Sächsischer Landtag DRUCKSACHE 3/6775

3. Wahlperiode

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

10. Tätigkeitsbericht
des
Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31. März 2002

gemäß § 27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 17. Oktober 2002 Ausgegeben am: 17. Oktober 2002

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

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

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

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

Besucheranschrift: Devrientstraße 1
01067 Dresden

Vervielfältigung erwünscht.

Herstellung: OTTO Verlag & Druckerei 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.

ALG	Gesetz über die Alterssicherung der Landwirte vom 29. Juli 1994 (BGBl. I S. 1890)
ArbZG	Arbeitszeitgesetz vom 6. Juni 1994 (BGBl. I S. 1170, 1171), zuletzt geändert durch Artikel 35 des Gesetzes vom 21. Dezember 2001 (BGBl. I S. 1983)
ASiG	Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit vom 12. Dezember 1973 (BGBl. I S. 1885), zuletzt geändert durch Artikel 32 des Gesetzes vom 21. Dezember 2000 (BGBl. I S. 1983)
BAT-O	Bundes-Angestelltentarifvertrag Ost in der in den neuen Ländern geltenden Fassung
BDSG	Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Bundesdatenschutzgesetz)
BGB	Bürgerliches Gesetzbuch
BJagdG	Bundesjagdgesetz in der Fassung der Bekanntmachung zur Neufassung vom 29. September 1976 (BGBl. I S. 2849), zuletzt geändert durch Artikel 10 des Gesetzes vom 14. Dezember 2001 (BGBl. I S. 3714)
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)

DRiG	Deutsches Richtergesetz in der Fassung der Bekanntmachung vom 19. April 1972 (BGBl. I S. 713), zuletzt geändert durch Artikel 10 des Gesetzes vom 9. Juli 2001 (BGBl. I. S. 1510)
EG-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbebezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 (ABl. EG L 281 vom 23. November 1995, S. 31)
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EStG	Einkommensteuergesetz
GeschlKrG	Gesetz zur Bekämpfung von Geschlechtskrankheiten vom 23. Juli 1953 (BGBl. I S. 700; BGBl. III 2126-4), zuletzt geändert durch Art. 7 des Gesetzes zur Reform des Rechts der Vormundschaft und Pflegschaft für Volljährige vom 12. September 1990 (BGBl. I S. 2002)
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz)
GVO	Verordnung über den Verkehr mit Grundstücken (Grundstücksverkehrsordnung [früher Grundstücksverkehrsverordnung - GVVO]) vom 15. Dezember 1977 (DDR-GBl. I 1978 Nr. 5 S. 73) in der Fassung der Bekanntmachung vom 18. April 1991 (BGBl. I S. 999), geändert durch Art. 4 des 2. VermRÄndG vom 14. Juli 1992 (BGBl. I S. 1257, 1266), neu gefaßt durch Art. 15 § 1 des Registerverfahrensbeschleunigungsgesetzes vom 20. Dezember 1993 (BGBl. I S. 2182, 2221), geändert durch Art. 2 des Gesetzes vom 4. Juli 1995 (BGBl. I S. 895) sowie zur Umstellung von Vorschriften auf Euro vom 27. Juli 2000 (BGBl. I S. 897)
KomWG	Gesetz über die Kommunalwahlen im Freistaat Sachsen (Kommunalwahlgesetz - KomWG) vom 18. Oktober 1993 (GVBl. S. 937), zuletzt geändert durch Gesetz vom 28. Juni 2001 (GVBl. S. 426)

Krw-/AbfG	Gesetz zur Förderung der Kreislaufwirtschaft und Sicherung der umweltverträglichen Beseitigung von Abfällen (Kreislaufwirtschafts- und Abfallgesetz) vom 27. September 1994 (BGBl. I S.2705), zuletzt geändert durch Art. 57 der Verordnung vom 29. Oktober 2001 (BGBl. I. S.2785)
LSVOrgG	Gesetz zur Organisationsreform der landwirtschaftlichen Sozialversicherung vom 17. Juli 2001 (BGBl. I S. 1600)
MDStV	Entwurf eines Staatsvertrages über Mediendienste - Mediendienste-Staatsvertrag
MRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (BGBl. 1952 II S. 685)
Ordensgesetz	Gesetz über Titel, Orden und Ehrenzeichen vom 26. Juli 1957 (BGBl. I S. 844), zuletzt geändert durch Artikel 3 des Gesetzes vom 18. Juni 1997 (BGBl. I S. 1430)
RöV	Verordnung über den Schutz vor Schäden durch Röntgenstrahlen (Röntgenverordnung) vom 8. Januar 1987 (BGBl. I S. 114), zuletzt geändert durch Artikel 11 der Strahlenschutzverordnung (StrlSchV) vom 20. Juli 2001 (BGBl. I S. 1714)
SachenRBerG	Gesetz zur Sachenrechtsbereinigung im Beitrittsgebiet (Sachenrechtsbereinigungsgesetz) vom 21. September 1994 (BGBl. I S. 2457), zuletzt geändert durch Gesetz vom 26. November 2001 (BGBl. I S. 3138)
SächsABG	Sächsisches Abfallwirtschafts- und Bodenschutzgesetz in der Fassung der Bekanntmachung vom 31. Mai 1999 (GVBl. S. 261), geändert durch Art. 21. des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBL. S. 426)
SächsAGVermG	Sächsisches Gesetz zur Ausführung des Vermögensgesetzes vom 24. August 2000 (GVBl. S. 160), zuletzt geändert durch Gesetz vom 28. Juni 2001 (GVBl. S. 426)
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 Gesetz vom 28. Juni 2001 (GVBl. S. 426)
SächsBG	Beamtengesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 370, berichtigt durch Bekanntmachung vom 16. Dezember 1999 GVBl. 2000 S. 7)
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)
SächsFFStatVO	Verordnung der Sächsischen Staatsministerin für Fragen der Gleichstellung von Frau und Mann über die statistischen Angaben für die Frauenförderung in Dienststellen im Freistaat Sachsen (Sächsische Frauenförderungsstatistikverordnung) vom 22. August 1995 (GVBl. S. 295)
SächsGDG	Gesetz über den öffentlichen Gesundheitsdienst im Freistaat Sachsen (Sächsisches Gesundheitsdienstgesetz) vom 11. Dezember 1991 (GVBl. S. 413), geändert durch Art. 15 des 2. Gesetzes zur Euro-bedingten Änderung des Sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)
SächsGemO	Gemeindeordnung für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 14. Juni 1999 (GVBl. S. 345), zuletzt geändert durch Änderungsgesetz vom 28. Juni 2001 (GVBl. S. 425) und durch Art. 9 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)
SächsGKV	Gesetz über den kommunalen Versorgungsverband Sachsen in der Fassung der Bekanntmachung vom 16. Januar 1997 (GVBl. S. 74), zuletzt geändert durch Gesetz vom 17. Februar 1999 (GVBl. S. 46)
SächsHG	Gesetz über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz) vom 11. Juni 1999 (GVBl. S. 294), zuletzt geändert durch Art. 26 des Gesetzes vom 28. Juni 2001 (GVBl. S. 426)

SächsKAG	Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (GVBl. S. 502), geändert durch Art. 57 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426
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)
SächsKomZG	Sächsisches Gesetz über die kommunale Zusammenarbeit vom 19. August 1993 (GVBl. S. 815, berichtigt GVBl. 1993 S. 1103), zuletzt geändert durch Art. 7 des Gesetzes zur Änderung verschiedener Vorschriften des Sächsischen Landesrechts vom 25 Juni 1999 (GVBl. S. 398)
SächsLJagdG	Sächsisches Landesjagdgesetz vom 8. Mai 1991 (GVBl. S. 67), zuletzt geändert durch Art. 50 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)
SächsLKrO	Landkreisordnung für den Freistaat Sachsen vom 19. Juli 1993 (GVBl. S. 577), zuletzt geändert durch Art. 10 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28 Juni 2001 (GVBl. S. 426)
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 in der Fassung der Bekanntmachung vom 11. April 1997 (GVBl. S. 377), geändert durch Art. 4 des Gesetzes zum 4. Staatsvertrag rundfunktrechtlicher Staatsverträge vom 16. März 2000 (GVBl. S. 89)
SächsPetAG	Gesetz über den Petitionsausschuss des Sächsischen Landtages (Sächsisches Petitonsausschussgesetz) vom 11. Juni 1991 (GVBl. S. 90)

SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (GVBl. S. 466)
SächsPresseG	Sächsisches Gesetz über die Presse vom 3. April 1992 (GVBl. S. 125), geändert durch Art. 30 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (GVBl. S. 453), geändert durch Art. 2 des Gesetzes von 12. Februar 1999 (GVBl. S. 49) und durch Art. 36 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (GVBl. S. 243)
SächsVwZG	Verwaltungszustellungsgesetz für den Freistaat Sachsen vom 21. April 1993 (GVBl. S. 362 ber. in GVBl. 1995 S. 182)
SächsWG	Sächsisches Wassergesetz in der der Fassung der Bekanntmachung vom 21. Juli 1998 (GVBl. S. 393), zuletzt geändert durch Art. 44 des 2. Gesetzes zur Euro-bedingten Änderung des sächsischen Landesrechts vom 28. Juni 2001 (GVBl. S. 426) und durch § 9 SächsEntEG vom 18. Juli 2001 (GVBl. S. 453)
SGB I	Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Gesetz vom 5. November 2001 (BGBl. I S. 2950)
SGB III	Sozialgesetzbuch (SGB) Drittes Buch (III) - Arbeitsförderung – vom 24. März 1997 (BGBl. I S. 594, zuletzt geändert durch Gesetz vom 23. März 2002 (BGBl. I S 1130)
SGB IV	Sozialgesetzbuch (SGB) Viertes Buch (IV) - Gemeinsame Vorschriften für die Sozialversicherung - vom 23. Dezember 1976 (BGBl. I S. 3845), zuletzt geändert durch Gesetz vom 10. Dezember 2002 (BGBl. I S. 3443)
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - vom 20. Dezember 1988 (BGBl. I

	S. 2477), zuletzt geändert durch Gesetz vom 23. März 2002 (BGBl. I S. 1169)
SGB VI	Sozialgesetzbuch (SGB) Sechstes Buch (VI) - Gesetzliche Rentenversicherung – in der Fassung der Bekanntmachung vom 19. Februar 2002 (BGBl. I S. 754)
SGB VII	Siebentes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung - vom 7. August 1996 (BGBl. I S. 1254), zuletzt geändert durch Gesetz vom 13. September 2001 (BGBl. I S. 2376)
SGB VIII	Sozialgesetzbuch (SGB) Achtes Buch (VIII) - Kinder- und Jugendhilfe - in der Fassung der Bekanntmachung vom 8. Dezember 1998 (BGBl. I S. 3546), zuletzt geändert durch Gesetz vom 19. Juni 2001 (BGBl. I S. 1046)
SGB IX	Sozialgesetzbuch (SGB) Neuntes Buch (IX) – Rehabilitation und Teilhabe behinderter Menschen – vom 19. Juni 2001 (BGBl. I S. 1046), geändert durch Gesetz vom 10. Dezember 2001 (BGBl. I S. 3443)
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 9. Januar 2002 (BGBl. I S. 363)
SGB XI	Sozialgesetzbuch (SGB) Elftes Buch (XI) - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014), zuletzt geändert durch Gesetz vom 14. Dezember 2001 (BGBl. I S. 3728)
SGG	Sozialgerichtsgesetz
SigG	Signaturgesetz vom 22. Juli 1997 (BGBl. I S. 1872 Art. 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung

StrlSchV	Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung) in der Fassung der Bekanntmachung vom 30- Juni 1989 (BGBl. I S. 1926), zuletzt geändert durch Verordnung vom 25. Juli 1006 (BGBl. I S. 1172)
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 Artikel 3 Nr. 3 des Gesetzes vom 20. Dezember 2001 (BGBl. I S. 3926)
StVollzG	Gesetz über den Vollzug der Freiheitsstrafe und der Freiheitsentziehenden Maßregeln der Besserung und Sicherung (Strafvollzugsgesetz) vom 16. März 19976 (BGBl. I S. 581, 2088; 1977 I S. 436), zuletzt geändert durch fünftes Gesetzt zur Änderung des Strafvollzugsgesetzes vom 27. Dezember 2000 (BGBl. I S. 2043)
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TDDSG	Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG) vom 22. Juli 1997 (BGBl. I S. 1870)
TDSV	Telekommunikations-Datenschutzverordnung vom 18. Dezember 2000 (BGBl. I S. 1740)
TFG	Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz) vom 1. Juli 1998 (BGBl. I S. 1752), zuletzt geändert durch Art. 7 des Gesetzes vom 23. Oktober 2001 (BGBl. I S. 2702)
TKG	Telekommunikationsgesetz vom 25. Juli 1996 (BGBl. I S. 1120), zuletzt geändert durch Art. 2 Abs. 6 des Gesetzes vom 26. August 1998 (BGBl. I S. 2521)
VermG	Gesetz zur Regelung offener Vermögensfragen (Vermögensgesetz) vom 23. September 1990 (BGBl. II S. 885, 1159) in der Fassung der Bekanntmachung vom 2. Dezember 1994, BGBl. I S. 3610), geändert durch Art. 1 des Vermögensrechtsanpassungsgesetzes vom 4. Juli 1995 (BGBl. I S. 895)
VwGO	Verwaltungsgerichtsordnung

VwVAktO	Verwaltungsvorschrift über die Aktenordnung für die Geschäftsstellen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften
VwVfG	Verwaltungsverfahrensgesetz
VwVPersAktenB	Verwaltungsvorschriften des Sächsischen Staatsministeriums des Innern über die Führung und Verwaltung von Personalakten der Beamten (Verwaltungsvorschrift Personalakten Beamte) vom 11. Dezember 1998 (SächsABl. vom 14. Januar 1999 S. 10)
VwVPersonalakten	Gemeinsame Verwaltungsvorschrift der Sächsischen Staatskanzlei und der Sächsischen Staatsministerien zur Führung und Verwaltung von Personalakten für Angestellte, Arbeiter und die zu ihrer Ausbildung Beschäftigten im öffentlichen Dienst des Freistaates Sachsen vom 7. Dezember 1996 (SächsABl. vom 6. Februar 1997 S. 145), geändert durch Verwaltungsvorschrift vom 20. Juli 1999 (SächsABl. S. 866)

Sonstiges

a. E.	am Ende
a. F.	alte Fassung
AfL/ÄfL	Amt/Ämter für Landwirtschaft
AfNS	Amt für Nationale Sicherheit
ÄndVO	Änderungs-Verordnung
AOK	Allgemeine Ortskrankenkasse
ARoV	Amt zur Regelung offener Vermögensfragen
AZR	Ausländerzentralregister
BA	Bundesanstalt für Arbeit
BAGE	Amtliche Sammlung der Entscheidungen des Bundesarbeitsgerichts

