeber bietet dem Arbeitnehmer keinen Dienst an, sondern stellt ihm lediglich ein Arbeitsmittel zur Verfügung; bei diesem „In-Sich-Verhältnis" fehlt das vom Teledienstegesetz vorausgesetzte Merkmal, dass es sich bei Diensteanbieter und Nutzer um zwei unterschiedliche Rechtssubjekte handelt (vgl. § 3 TDG). Damit finden die Vorschriften des Teledienstedatenschutzgesetzes auf die Protokollierung der ausschließlich dienstlichen Nutzung von Telediensten keine Anwendung.
Zulässigkeit und Umfang der Protokollierung richtet sich in diesen Fällen vielmehr nach den Vorschriften, die auf die Verarbeitung von Daten im jeweiligen Beschäftigungsverhältnis Anwendung finden, also z. B. nach dem jeweiligen Landesdatenschutz- bzw. Landesbeamtengesetz. Art und Umfang einer Protokollierung sollte durch eine Dienstvereinbarung geregelt werden.
Dagegen sollte die Protokollierung der dienstlichen Nutzung nicht auf die Einwilligung der Arbeitnehmer gestützt werden, da es auf Grund der Abhängigkeit im Beschäftigungsverhältnis häufig an der erforderlichen Freiwilligkeit der Einwilligung fehlt.
Bei der dienstlichen Nutzung hat der Arbeitgeber grundsätzlich auch das Recht zu prüfen, ob das Surfen der Mitarbeiter im WWW tatsächlich vollständig dienstlich motiviert war. Allerdings gilt hier, wie bei der Kontrolle der ausgehenden dienstlichen E-Mails, dass eine automatisierte Vollkontrolle im Hinblick auf das Persönlichkeitsrecht der Beschäftigten auf erhebliche Bedenken stößt. In jedem Fall müssen die Beschäftigten auf die geplanten Überwachungsmaßnahmen und die drohenden Sanktionen ausdrücklich hingewiesen werden.
In der Regel geht es darum zu vermeiden, dass Mitarbeiter in der Arbeitszeit und

unter Nutzung dienstlicher Ressourcen aus rein privatem Interesse auf Informationen zugreifen. Daher sollten nach Möglichkeit die bekanntesten Angebote (z. B. erotische Angebote, Spiele oder Börsenkurse) bereits gesperrt sein. Umgekehrt wäre es auch denkbar, die Zugriffe auf dienstlich erforderliche Angebote zu beschränken (Positivliste). Um weiteren Missbrauch zu verhindern, bietet es sich an, in einer Dienstvereinbarung datenschutzfreundliche Verfahren (z. B. stufenweise, zunächst nicht personenbezogene, Protokollierung der Zugriffe) festzulegen.

3.1.2 Private Nutzung

Bei der privaten Nutzung eines vom Dienstherren zur Verfügung gestellten Internet-Zuganges handelt es sich um die Nutzung eines Teledienstes im Sinne des Teledienstegesetzes. Wenn der Arbeitgeber die private Nutzung gestattet, wird er damit zum Dienstanbieter im Sinne des § 3 des TDG. Art und Umfang der Protokollierung von Nutzungs- und Abrechnungsdaten richten sich nach § 6 des TDDSG. Außerdem gilt das Fernmeldegeheimnis aus § 85 TKG. Sind bestimmte Protokollierungen aus technischer Sicht für die Aufrechterhaltung eines regelgerechten Firewall-Betriebs unabdingbar, können sie ergänzend auf § 9 BDSG nebst Anlage bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze gestützt werden.