BAnz.	Bundesanzeiger
BARoV	Bundesamt zur Regelung offener Vermögensfragen
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Der Bundesbeauftragte für den Datenschutz
BFH	Bundesfinanzhof
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Zivilsachen
BGS	Bundesgrenzschutz
BHW	Beamtenheimstättenwerk
BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BML	Bundesministerium für Ernährung
BMWi	Bundesministerium für Wirtschaft
BND	Bundesnachrichtendienst
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
BVVG	Bodenverwertungs- und verwaltungs GmbH
BZR	Bundeszentralregister
CD-ROM	Compact disc-read only memory
CR	Computer und Recht (Zeitschrift)
DKFZ	Deutsches Krebsforschungszentrum
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
IM	Inoffizieller Mitarbeiter (des MfS/AfNS)
INPOL	Polizeiliches Informationssystem des Bundes und der Länder
ISDN	Integrated services digital network
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis
KBA	Kraftfahrtbundesamt
KfW	Kreditanstalt für Wiederaufbau
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
MdI	Ministerium des Innern (DDR)
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
PASS	Polizeiliches Auskunftssystem Sachsen
PersR	Personalvertretungsrecht (Zeitschrift)

PersV	Die Personalvertretung (Zeitschrift)
PIN	Personal identification number (Persönliche Identifikationsnummer)
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
SLBG	Sächsische landwirtschaftliche Berufsgenossenschaft
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

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
TLG	Treuhand Liegenschaftsgesellschaft mbH
TÜ	Telefonüberwachung
TÜV	Technischer Überwachungsverein
VG	Verwaltungsgericht
VIZ	Zeitschrift für Vermögens- und Investitionsrecht
VO	Verordnung
VwV	Verwaltungsvorschrift
VZR	Verkehrszentralregister
WWW	World wide web

Verweise im Text auf Ausführungen in früheren Tätigkeits-berichten 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

Auch in diesem Jahr lege ich meinen Tätigkeitsbericht mit einer erheblichen Verspätung vor. Dies ist auf die besondere Arbeitsbelastung meiner Behörde zurückzuführen, die ich bereits im letzten Jahr (9. TB, Seite 28) dargelegt habe. In diesem Jahr ist die längere Krankheit eines Referatsleiters und die Pensionierung eines anderen Referatsleiters dazugekommen. Der Mutterschutz und andere gute Gründe haben Weiteres dazu beigetragen, dass meine personelle Ausstattung unzureichend ist. Meine Mitarbeiter haben Ihre Arbeit fleißig und innovativ getan. Das kann aber nicht aufwiegen, was mir an personellen Ressourcen fehlt.

Gemäß § 23 Abs. 4 ist dem Datenschutzbeauftragten „für die Erfüllung seiner Aufgaben die notwendige Personal- und Sachausstattung zur Verfügung zu stellen". Da ich der Meinung bin, dass diese Aufgabe durch den Sächsischen Landtag zu erledigen ist, habe ich dort um sechs zusätzliche Stellen gebeten. Auf diesen Antrag habe ich bis heute keine offizielle Nachricht erhalten. Deshalb wiederhole ich: Die Ausgaben der öffentlichen Hand für Hard- und Software in der automatischen Datenverarbeitung sind exponentiell gestiegen. Wir müssen uns vergegenwärtigen, dass jede Behörde, ja fast jeder Mitarbeiter im öffentlichen Dienst im Freistaat Sachsen von morgens bis abends personenbezogene Daten verarbeitet. Dann wird deutlich, dass lediglich 18 Mitarbeiter des Sächsischen Datenschutzbeauftragten nicht dazu in der Lage sein können, die ca. 250.000 Bediensteten in der Staatsverwaltung, in der Kommunalverwaltung, in der Hochschulverwaltung und in den Kammern und Stiftungen sowie in den Krankenkassen umfassend und effizient zu beraten und zu kontrollieren.

Insbesondere unsere Beratungstätigkeit hat regelmäßig zu Einsparungen und Effizienzsteigerungen geführt, die weit über den für uns notwendigen Ausgaben liegen. Mit anderen Worten: Wir sind nicht nur unser Geld wert, sondern wir tragen mit unserer Beratungstätigkeit zu erheblichen Einsparungen bei. Dieser Aspekt unserer Arbeit ist bislang möglicherweise nicht hinreichend erkannt worden. Es geht uns da ähnlich wie den Prüfern der Finanzämter: Jeder Prüfer spielt das Mehrfache seines Gehaltes ein. Ich gebe zu, dass wir in mancher Behörde auch gleichermaßen unbeliebt sind, wie dies bei Finanzamtsprüfern in der Marktwirtschaft angeblich der Fall ist. Andererseits freue ich mich darüber, dass unsere Zusammenarbeit mit den Behörden alles in allem kollegial und freundlich verläuft. Wir lernen voneinander und singen meist vom gleichen Blatt.

Von Anfang an habe ich darum geworben, dass meine Behörde frühzeitig in die Planungs- und Entwicklungsprozesse der Datenverarbeitung einbezogen wird. Anders als dies in anderen Ländern der Fall sein mag, ist nämlich der Sächsische Datenschutzbeauftragte bereit, von Anfang an eine Mitverantwortung für diese Projekte

zu übernehmen. Im Sinne einer Gesamtverantwortung für den Freistaat Sachsen muss die Beratungspflicht meiner Behörde im Rang vor meiner Kontrollpflicht stehen. Denn zum einen dient es dem Persönlichkeitsrecht am besten, wenn Verstöße von Anfang an vermieden werden, zum anderen ist es eine Verschwendung öffentlicher Ressourcen, wenn falsche Pläne entwickelt und umgesetzt werden und danach erst unter dem Druck einer datenschutzrechtlichen Kontrolle die Dinge ins Lot gebracht werden. Zum einen kann ich insofern auf sehr gute Beispiele einer frühzeitigen Zusammenarbeit mit sächsischen Behörden verweisen, zum anderen wiederhole ich hier meinen Appell, dass auch diejenigen Behördenleiter, die bislang - vielleicht, um keine „schlafenden Hunde zu wecken“ - auf eine frühzeitige Information meiner Behörde verzichtet und darauf vertraut haben, dass eine Kontrolle nicht stattfindet, das Beratungsangebot meiner Dienststelle frühzeitig zu nutzen.

Über einen neuen, leicht veränderten Gesetzentwurf der (ehemaligen) Staatsregierung zur Anpassung des Sächsischen Datenschutzgesetzes an die EG-Richtlinie wird der Landtag nach Anhörung von Sachverständigen beschließen.

2 Parlament

In diesem Jahr nicht belegt

3 Europäische Union / Europäische Gemeinschaft

In diesem Jahr nicht belegt.

4 Medien

In diesem Jahr nicht belegt.

5 Inneres

5.1 Personalwesen

5.1.1 Nochmals: Gefährdungsanalyse im Geschäftsbereich des SMI

Erfreulicherweise hat sich das SMI doch noch von der Irrelevanz „mentaler Daten“ (Stressfaktoren) für die Gefährdungsanalyse an Bildschirmarbeitsplätzen überzeugen lassen (vgl. 9/5.1.10, S. 37, 39), so dass in Erwiderung auf meinen Tätigkeitsbericht (s. Landtagsdrucksache 3/5765) sinngemäß mitgeteilt wird: Die auf dem Fragebogen für Bildschirmarbeitsplätze kritisierten „mentalen“ Fragen seien zwar an einer Universität entwickelt und tausendfach erprobt worden (und mithin offenbar über jeden Zweifel erhaben); auf ihre Erhebung werde aber in Zukunft trotzdem verzichtet. Diese Entscheidung begrüße ich sowohl fallspezifisch als auch grundsätzlich, denn sie legt Zeugnis davon ab, dass der Zweck einer Maßnahme offenbar auch mit weniger Daten-Sammelleidenschaft erfüllt werden kann, wenn nämlich vorher exakt geprüft wird, was erforderlich und nicht erforderlich ist.

Allerdings verwendet das SMI mittlerweile ein neuartiges rechnergestütztes Programm namens „Handlungshilfe, Version 2.0“, welches ich mir ebenfalls vorlegen ließ. Es wurde erstellt durch die Zentralstelle für Arbeitsschutz beim Bundesministerium des Innern und der Bundesausführungsbehörde für Unfallversicherung (BAfU) im Auftrag der Zentralstelle für Arbeitsschutz. Meine Prüfung, die ich dem SMI übermittelt habe, ergab Folgendes: „Gegen die Verwendung der ‚Handlungshilfe, Version 2.0‘ bestehen inhaltlich keine datenschutzrechtlichen Bedenken. Hinsichtlich des System-Bausteins ‚5.4.1. Psychische Belastungen‘ gehe ich davon aus, dass bei dessen Anwendung den im ‚Vorwort‘ formulierten Hinweisen Rechnung getragen wird. Dort heißt es u. a.: ‚Die Anwendung dieses Bausteins ist nicht obligatorisch. Bei Anwendung ist eine fachliche Begleitung sicherzustellen (z. B. durch den Ärztlichen Sozialen Dienst, psychologischen Dienst, Betriebsarzt).‘ “

Selbstverständlich ist die Erhebung von Stressfaktoren im Rahmen einer Gefährdungsanalyse nicht quer Beet für alle Tätigkeitsbereiche abzulehnen. Hintergrund dieses Hinweises ist die Zweckbestimmung des integrierten Bausteins 5.4.1. Er enthält nämlich wiederum beinahe ausschließlich Fragen zur „mentalen“ Belastung an Arbeitsplätzen, etwa: „Besteht ein positives soziales Klima?“ Eine solche Frage kann zur Erhellung von Arbeitsschutz- und Sicherheitsfragen nur in einer ganz besonderen Fallkonstellation beitragen und zwar in einem sehr eingegrenzten Anwenderbereich. Personen, die in erheblichem Maße einer psychischen Anspannung unterliegen und auf deren uneingeschränkt intaktes Reaktionsvermögen es als Sicherheitsfaktor für sich wie für andere Personen ebenso ankommt wie auf ihre

psychische Stabilität, kann die Kenntnis von spezifischen Belastungen lebensrettend sein. Als Beispiele, woran dies leicht ersichtlich wird, seien nur einige genannt: Rettungskräfte, intensivmedizinisches Personal, Polizeitaucher, Berufskraftfahrer, Fluglotsen.

Jedenfalls sind derartige Gefährdungen für normale Bildschirmarbeitsplätze in Behörden und Einrichtungen nicht ersichtlich. Deshalb ist es richtig, insoweit von ihrer Erhebung abzusehen.

Zu verbliebenen offenen Fragen der Auswertung und Aufbewahrung des erhobenen Datenmaterials habe ich das SMI um Darlegungen gebeten, die bislang aber noch nicht vorliegen. Ich werde die Angelegenheit deshalb weiter im Auge behalten.

5.1.2 Einstellung einer „Abwesenheitstafel“ ins innerbehördliche Intranet

Der örtliche Personalrat einer öffentlichen Stelle wandte sich an mich mit der Frage, ob es Bedenken dagegen gebe, die bislang für alle Mitarbeiter im zentralen Sekretariat angebrachte Abwesenheitsübersicht zu digitalisieren und ins behördeninterne Intranet einzustellen. Nach der Versuchsphase habe es Beschwerden gegeben, weil der Abwesenheitsgrund, z. B. Krankheit, ausdrücklich angegeben wurde. Daraufhin habe man die Abwesenheitsübersicht ganz aus dem Netz genommen, was aber ebenfalls auf Widerspruch gestoßen sei, denn die Information der Mitarbeiter über die Abwesenheit von Kollegen sei aus organisatorischen Gründen erforderlich.

Ich habe mich gegenüber dem Personalrat wie folgt geäußert: An der grundsätzlichen Zulässigkeit einer Abwesenheitsübersicht, ob nun als Tafel oder wie hier als Tabellendokument im Intranet, bestehen aus datenschutzrechtlicher Sicht keine Bedenken. § 31 Abs. 1 SächsDSG erlaubt die Verarbeitung von Beschäftigtendaten zu Organisationszwecken. Das ist hier der Fall, denn eine Abwesenheitsübersicht wird zu dem Zweck erstellt, diejenigen Kollegen in den (übrigen) Organisationseinheiten zu unterrichten, die nicht wie z. B. ein Vorgesetzter unmittelbar Kenntnis von einer plan- oder außerplanmäßigen Abwesenheit eines Beschäftigten haben. Die innerbehördliche Zusammenarbeit wird durch die Information, ob ein Kollege anwesend ist, bzw. wie lange er abwesend sein wird, erheblich erleichtert.

Allerdings haben sich die in der Übersicht genannten Abwesenheitsgründe an der dienstlichen Erforderlichkeit zu orientieren. Insoweit kann darauf verzichtet werden, die Abwesenheitsgründe zu nennen, die den Privatbereich des Beschäftigten berühren (z. B. Mutterschutz, Urlaub und Krankheit). Stattdessen reicht es aus, sie allgemein mit „Abwesenheit bis zum (Datum)“ zu bezeichnen. Für anders gelagert erachte ich dienstliche Abwesenheitsgründe wie z. B. Fortbildung oder Dienstreise, da diese

Gründe auch innerhalb der Abwesenheitsperiode für die Organisation des Dienstes Bedeutung erlangen können.

5.1.3 Durchführung von Krankenrückkehrgesprächen zur Senkung krankheitsbedingter Fehlzeiten bei den Beschäftigten

Ein Sächsisches Staatsministerium plante, ein anderes Ministerium praktizierte bereits so genannte „Krankenrückkehrgespräche“ im Anschluss an die Genesung eines Beschäftigten. In beiden Fällen war die Dokumentation in der Personalakte vorgesehen.

Die Regelungen in den zugehörigen Verwaltungsvorschriften haben bei mir den Eindruck erweckt, hinter der Maßnahme stehe weniger der behauptete Fürsorgegedanke als vielmehr die Vermutung, die Beschäftigten würden Erkrankungen vortäuschen und man wolle - was löblich wäre - die wirklichen Gründe für eine „Flucht in die Krankheit“ erforschen. So hieß es z. B. an einer Stelle, dass auf „wiederholte und auffällige Ausfallzeiten an bestimmten Tagen oder zu bestimmten Terminen abzustellen“ sei.

Dazu habe ich mich wie folgt geäußert:

Aus datenschutzrechtlicher Sicht bestehen Bedenken gegen die Zulässigkeit solcher Krankenrückkehrgespräche, und zwar aus folgenden Gründen:

Gemäß § 31 Abs. 1 SächsDSG dürfen öffentliche Stellen Daten ihrer Beschäftigten „nur verarbeiten, soweit dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes *erforderlich* ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht“. Dass eine dieser Voraussetzungen, insbesondere die Erforderlichkeit, erfüllt ist, ist mir noch nicht ganz klar. Aber was nicht ist, kann ja noch werden ...

Weder das Sächsische Beamtengesetz noch die Tarifverträge für die Beschäftigten des öffentlichen Dienstes sehen Krankenrückkehrgespräche vor. Damit ist - jedenfalls grundsätzlich, also von Ausnahmen abgesehen - kein Beschäftigter verpflichtet, sich zu den Ursachen seiner Erkrankung zu äußern. Und für den beabsichtigten Zweck, nämlich krankheitsbedingte Fehlzeiten zu senken, sind spezielle Krankenrückkehrgespräche *nicht dienlich.* Die Feststellung, ob die Ursachen für überdurchschnittlich hohe Krankenquoten im Arbeitsumfeld und/oder in den Arbeitsbedingungen zu suchen ist, kann aber auch nicht durch eine anonyme Fragebogenaktion erfolgen.

Denkbar und datenschutzrechtlich unbedenklich ist auch das Angebot an die Beschäftigten, sich im Hinblick auf krank machende Arbeitsbedingungen vertrauensvoll an ihre Vorgesetzten zu wenden. Sofern dies in der Vergangenheit unterblieben ist, gilt, dass es zu den Selbstverständlichkeiten gehören sollte. Erfahrungsgemäß hat eine mangelhafte Kommunikation manchmal ihre Ursache in der Personalführung.