3.2 Protokollierung der von außen (aus dem Internet) erfolgenden Zugriffe

3.2.1 Nur Anschluss des internen Netzes an das Internet; keine Angebote der öffentlichen Stelle nach außen

In diesen Fällen ist die Firewall nicht Bestandteil eines Tele- bzw. Mediendienstes. Die Vorschriften des Teledienstegesetzes bzw. des Teledienstedatenschutzgesetzes finden daher keine Anwendung.
Zulässigkeit und Umfang der Protokollierung richten sich nach § 9 BDSG und Anlage. Für öffentliche Stellen des Bundes kommt als Rechtsgrundlage § 14 BDSG in Betracht; in den Ländern ggf. entsprechende Vorschriften der Landesdatenschutzgesetze.

3.2.2 Angebot nach außen (Web-Server)

Soll über eine Firewall der Zugriff auf einen Web-Server einer öffentlichen Stelle aus dem Internet reguliert werden, so bemisst sich die rechtliche Einordnung der Firewall nach der Einordnung des Angebots, das die öffentliche Stelle auf dem betreffenden Web-Server macht.
Dabei kann es sich - je nach Art des Angebotes - entweder um einen Teledienst im Sinne des Teledienstegesetzes handeln, aber auch um einen Mediendienst nach dem Mediendienste-Staatsvertrag (MDStV). Zulässigkeit und Umfang der Protokollierung von Nutzungs- und Abrechnungsdaten richten sich nach § 6 TDDSG bzw. § 15 MDStV.
Für Zwecke der Datensicherung kann die Protokollierung auf § 9 BDSG und Anlage bzw. für öffentliche Stellen des Bundes ergänzend auf § 14 BDSG, in den Ländern auf entsprechende Vorschriften der Landesdatenschutzgesetze gestützt werden.
Die Protokollierung ist dabei auf das unabdingbar Notwendige zu begrenzen; der Anbieter unterliegt hier den Verpflichtungen zur datenarmen Gestaltung des Tele- bzw. Mediendienstes gemäß § 3 Abs. 4 TDDSG bzw. § 13 Abs. 5 MDStV.
Soweit die Protokollierung personenbezogen erfolgt, unterliegt der Anbieter darüber

hinaus den Informationspflichten nach § 3 Abs. 5 TDDSG bzw. § 12 Abs. 6 MDStV auch hinsichtlich der Protokollierung personenbezogener Daten auf der Firewall.
Soweit die Daten zur Gewährleistung der Datensicherheit oder des Datenschutzes gespeichert werden, unterliegen sie der besonderen Zweckbindung nach § 14 Abs. 4 BDSG bzw. den entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG).
In dieser Konstellation kann die Protokollierung an der Firewall nicht auf die Einwilligung des bzw. der Betroffenen gestützt werden, da eine rechtswirksame Einholung der Einwilligung von Betroffenen auf Grund der technischen Gegebenheiten im Internet nicht möglich ist.

V. Auswahl und Umsetzung der Sicherungsmaßnahmen; Betriebsphase

1. Security Policy und Sicherheitskonzept

Aus den Anforderungen der im Vorfeld gemachten Sicherheitsbetrachtungen der Kommunikations- und der Risikoanalyse ist ein Regelwerk zu erstellen. In dieser Security Policy sind die Rahmenbedingungen zur Einrichtung, zum Betrieb und zur Verwaltung der Systeme für die interne Kommunikation und die Verbindungen zum Internet festzulegen.
Die Zuständigkeiten für Betrieb, Verwaltung und Administration der für den Verbund eingesetzten Kommunikationssyteme müssen aufeinander abgestimmt sein. Es müssen die notwendigen Maßnahmen aufgeführt werden, die dem Schutz nach innen und außen dienen. Bereiche mit sensiblen Datenbeständen müssen besonders berücksichtigt werden.
In Bezug auf die Firewall sollte die Security Policy folgende Festlegungen enthalten:

- Was soll geschützt werden?
- Welche Dienste sind erforderlich?
- Welche Benutzer werden zugelassen?
- Welche Ereignisse werden protokolliert und wer wertet diese Daten aus?
- Welcher Datendurchsatz ist zu erwarten?