Für den Fall, dass der Dienstherr/Arbeitgeber die Erkrankung eines Beschäftigten anzweifelt, enthalten § 92 Abs. 2 SächsBG bzw. § 7 BAT-O eindeutige Regelungen. Danach kann der Nachweis der Dienstunfähigkeit durch ein ärztliches Attest verlangt oder eine amtsärztliche Untersuchung veranlasst werden. Solange ein Beschäftigter jedoch ein ordnungsgemäß ausgestelltes Attest vorlegt, ist es in der Regel der Beweis für die Tatsache, dass er infolge Krankheit arbeitsunfähig war. Die Behandlung der Ausnahmen von dieser Regel erfordert Fingerspitzengefühl und ein behutsames Vorgehen.

Jede Rückkehr aus dem Urlaub, von einem Lehrgang oder einer Abordnung, von der Kur oder einer (nicht ganz kurzen) Krankheit bedarf eines „Rückkehrgesprächs“. Die Information über Veränderungen und neue Anforderungen des Dienstbetriebes, die Frage nach neuen Aufgaben und frischer Motivation sind wichtige vertrauensfördernde Maßnahmen, sie gehören dazu. Von leitenden Mitarbeitern, auch von Kollegen, die ihr Team ernst nehmen, erwartet man die Initiative zu solchen Gesprächen. In großen Behörden muss es nicht unbedingt der Chef sein, der sie führt; er kann einen leitenden Mitarbeiter damit beauftragen.

In dem Gespräch darf durchaus zur Sprache kommen, welche Auswirkungen die Abwesenheit auf die künftige Arbeitsgestaltung hat. Dabei sind auch Ursachen und Folgen von Krankheit kein Tabu; hier darf zwar keine Abfrage von Krankheitsdaten erfolgen. Das hat auch niemand im Sinn. Aber die Frage nach krank machenden oder demotivierenden Arbeitsumständen ist ebenso gestattet wie die (ehrliche!) gemeinsame Suche nach Verbesserungsvorschlägen. Die Gesprächsteilnehmer merken meist schnell, ob der Vorgesetzte und der Mitarbeiter sich ernsthaft oder lauernd verhalten.

Ich habe vorgeschlagen, „Rückkehrgespräche“ zu führen; die Krankheit soll nur zur Sprache kommen, soweit sie - körperlich oder psychisch - Auswirkungen auf die künftige Dienstgestaltung hat.

Wenn Zweifel an der Lauterkeit einer Krankmeldung bestehen (z. B. wiederholt an bestimmten Wochentagen; nach dienstlichen Auseinandersetzungen; häufige Arztwechsel) soll die Personalabteilung schriftlich agieren, z. B. den Polizeiarzt oder den Amtsarzt einschalten.

5.1.4 Datenschutzkontrolle der automatisierten Arbeitszeiterfassung

In einem Regierungspräsidium habe ich die Durchführung der automatisierten Arbeitszeiterfassung sowie die getroffenen Maßnahmen zur Gewährleistung des Datenschutzes nach § 9 SächsDSG kontrolliert. An der Verfahrenseinführung bin ich zuvor gemäß § 31 Abs. 7 SächsDSG beteiligt worden, ebenso am Entwurf der Dienstvereinbarung, die die Grundlage der automatisierten Arbeitszeiterfassung bildet.

Im Einzelnen habe ich folgende Feststellungen getroffen:

- Die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes gemäß § 9 SächsDSG (Zugriffsregelungen, Rechteverteilung, Passwortschutz für PC und das Zeiterfassungsprogramm, Bildschirmschoner) waren nicht zu beanstanden.

- Die gemäß § 16 Abs. 2 Arbeitszeitgesetz (ArbZG) zwingend zu speichernden Zeitwertdaten werden nach der zweijährigen Aufbewahrungsfrist automatisch gelöscht.

- Vorgesetzte können nach den Regelungen in der Dienstvereinbarung zu Kontrollzwecken Auswertungslisten anfordern. Nach Aufgabenerledigung sind diese im Original an die Personalsachbearbeiter für Zeiterfassung zurückzugeben und werden durch sie vernichtet. Das halte ich für eine datenschutzfreundliche Lösung.

- Abweichungen vom Umfang der nach der Dienstvereinbarung zu erfassenden Beschäftigtendaten sowie der Zeitwertdaten wurden nicht festgestellt.

- Auf Antrag des Beschäftigten wird ein Monatsjournal ausgedruckt. Wie in der Dienstvereinbarung vorgesehen, erfolgt eine datenschutzgerechte Übergabe im verschlossenen Umschlag.

- In einem Fall wurden die Kernzeitverletzungen eines Bediensteten seit Juli 1996 als Listen in der Sachakte „Zeiterfassung“ aufbewahrt. Diese Auswertungslisten sind aber nach Aufgabenerledigung, spätestens nach sechs Monaten, zu vernichten. Die Überschreitung der Aufbewahrungsfrist wurde mit einem für erforderlich gehaltenen Nachweis der Verletzungen der Dienstzeiten in einem Gerichtsverfahren begründet. Das habe ich für unzulässig gehalten, da dem Betroffenen innerhalb der sechsmonatigen Aufbewahrungszeit keine Gelegenheit zur Stellungnahme (Anhörung) gegeben wurde. Nur im Zusammenhang mit einer Anhörung im Hinblick auf konkrete arbeitsrechtliche Konsequenzen hätten die Unterlagen so

genannte Personalaktenqualität erhalten und gemäß § 31 Abs. 1 SächsDSG zur Durchführung bzw. Beendigung des Arbeitsverhältnisses genutzt werden dürfen. Nach der Anhörung hätten die Unterlagen über Dienstzeitverletzungen dann in die Personalakte/Disziplinarakte aufgenommen werden müssen und nicht in der Sachakte Zeiterfassung verbleiben dürfen.

Der zuständige Referatsleiter hat zugesichert, diese Listen umgehend zu vernichten. Außerdem habe ich angeregt, dass der Betroffene davon unterrichtet wird.

In diesem Zusammenhang habe ich auch nochmals darauf hingewiesen, dass die Zeitwertdaten, die gemäß § 16 Abs. 2 ArbZG zwei Jahre im System gespeichert werden, nicht zum Nachweis von Arbeits- bzw. Dienstzeitverletzungen genutzt werden dürfen. Diese Zeitwertdaten sind ausschließlich durch den Dienstherrn als Nachweis der arbeitstäglichen Arbeitszeit gemäß § 3 ArbZG gegenüber der Aufsichtsbehörde (§ 17 ArbZG) zu verwenden (§ 12 Abs. 1 Nr. 2 SächsDSG).

Mein Kontrollbericht war der zuständigen Personalvertretung zuzuleiten.