Da die Sicherheit des Gesamtsystems nicht allein von der Firewall bestimmt wird, sind in die Security Policy auch flankierende Vorgaben aufzunehmen, wie das Verbot von zusätzlichen Netzzugängen, z. B. per Modem oder ISDN, Virenschutz und Backup-Konzept.
Basierend auf der Security Policy ist ein Sicherheitskonzept zu erstellen, welches die Vorgaben in konkrete Maßnahmen (Konfigurationen, Filterregeln etc.) umsetzt.

Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist das Vorliegen einer schlüssigen Security Policy und eines davon abgeleiteten Sicherheitskonzepts sowie dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

2. Auswahl, Konfiguration und Wartung von Firewall-Systemen

Firewall-Systeme müssen transparent und einfach aufgebaut sein. Mit zunehmender Komplexität steigt auch die Wahrscheinlichkeit von Fehlern. Nicht für den Betrieb der Firewall benötigte Anwendungen und Systemprogramme sind daher zu löschen.

Auch die Bedienung und die Konfiguration der Firewall müssen benutzungsfreundlich realisiert sein, da sonst unbeabsichtigte Fehleinstellungen Sicherheitseinbußen mit sich bringen. Vertrauenswürdige Systeme müssen ihre Funktionsweise offen Legen, denn nur dann ist es Experten möglich, Hintertüren auszuschließen und die Gefahr von Sicherheitslücken fundiert zu diskutieren. Sicherheitszertifikate für Firewalls können dazu beitragen, dass sich der Grad des Schutzes, den das jeweilige Produkt bietet, leichter einschätzen lässt und Vergleiche zwischen verschiedenen Produkten möglich werden.
Durch den Einsatz verschiedener Produkte, die unabhängig voneinander entwickelt wurden und arbeiten, lässt sich das Sicherheitsniveau steigern. „Monokulturen" sollten vermieden werden, denn wenn ein Angreifer einen bisher unentdeckten Fehler ausnutzt, kann dort leicht der gesamte Schutzwall zusammenbrechen.
Bei der Konfiguration einer Firewall folgt man am besten der Regel: „Alles, was nicht ausdrücklich erlaubt ist, ist verboten." Wenn man bei der Definition der Regeln etwas übersehen hat, wird nur die Funktionalität und nicht die Sicherheit eingeschränkt. Während man eine Einschränkung der Funktionalität im Bedarfsfall schnell merkt, bleiben Einbußen in der Sicherheit oft unerkannt.
Es gibt keine 100%ige Sicherheit. Hinzu kommt, dass sich meist im Laufe der Zeit die Stärke der Sicherheit verringert, z. B. durch Entdeckung von Fehlern, Herausbildung neuer Angriffsformen oder auch Verbesserung der Systemausstattung von Angreifern. Unverzichtbar ist es daher, eine ausreichende und fortlaufende Betreuung des eingesetzten Firewall-Systems durch qualifiziertes Personal zu gewährleisten. Die Administratoren sollten ständig die Diskussion um Sicherheitslücken verfolgen und sich auch weiterbilden. Das Sicherheitsniveau des Firewallsystems ist regelmäßig neu zu bewerten, damit die Systeme auf den aktuellen Stand gebracht werden.
Treten neue Bedrohungen auf, so ist die Kommunikations- und Risikoanalyse entsprechend zu aktualisieren. Eine solche Anpassung ist auch notwendig, wenn beabsichtigt ist, bisher nicht vorgesehene Internetdienste zur Verfügung zu stellen. Die Firewallsoftware ist laufend zu aktualisieren. Falls notwendig, ist das Firewallsystem umzukonfigurieren oder es sind einzelne Module oder die gesamte Firewall auch außerplanmäßig auszutauschen.
Da nicht alle Angriffsversuche auf das lokale Netz von der Firewall vollständig abgeblockt werden können, ist durch die Systemadministration der laufende Betrieb der Firewall zu überwachen. Dazu müssen die Protokolle regelmäßig ausgewertet werden, um auch solche Angriffsversuche zu entdecken, die durch die Firewall nicht abgewiesen werden können. Es ist dafür zu sorgen, dass dringende Warnmeldungen der Firewall der Bedrohungslage angemessen konfiguriert sind. Ferner müssen diese Meldungen das Wartungspersonal unverzüglich erreichen und zeitnah behandelt werden.
Die Firewalladministration kann nicht losgelöst von der Verwaltung des (lokalen) Verwaltungsnetzes gesehen werden. Kommen beispielsweise Benutzerinnen und Benutzer hinzu, scheiden sie aus oder wechseln sie ihr Aufgabengebiet, so kann sich daraus eine Veränderung in den zur Verfügung zu stellenden Diensten ergeben. Dies erfordert eine entsprechende Aktivität der Firewalladministration. Umgekehrt hat die lokale Administration den Schwachstellen im lokalen Netz besondere Aufmerksamkeit zu schenken, die durch Angriffe von außen ausgenutzt werden können.
Werden aufgrund der Größe oder Struktur der Verwaltungseinheit auch zwischen