5.1.5 Zum Umgang mit BStU-Unterlagen (Aufbewahrung, Archivierung, Vernichtung)

Die Anfrage eines kommunalen Datenschutzbeauftragten, ob

- „über den Fragebogen und die Mitteilung(en) des Bundesbeauftragten hinausgehende Stasi-Unterlagen in die Personalakte gehören“,
- „Stasi-Unterlagen“ in Personalakten vor der Abgabe der Personalakte an ein Archiv oder einer „Weitergabe im Rahmen von Privatisierungen“ (öffentlicher Stellen) zu entfernen und zu vernichten seien,
- das Verwendungsverbot nach § 21 Abs. 3 StUG die Vernichtung der BStU-Aktenteile nach Ablauf der 15-Jahres-Frist am 20. Dezember 2006 gebiete,

gibt mir Anlass, an dieser Stelle klarzustellen:

1. Die vom Fragesteller gewählte Bezeichnung der Unterlagen, die der BStU an die Arbeitgeber/Dienstherrn übersandt hat, als „Stasi-Unterlagen“ ist unzutreffend. Denn „Stasi-Unterlagen“ sind die in § 6 Abs. 1 und 2 StUG definierten Informationsträger des Staatssicherheitsdienstes oder des Arbeitsgebiets 1 der DDR-Kriminalpolizei - mithin ist für ihre Klassifizierung allein ihre Originalität und der Zeitpunkt ihres Entstehens maßgebend. Sie werden deshalb in der Regel durch den BStU nicht herausgegeben und demgemäß auch nur in Kopie an den Arbeitgeber/Dienstherrn übersandt. Dagegen sind die von der Bundesbehörde BStU übersandten Bescheide (nebst kopierter Anlagen) reine

Verwaltungsunterlagen, die nicht den Verarbei-tungsbestimmungen des Stasi-Unterlagengesetzes unterliegen. Die Bezeichnung „Stasi-Unterlagen“ muss daher unterbleiben.

2. Ob und welche BStU-Unterlagen in Personalakten eingefügt werden dürfen, bemisst sich danach, ob die BStU-Unterlagen zur Verfolgung der in § 31 Abs. 1 SächsDSG oder der in § 117 Abs. 4 SächsBG genannten Zwecke erforderlich sind. So sind diejenigen BStU-Unterlagen erforderlich, die einen engen und unmittelbaren inneren Zusammenhang mit den in den Rechtsvorschriften genannten Zwecken aufweisen („materieller Personalaktenbegriff“). Insofern weise ich auf Punkt A I. 5. der VwVPersAktenB des SMI vom 11. Dezember 1998 (SächsABl. S. 10 ff.) hin, der in den Kommunen entsprechend anwendbar ist. Somit bleibt es dabei, dass lediglich der Erklärungsbogen, die Anfrage beim BStU sowie dessen Bescheid in die Personalakte eingefügt werden dürfen. An dieser Stelle weise ich darauf hin, dass Anlagen zu den Bescheiden des BStU, die etwa „zum Zwecke beispielhafter Erläuterung beigefügt sind“, keine Personalaktenqualität besitzen und daher nicht in die Personalakte eingefügt werden dürfen.

3. Nach Ablauf einschlägiger Aufbewahrungsfristen sind die Personalakten zusammen mit den vom BStU stammenden Unterlagen dem zuständigen Archiv nach Maßgabe archivrechtlicher Vorschriften vollständig anzubieten, vgl. auch § 123 Abs. 4 SächsBG. Die vorherige Vernichtung einzelner Aktenteile, etwa der BStU-Unterlagen, wäre damit nicht zu vereinbaren. Erst wenn das zuständige Archiv die Archivierung der Personalakten abgelehnt hat, müssten die Personalakten - vollständig - vernichtet werden.

   Im zuständigen Archiv unterliegen die Personalakten samt der BStU-Aktenteile den Schutzfristen nach §§ 10 Abs. 1 Sätze 3 und 4, 13 Abs. 3 SächsArchivG für personenbezogenes Archivgut. § 10 Abs. 2 Satz 2 SächsArchivG, wonach die Schutzfristen nicht für DDR-Unterlagen gelten, wäre in diesem Fall nicht anwendbar, denn die betreffenden BStU-Unterlagen wären im Freistaat Sachsen zur Aufgabenerfüllung des Arbeitgebers/Dienstherrn erforderlich und sind daher kein „Archivgut der Rechtsvorgänger des Freistaates Sachsen und der Funktionsvorgänger der in Satz 1 genannten Stellen“ nach § 4 Abs. 2 Sätze 2 und 3 SächsArchivG.

4. Für die Aufbewahrung (Speicherung) der Daten bei der Privatisierung personalaktenführender Stellen ist Folgendes zu beachten: Art. 119 SächsVerf, wonach eine Mitarbeit beim MfS/AfNS die Eignung für den öffentlichen Dienst grundsätzlich ausschließt, bindet nur öffentliche Arbeitgeber und Dienstherren. Nicht-öffentliche Arbeitgeber sind davon nicht betroffen. Ihnen ist nach §§ 19, 21 StUG - allerdings unter bestimmten Voraussetzungen - grundsätzlich die

Befugnis zur Verwendung personenbezogener BStU-Unterlagen im Hinblick auf Weiterbeschäftigung oder Einstellung erteilt worden.
Hinzu kommt, dass nach § 31 Abs. 2 SächsDSG „eine Übermittlung von Daten von Beschäftigten an Personen oder Stellen außerhalb des öffentlichen Bereichs nur auf gesetzlicher Grundlage oder mit der Einwilligung des Betroffenen zulässig“ ist. Dies gilt auch für Datenübermittlungen an einen künftigen Arbeitgeber des Betroffenen (vgl. 7/5.5.3).

Aus der Wertung der Verfassung sowie dem Erfordernis einer gesetzlichen Grundlage für die Übermittlung ergibt sich für den Fall des Betriebsübergangs im Rahmen von Privatisierungen Folgendes:

Dem neuen (privaten) Inhaber der personalaktenführenden Stelle dürfen lediglich BStU-Unterlagen in Personalakten
- der vorgenannten Personen,
- mit deren Kenntnis (§ 21 Abs. 1 Nr. 6 StUG) bzw. im Falle von Betriebsräten mit deren Einwilligung (§ 21 Abs. 1 Nr. 7 StUG),
- zu den in § 21 Abs. 1 Nrn. 6, 7 StUG genannten Zwecken und
- unter den allgemeinen Voraussetzungen von § 19 Abs. 1 Satz 2 StUG

übergeben werden. In allen anderen Fällen sowie in den Fällen, in denen die Einwilligung nicht erteilt wird, sind die BStU-Unterlagen vor dem Betriebsübergang zu entfernen und dem zuständigen Archiv anzubieten.

5. Das Verwendungsverbot nach § 21 Abs. 3 StUG enthält kein Gebot zur Vernichtung der BStU-Aktenteile nach Ablauf der 15-Jahres-Frist am 20. Dezember 2006. Denn BStU-Aktenteile müssen vielmehr wegen des Grundsatzes der Vollständigkeit der Personalakte in der Personalakte verbleiben und nach Maßgabe der vorgenannten archivrechtlichen Vorschriften dem zuständigen Archiv mit angeboten werden. Sie dürfen lediglich nicht mehr weiter verwendet werden (z. B. zu Zwecken der Kündigung). § 122 Abs. 1 Satz 1 Nr. 2 SächsBG, wonach dem Beamten ungünstige oder nachteilige Unterlagen über Beschwerden, Behauptungen und Bewertungen auf Antrag des Beamten nach drei Jahren entfernt und vernichtet werden dürfen, ist nicht anwendbar, denn die Informationen aus den Stasi-Unterlagen sind „Teil ... einer anderen die ... Eignung betreffenden förmlichen Feststellung“ (vgl. F I. 2. der VwVPersAktenB).

5.2 Personalvertretung

In diesem Jahr nicht belegt.

5.3 Einwohnermeldewesen

5.3.1 Speicherung und Änderung von Meldedaten; sorgfältiger Umgang mit Meldedaten

Ein Petent hat mir folgenden Sachverhalt mitgeteilt: Beim kürzlichen Umtausch seines Führerscheins musste er feststellen, dass ein falscher Geburtsort im neuen Führerschein stand. Es stellte sich heraus, dass auch im Melderegister, aus dem die Daten in den neuen Führerschein übernommen worden waren, der falsche Geburtsort gespeichert war. Das war insofern unverständlich, als die Meldebehörde dem Petenten bereits im September 1992 einen Personalausweis und im Dezember desselben Jahres einen Reisepass mit dem korrekten Geburtsort ausgestellt hatte. Der Petent fragte daher zu Recht: Wie konnte dieser - nur auf den ersten Blick harmlose - Fehleintrag geschehen?