verschiedenen Teilen dieser Einheit Firewalls eingesetzt, so können bestimmte Aufgaben der Firewall-Administration sinnvoll zentralisiert werden. Insbesondere zählen dazu diejenigen Tätigkeiten, die unabhängig von der Rechteverwaltung der einzelnen Benutzerinnen und Benutzer sind.

3. Rahmenbedingungen für Konfiguration und Betrieb

Sind bereits für die Planung und Einführung eines Firewall-Systems[1] eine Vielzahl von Fragestellungen hinsichtlich technischer, organisatorischer, planerischer und rechtlicher Art zu beachten, kommen während der Betriebsphase weitere Problemkreise hinzu, die durch den Betreiber, ggf. in Abstimmung mit den Benutzern bzw. deren Personalvertretung, zu beantworten sind.
Da die in diesem Zusammenhang zu treffenden Maßnahmen teilweise auch auf die Planungs- und Einführungsphase zurückwirken, sollte auch die Betriebsphase der Firewall bereits frühzeitig berücksichtigt werden. Die rechtlichen Rahmenbedingungen ergeben sich aus Kapitel IV.
Typische Anforderungen während des Betriebs eines Firewall-Systems sind:

A1 Schutz des ordnungsgemäßen Betriebs der Firewall, d. h. der Durchlässigkeit für zugelassenen Netzverkehr einerseits und der Undurchlässigkeit für nicht zugelassenen Netzverkehr andererseits (eingehend oder ausgehend),

A2 Schutz des internen Netzes vor Angriffen von außen, sowohl bezogen auf online-Angriffe als auch auf offline-Angriffe (z. B. durch eingeschleuste Viren),

A3 Schutz vor einer unzulässigen bzw. rechtswidrigen Nutzung der Firewall, sei es von außen (z. B. Hacking) oder von innen (z. B. unerlaubte private Nutzung oder unzulässiger Zugriff auf für dienstliche Zwecke nicht erforderliche Informationsangebote),

A4 die rechtliche, organisatorische und technische Differenzierung zwischen der dienstlichen und der privaten Nutzung des Internet-Anschlusses, soweit eine außerdienstliche Nutzung überhaupt zugelassen wird,

A5 Abrechnung von Leistungen, die durch die Firewall erbracht werden,

A6 Statistische Auswertungen der Firewall-Benutzung z. B. zur Angebotsoptimierung.

Um diese Anforderungen umzusetzen, stehen - im Wesentlichen unabhängig von der technischen Entwicklung oder einer rechtlichen Beurteilung - folgende technisch-organisatorische Maßnahmen zur Verfügung:

M1 Gestaltung der Netzzugangspolicy und der Betriebsparameter der Firewall allgemein,

M2 Auswertung der Inhalte übertragener Daten (z. B. hinsichtlich eines potentiellen Virenbefalls),

M3 Auswertung der Verbindungsdaten, insbesondere der URL (z. B. hinsichtlich Datenvolumen, Adressen).

[1] Mit Firewall-System ist nicht nur die Firewall im eigentlichen Sinne, sondern auch das System, das den Zugang zum Internet ermöglicht gemeint. So sollten auf der Firewall selbst keinerlei Accountingfunktionen laufen. Diese können aber im Zugangssystem integriert sein.

Dabei ergibt sich grundsätzlich folgende Eignungsmatrix für die genannten Maßnahmen, wobei die rechtliche Zulässigkeit der jeweiligen Maßnahme im Einzelfall zu prüfen bleibt:

	A1	A2	A3	A4	A5	A6
M1	x	x	x	x	x	x
M2	-	x	x	x	-	-
M3	x	x	x	-	x	x

4. Empfehlungen für den Betrieb einer Firewall

Die nachfolgenden Empfehlungen gelten unabhängig davon, ob öffentliche Stellen selbst die Internet-Dienste anbieten oder ob sie sich dabei eines Providers bedienen.

- Aufgrund der rechtlich unterschiedlichen Bewertung der Datenübertragung für eigene Zwecke der Stelle einerseits und für Dritte andererseits sowie der damit verbundenen praktischen Konsequenzen sollte in einer Dienst- oder Betriebsvereinbarung klar geregelt werden, ob und wenn ja welche Dienste zur privaten Nutzung freigegeben sind.
- Im Hinblick darauf, dass bei behörden- und unternehmensinternen Systemen Mitbestimmungstatbestände erfüllt sind (Verhaltens- und Leistungskontrolle), müssen die Personalvertretungen und Betriebsräte schon bei der Planung und Einführung von Firewallsystemen und insbesondere der Protokollierung beteiligt werden. Gegebenenfalls müssen entsprechende Betriebs- oder Dienstvereinbarungen abgeschlossen werden, in denen das Verfahren der Protokollierung, der Kontrolle und der Auswertung der Protokolle verbindlich geregelt wird. Eine Einwilligung der Arbeitnehmer als Grundlage für die Protokollierung der dienstlichen Nutzung ist abzulehnen.
- Bei Datenübertragung für eigene Zwecke der Stelle sind die Mitarbeiter auf die Art und den Umfang technischer Kontrollen hinzuweisen, damit sie ihr Nutzerverhalten entsprechend steuern können; ferner müssen sie darüber informiert werden, welche Folgen es hat, wenn Nachrichten ausgefiltert werden.
- Zur Durchsetzung des Verbots einer privaten Nutzung oder des Zugriffs auf unerwünschte Adressen sollte grundsätzlich auf eine Protokollierung verzichtet werden. Die Durchsetzung dieses Verbots sollte so weit möglich durch die Beschränkung der Zugriffe auf dienstlich erforderliche Angebote (Positivliste) oder über die Sperrung der unerwünschten Adressen versucht werden. Zugriffsversuche auf gesperrte Adressen sollten protokolliert werden. Für erforderliche Protokollierungen sollte in der Dienstvereinbarung ein stufenweises, zunächst nicht personenbezogenes Verfahren festgelegt werden.
- Eine vollständige Protokollierung aller Internetzugriffe der Mitarbeiter zur Verhaltens- und Leistungskontrolle ist grundsätzlich nicht erforderlich und damit unzulässig.
- Die erlaubte private Nutzung des Internet-Zugangs unterliegt dem Fernmeldegeheimnis nach § 85 TKG. Für die Protokollierung gelten § 6 TDDSG und § 9 BDSG. Sie darf danach grundsätzlich nur insoweit erfolgen, als es für die Abrech-

nung der Dienste oder zur Aufrechterhaltung eines regelgerechten Firewallbetriebs unerlässlich ist.