Das Einwohnermeldeamt hat auf mein Bitten hin den Datenfehler anhand der archivierten Unterlagen rekonstruiert und kam zu folgendem Ergebnis:

Auf der aus der frühen DDR-Zeit stammenden „Kerblochkarteikarte“ war noch der korrekte Geburtsort eingetragen. Erst nachdem (von 1978 bis 1980) für das Zentrale Einwohnerregister Berlin (ZER) eine Erfassung auf maschinenlesbaren Datenblättern durch Arbeitskräfte erfolgte, die monatelang nur diese Tätigkeit ausführten, erschien plötzlich ein falscher Geburtsort in den Meldedaten. Die Stadtverwaltung ist sich sicher, dass ein Versehen vorlag und sich der im Zuge der Routinetätigkeit am häufigsten auftretende Ortsname eingeschlichen hat. Ein Indiz dafür ist auch die Tatsache, dass dieser falsche Geburtsort dem Wohnort des Petenten entspricht.

Bis zur Einrichtung des kommunalen Melderegisters waren dann keine Änderungen mehr erfolgt, so dass der falsche Geburtsort im August 1992 bei Übernahme der Daten aus dem ZER in das automatisierte kommunale Melderegister mit übernommen wurde. Mit diesem System gab es erhebliche Anfangsschwierigkeiten, und just in diese Zeit fiel die Personalausweis- und Passantragstellung des Petenten. Der falsche Geburtsort wurde damals durch den Petenten selbst beanstandet und durch die Sachbearbeiterin des Meldeamtes in den Ausweisdokumenten berichtigt. Allerdings unterblieb die Korrektur im elektronischen Datensatz des Einwohnerverfahrens. Erst nach mehr als neun Jahren, nämlich mit dem Umtausch des Führerscheins Anfang 2002, wurde der Fehler bemerkt und endgültig behoben. Dazu verlangte die Meldebehörde jedoch die Geburtsurkunde.

5.3.2 Weitergabe von Meldedaten an Adressbuchverlage

Ein Petent fragte, ob die Weitergabe von Meldedaten an Adressbuchverlage mit dem Sächsischen Datenschutzgesetz vereinbar sei. Ich habe ihm wie folgt geantwortet:

Gegen diese Praxis ist nichts einzuwenden, da sie spezialgesetzlich geregelt ist. So erlaubt § 33 Abs. 3 SächsMG der Meldebehörde u. a., „Vor- und Familiennamen, Doktorgrad und Anschriften der volljährigen Einwohner in alphabetischer Reihenfolge der Familiennamen“ an Dritte zum Zwecke der Veröffentlichung zu übermitteln. Eine solche spezialgesetzliche Vorschrift („lex specialis“) geht dem Sächsischen Datenschutzgesetz vor (§ 2 Abs. 4).

Außerdem kritisierte der Betroffene, dass der Einzelne es nur im Wege des Widerspruchs verhindern kann, in die Datenspeicher kommerzieller Adressbuchverlage zu gelangen. Er hätte es bevorzugt, um Einwilligung gebeten zu werden. Die Frage, „Widerspruch oder Einwilligung?“ hatte seinerzeit, anlässlich der parlamentarischen Beratung zum Sächsischen Meldegesetz, eine intensive Erörterung ausgelöst. Die Einwilligungslösung - jeder muss nach seiner Meinung gefragt werden - ist aber letztlich doch als unverhältnismäßig aufwändig verworfen worden. Statt dessen wurde die Möglichkeit geschaffen, der Datenübermittlung zu widersprechen (§ 33 Abs. 4 Satz 1 SächsMG). In Satz 2 dieser Vorschrift ist näher ausgeführt, wie die Meldebehörde auf dieses Widerspruchsrecht hinzuweisen hat, und zwar bei der melderechtlichen Anmeldung und durch „öffentliche Bekanntmachung“. Diese hat ortsüblich zu sein. Als ortsüblich ist sie insbesondere nicht schon dann anzusehen, wenn sie rechtzeitig im jeweiligen Amtsblatt erscheint; vielmehr sollte diese Bekanntmachung auch in der Tagespresse veröffentlicht werden.

Bürgern, denen an einer Weitergabe ihrer Meldedaten an kommerzielle Anbieter nicht gelegen ist (Stichwort: Bitte keine Werbung einwerfen!) ist daher zu empfehlen, der Meldebehörde einen entsprechenden Widerspruch zuzuleiten, sich dessen Eingang bestätigen zu lassen und darauf zu achten, dass er in der folgenden Auflage des Adressbuchs nicht mehr erscheint. Verstöße bitte ich mir mitzuteilen. Ich werde dann eine Beanstandung aussprechen.

5.3.3 Übermittlung von Meldedaten im Abrufverfahren an die Finanzämter gemäß § 10 SächsMeldDÜVO

Zur Feststellung einer Person und deren Anschrift im Rahmen eines Besteuerungsverfahrens dürfen Meldedaten für die zuständigen Finanzämter gemäß § 10 SächsMeldDÜVO zum Abruf bereitgehalten werden.
Eine Stadtverwaltung hat mich gemäß § 8 Abs. 3 SächsDSG über die beabsichtigte Einführung des Abrufverfahrens unterrichtet. Allerdings hatte man seitens der Stadtverwaltung übersehen, dass die Meldebehörde *und* der Datenempfänger (hier das Finanzamt) gemäß § 3 SächsMeldDÜVO das automatisierte Abrufverfahren zu regeln haben, insbesondere die erforderlichen personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes (§ 4 Abs. 1 SächsMeldDÜVO). Das war nicht geschehen.

Die Vereinbarung zwischen dem Meldeamt der Stadtverwaltung und dem Finanzamt liegt jetzt vor.

5.4 Personenstandswesen

In diesem Jahr nicht belegt.

5.5 Kommunale Selbstverwaltung

5.5.1 Weitergabe von Bürgereinwendungen gegen ein Bauvorhaben an den Investor

Gleich drei Eingaben betrafen ein größeres Bauvorhaben in einem Naturschutzgebiet. Etwa 350 Einwohner einer anliegenden Gemeinde hatten sich schriftlich an den Bürgermeister gewandt und ihre ganz persönlichen Bedenken gegen das Bauvorhaben geäußert. Dabei wurden auch Krankengeschichten, Familienverhältnisse und erwogene Schadensersatzklagen offen gelegt. Diese Schreiben hat der Bürgermeister in Kopie an den Investor weitergegeben. Diese Datenübermittlung war unzulässig. Ich habe sie beanstandet, und zwar aus folgenden Gründen:

Adressat der Bürgereinwendungen war die Gemeinde. Bei dieser liegt als Träger der kommunalen Selbstverwaltung die Planungshoheit. Da weder das Baugesetzbuch noch die Sächsische Bauordnung und die dazu ergangene Durchführungsverordnung Regelungen zum Umgang mit personenbezogenen Daten enthalten, finden die Vorschriften des Sächsischen Datenschutzgesetzes subsidiär Anwendung (§ 2 Abs. 4 SächsDSG). Einschlägig für die Zulässigkeit der Übermittlung von personenbezogenen Daten an Private, hier den Investor, ist § 15 SächsDSG.

§ 15 SächsDSG erlaubt die Datenübermittlung, wenn sie
1. „zur Erfüllung der Aufgaben der übermittelnden Stelle *erforderlich* ist und für Zwecke erfolgt, für die eine Nutzung nach § 12 Abs. 1 bis 4 zulässig wäre oder
2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft dargelegt hat und der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat“.