- Die Protokollierung der von außen (aus dem Internet) erfolgenden Zugriffe oder Zugriffsversuche, die einen Angriff darstellen, ist im Rahmen von §§ 9, 14 BDSG bzw. der entsprechenden Normen der Landesdatenschutzgesetze zulässig. Darüber hinaus ist eine derartige Protokollierung auch erlaubt, wenn sie zum Erkennen potentieller Angriffe erforderlich ist.
- Für die Protokollierung der Zugriffe von außen auf Informationsangebote für die Öffentlichkeit gelten - in Abhängigkeit von der Art des Dienstes - § 6 TDDSG bzw. § 15 MDStV hinsichtlich der Nutzungs- und Abrechnungsdaten. Der Nutzer muss auf der entsprechenden Web-Site über den Umfang der Protokollierung informiert werden.
- Jede nach den voranstehenden Ausführungen zulässige Protokollierung ist so auszugestalten, dass ein datenschutzrechtlicher Missbrauch vermieden wird, d. h.:
  - der Umfang der Protokolle sollte im Rahmen des Möglichen minimal sein,
  - aufgrund der Datenschutzgesetze (z. B. § 14 Abs. 4 BDSG) dürfen Protokolldaten nicht für andere Zwecke verwendet werden,
  - Protokolle sind durch Zugriffsmaßnahmen gegen unbefugte Kenntnisnahme zu sichern,
  - es sind technisch-organisatorische Auswertungsverfahren festzulegen,
  - es sind möglichst kurze Löschfristen vorzusehen.
- Bei eingehenden Daten, beispielsweise E-Mails, sind, unabhängig davon, ob sie dienstlicher oder privater Natur sind, automatisiert ablaufende zentrale und dezentrale Virenchecks zulässig und angezeigt. Dies gilt auch dann, wenn die Daten im Auftrag verarbeitet werden. Dabei ist zu beachten, dass
  - nur eine automatisierte Kontrolle ohne regelmäßige Kenntnisnahme des Kontrollvorgangs oder -ergebnisses durch Administratoren o. Ä.. erfolgt,
  - das Inhalts-Scanning auf fest definierte Pattern (Virensignaturen) begrenzt und das Scanning nach frei wählbaren Textstellen ausgeschlossen ist,
  - der Betroffene über das Auffinden von Viren in einer für ihn bestimmten Nachricht unterrichtet wird und mit dieser nur unter seiner Beteiligung oder nach Rücksprache umgegangen wird.
- Private E-Mails der Beschäftigten unterliegen dem Fernmeldegeheimnis. Ihre Kenntnisnahme durch den Arbeitgeber über das für die Erbringung des Dienstes erforderliche Maß ist daher unzulässig.
- Der Einsatz von Programmen zur Auswertung von E-Mails ist wegen des damit verbundenen weitgehenden Eingriffs in das Persönlichkeitsrecht der Beschäftigten nur zulässig, wenn die folgenden drei Voraussetzungen kumulativ gegeben sind:
  - es handelt sich ausschließlich um dienstliche E-Mails,
  - das Vorgehen ist in einer Dienstvereinbarung geregelt,
  - es liegt ein die Auswertung rechtfertigender Ausnahmefall vor.
- Bei Datenübertragung für Dritte sind Inhaltskontrollen nur im Auftrag bzw. mit der Einwilligung des Betroffenen zulässig (Bei der zulässigen privaten Nutzung kommt u. U. auch eine generelle Einwilligung durch den Personal- oder Betriebsrat in Betracht. Die Betroffenen sind hierüber ausführlich zu informieren.), wobei dem Auftraggeber (z. B. beim Outsourcing) Gestaltungsmöglichkeiten hinsicht-

lich folgender Aspekte einzuräumen sind:
- Nutzung bzw. Umfang der Inhaltskontrolle,
- technische und organisatorische Folgen bei ausgefilterten Nachrichten.

VI. Ausblick

In der Vergangenheit war das Design und die Weiterentwicklung der TCP/IP-Protokollfamilie nicht an Zielen wie IT-Sicherheit oder Datenschutz ausgerichtet; lediglich die Ausfallsicherheit von Netzwerken ist als Designkriterium erkennbar und durchgehalten. Inzwischen werden in den einschlägigen RFCs jedoch eine Reihe von sicherheitsrelevanten Problemen behandelt. Um die Dynamik dieses Prozesses zu verdeutlichen, sei hier auf eine zentrale und für die Entwicklung der Firewallsysteme besonders bedeutsame Neuerung hingewiesen, nämlich die Sicherheitsmerkmale (IPSec) der IP-Version 6 (IPv6). Sie sollen eine konsistente Lösung einer Reihe von Sicherheitsproblemen mit IPv4 ermöglichen.

IPSec wird die wesentlichen Dienste Authentifikation und Vertraulichkeitssicherung implementieren. So wird auch ein Modus zur Vertraulichkeitssicherung verfügbar sein, bei dem komplette IP-Pakete verschlüsselt und mit einem neuen IP-Header versehen werden (sog. tunnel mode). Wird ein solches Verfahren in einem Gateway oder einer Firewall implementiert, so kann dadurch nicht nur der unbefugte Zugriff auf die Inhalte der Datagramme vermieden, sondern auch die Verkehrsflussanalyse erschwert werden. Denn die IP-Pakete tragen lediglich die Absenderadresse des Gateways oder der Firewall und aus dem Inhalt der Datagramme kann auch kein Rückschluss gezogen werden. Verbindungen dieser Art zwischen Firewalls eignen sich zur Kopplung von LANs eines VPN. Die Migration zu einer solchen Lösung gestaltet sich problemlos, da keine weiteren (insbesondere konzeptionellen) Änderungen nötig sind.

Sollen jedoch andere Szenarien als diese Art von VPN realisiert werden, sind weitere Probleme zu lösen. Zum einen ist eine Schlüsselverwaltung notwendig, die den Zugriff auf Authentifikationsschlüssel bisher unbekannter Partner ermöglicht. Eine solche Infrastruktur ist jedoch kein originäres Problem von IPSec, sondern wird in gleicher Weise für die Sicherung der Zurechenbarkeit etwa von elektronischer Post oder von HTTP-Verbindungsinhalten benötigt. Darüber hinaus lassen sich IP-Datagramme im tunnel mode auch durch eine Firewall senden, ohne dass diese die Datagramme in der bisher üblichen Weise analysieren kann. Hier stellt sich die Frage, ob man der Firewall erlauben sollte, die Pakete mitzulesen und ihr das Schlüsselmaterial zur Verfügung zu stellen oder nicht. Die erste Alternative erfordert ein hohes Maß an Hostsicherheit, stellt dafür aber eine echte, gegen Abhören auf dem gesamten Transportweg kryptographisch gesicherte Ende-zu-Ende-Verbindung dar. Im zweiten Fall bestehen an den beteiligten Firewalls Abhörmöglichkeiten, dafür kann die Firewall aber bestimmte Angriffe abwehren, die sonst erst beim Host erkennbar und behandelbar sind.

Neben den Protokollneuerungen im Rahmen der Version 6 des Internet Protocol sind noch weitere Änderungen zu erwarten. Das betrifft Fragen, die sich aus Protokollerweiterungen für mobile Teilnehmer ergeben, ebenso wie Probleme im Zusammenhang mit der Sicherung von Hochgeschwindigkeitsverbindungen.

Festzuhalten bleibt, dass der Anschluss von Netzen der öffentlichen Verwaltung an das Internet nur dann das Attribut datenschutzgerecht verdient, wenn auf die

sicherheitsrelevanten Entwicklungen auf dem Gebiet von Internet-Protokollen und -Werkzeugen bis hin zur Endgerätesicherheit zeitnah und adäquat reagiert wird.

Abkürzungsverzeichnis

ARP	Address Resolution Protocol
BDSG	Bundesdatenschutzgesetz
CGI	Common Gateway Interface
DMZ	Demilitarisierte Zone
DNS	Dynamic Name Service
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocols
IP	Internet Protocoll
MDStV	Mediendienste-Staatsvertrag
NFS	Network File System
SSH	secure shell
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
WWW	Word wide Web

16 Materialien

16.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.1.1 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 in Hannover zu den Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o. Ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich geprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.

- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind - es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann – zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden – nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden. Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o.g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum – ausschließlich zum Zweck der Sicherung des Rechtsschutzes – aufzubewahren.

- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung). Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen. Damit sind Regelungen z. B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann. Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.

- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.

- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.

- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung – bei Datenübermittlungen auch bei den Datenempfängern – erstrecken.

- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.

- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.

- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

16.1.2 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 in Hannover zu Data Warehouse, Data Mining und Datenschutz

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an.
Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse“ werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining“ bietet Werkzeuge, die die scheinbar zusammenhangslosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus“ gesammelt werden.

- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden sind. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.

- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.

- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.

- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern“ rechtswidrig.

- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining“ ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse“- und „Data Mining“-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

16.1.3 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 in Hannover: Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu“ eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderllichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere“ jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung“. Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten“, nicht die einzelne Person und auch nicht das „Gesamtbild einer Person“. Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

16.1.4 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 in Hannover zum Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,

- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,

- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,

- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

16.1.5 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 in Hannover: Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

Erhebliche Zunahme der Telekommunikationsvorgänge

Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, E-Mail und Mailboxen sowie das Internet genutzt.

Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten

- Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.

- Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch E-Mail-Adresse, IP-Nummer oder domain name gehören. So

können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.

- Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.

- Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.

- Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten

Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

Entwicklung des Internets zum Massenkommunikationsmittel

Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

Schwer durchschaubare Rechtslage

Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: 1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802

- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.

- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen „ENFOPOL“, befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.

- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.

- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffe-

nen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.

- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.

- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.

- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäusern oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungsverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.

- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

16.1.6 Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 in Hannover zu den Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und derLänder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozeßrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der

Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener – insbesondere biometrischer – Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch *öffentliche Stellen* dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

   - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen – soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen – unter anderem in Betracht*:

   - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.*

   - *für die Verkehrslenkung nur Übersichtsaufnahmen,*
   - *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*

- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chan-

cen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

Muster

Niederschrift über die Vereidigung

_____

(Behörde)

_____

(Amts- oder Dienstbezeichnung, Vor- und Zuname)

Dem Beamten/der Beamtin wurde der Inhalt des Diensteides gemäß § 70 SächsBG bekanntgegeben (Auszug):

„§ 70 Diensteid.
(1) Der Beamte hat folgenden Diensteid zu leisten:
„Ich schwöre, dass ich mein Amt nach bestem Wissen und Können führen, Verfassung und Recht achten und verteidigen und Gerechtigkeit gegenüber allen üben werden."

(2) Der Eid kann auch mit der Beteuerung „So wahr mir Gott helfe" geleistet werden.

(3) Gestattet ein Gesetz den Mitgliedern einer Religionsgemeinschaft, an Stelle der Worte „ich schwöre" andere Beteuerungsformeln zu gebrauchen, so kann der Beamte, der Mitglied einer solchen Religionsgemeinschaft ist, diese Beteuerungsformel sprechen."

Er/Sie wurde auf die Bedeutung des Diensteides hingewiesen.

Der Diensteid wurde ordnungsgemäß geleistet.

_____

Ort, Datum

Bestätigt:

_____

Unterschrift
Beamter/Beamtin

_____

Unterschrift
Behördeneleiter/in oder
Beauftragter/Beauftragte