Die Weitergabe der Bürgereinwendungen in Form von Kopien war nicht erforderlich. Datenschutzgerecht wäre es gewesen, die Einwendungen ihrer Art nach auszuwerten und das Ergebnis dem Investor als Bericht oder Statistik mitzuteilen (z. B. gesundheitliche Bedenken: xx Fälle, unzumutbare Lärmbelästigung: yy Fälle, erwogene Schadensersatzklagen: zz Fälle). Die Schwärzung von Namen und Anschriften allein hätte nicht genügt, da über den Inhalt der Bezug zu bestimmten

Personen hätte hergestellt werden können. Vom Sächsischen Datenschutzgesetz umfasst sind jedoch nicht nur die Daten bestimmter, sondern auch bestimmbarer Personen. Da es bereits an der *Erforderlichkeit* der Datenübermittlung fehlte, hat sich die Prüfung erübrigt, ob „eine Nutzung nach § 12 Abs. 1 bis 4 SächsDSG“ zulässig gewesen wäre.

Auch eine Zulässigkeit der Datenübermittlung nach § 15 Abs. 1 Nr. 2 SächsDSG habe ich verneint. Der Investor hatte gegenüber der Gemeinde kein berechtigtes Interesse an der Kenntnis der personenbezogenen Bürgereinwendungen dargelegt. Selbst wenn dies der Fall gewesen wäre, hätte das schutzwürdige Interesse der Betroffenen am Unterbleiben der Übermittlung geprüft werden müssen. Zu diesem Zweck hätte jeder einzelne Betroffene gemäß § 15 Abs. 3 SächsDSG gehört werden müssen. Auch dies ist nicht geschehen.

Ich habe den Bürgermeister aufgefordert, vom Investor die Rückgabe der Kopie zu verlangen und sich von diesem schriftlich bestätigen zu lassen, dass davon keine Kopien gefertigt und zurückbehalten wurden.

Dem Vernehmen nach haben die drei Petenten meine rechtliche Bewertung zum Anlass genommen, das Verhalten des Bürgermeisters beim zuständigen Regierungspräsidium nach § 32 SächsDSG als Ordnungswidrigkeit anzuzeigen.

Nachdem ich meine Beanstandung ausgesprochen hatte, wurde mir ein Zeitungsartikel zugesandt, wonach der Investor die Bürgereinwendungen niemals erhalten haben wollte.

Auf meine Nachfrage hin hat der Bürgermeister mir jedoch kurz nach Erscheinen des Artikels mitgeteilt, der Investor habe die Unterlagen „in einer seiner vielen Firmen wiedergefunden“ und er, der Bürgermeister, habe sie wieder in Empfang genommen.

Ein derart leichtfertiger und unzuverlässiger Umgang mit personenbezogenen Informationen kann in Sachsen nicht geduldet werden. Ich habe deshalb das SMI, das zuständige RP sowie das zuständige LRA gebeten, die notwendigen Aufsichtsmaßnahmen zu treffen, damit sich ein solcher Vorgang nicht wiederholt.

5.5.2 „Stationärer Bürgerladen“ - Umsetzung eines rechtswidrigen Pilotprojekts

Wie bereits in meinem 9. Tätigkeitsbericht (5.5.3) angekündigt, habe ich die Bündelung kommunaler Aufgaben und privater Dienstleistungen in einer (kommunalen) Hand durch die Gründung eines „Bürgerladens“ im August 2001 gemäß § 26 SächsDSG beanstandet.

Durch die Einrichtung eines „Bürgerladens“ sollen in Gemeinden, in denen sich Sparkassenfilialen nicht mehr rentieren, unter anderem Sparkassenaufgaben von städtischen Bediensteten erbracht werden. Auf die Gefahren infolge der Durchbrechung der „informationellen Gewaltenteilung“ und der Missachtung des Gebots der Zweckbindung der Daten, die durch die Abwicklung des Zahlungsverkehrs durch die Gemeinde als „Erfüllungsgehilfe“ der Sparkasse entstehen, habe ich bereits im 9. Tätigkeitsbericht eindringlich hingewiesen.

In meiner Beanstandung habe ich deutlich gemacht, dass die Verarbeitung der Angaben über persönliche und finanzielle Verhältnisse der Sparkassenkunden des „Bürgerladens“ gegen das verfassungsrechtlich verbürgte Recht auf informationelle Selbstbestimmung (Art. 33 SächsVerf) dieser Bürger verstößt, da jede Datenverarbeitung durch öffentliche Stellen nach dem Grundsatz des Vorbehaltes des Gesetzes einer Ermächtigungsgrundlage bedarf. Eine spezielle Befugnisnorm für die Datenverarbeitung der Stadt bei der Durchführung von Aufgaben und Dienstleistungen der Sparkasse gibt es jedoch nicht. So darf die Gemeinde die Erbringung von Sparkassen-Dienstleistungen weder als eigene noch als übertragene Aufgabe wahrnehmen; weder die Sächsische Gemeindeordnung noch das Sächsische Datenschutzgesetz bieten hierfür eine Rechtsgrundlage.

Aber auch von einer auf § 4 Abs. 1 SächsDSG gestützten freiwilligen Einwilligung der Gemeindebürger in die Verarbeitung ihrer Daten kann nicht die Rede sein. Die faktische Alleinstellung des „Bürgerladens“ in der betreffenden Gemeinde ermöglicht dem Gemeindebürger, der zugleich Sparkassenkunde ist oder bleiben oder werden möchte, keine völlig freie und folgenlose Einwilligung in die Verarbeitung seiner Daten. Dazu muss man sich nur vor Augen führen, dass der Sparkassenteil des „Bürgerladens“ einen Fundus von Daten enthält, der zu unterschiedlichen kommunalen Verwaltungszwecken genutzt werden kann. Der künftige Verwendungszusammenhang der Daten ist im Zeitpunkt der Einwilligung für die betroffenen Gemeindebürger noch unklar.

Trotz dieser durchgreifenden Bedenken befürwortet das SMI weiterhin die Errichtung des „Bürgerladens“ und hält aufsichtsrechtliche Maßnahmen nicht für angebracht. Ich sehe darin eine Verletzung der Pflicht des SMI zu aufsichtsrechtlichem Einschreiten.

Gegen meinen ausdrücklichen und dringenden Rat wurde der rechtswidrige Vertrag zur Gründung des Bürgerladens zwischen der Pilotgemeinde und der Sparkasse vollzogen. Auch von der Möglichkeit, den Vertrag, der zunächst für den Zeitraum vom 1. März 2001 bis zum 1. März 2002 mit automatischer Verlängerung geschlossen wurde, zu kündigen, wurde von den Vertragsparteien bisher kein Gebrauch gemacht.

Ich beobachte zudem mit Sorge, dass dem Pilotprojekt inzwischen eine zweifelhafte

Vorbildwirkung zukommt, da sich sechs weitere Gemeinden in Sachsen für dieses „Modell“ interessieren.

Die angebotene Allumsorgung kann sehr schnell in eine Allherrschaft staatlicher wie kommunaler Stellen umschlagen. Hierzu sollte es nicht mehr kommen. Ich gebe auch zu bedenken, dass Gemeinden und ihre Bediensteten nicht als Dienstleister für Banken, Sparkassen, Fuhrunternehmer, Teledienstanbieter und sonstige Wirtschaftsunternehmen - so honorig und versorgungsbedeutsam sie auch sein mögen - auftreten dürfen.
Die Gemeinden in Sachsen sollten sich bei der Verarbeitung personenbezogener Daten auf ihr „Kerngeschäft“ beschränken. Da haben sie - weiß Gott - genug zu tun.

5.5.3 Gewinnung von Wahlhelfern unter Kommunalbediensteten, die nicht Bürger der betreffenden Kommune sind

Große und zunehmend mehr Mühe bereitet es den Gemeinden, Städten und Landkreisen ausreichend Wahlhelfer zu finden. Eine Großstadt trat daher mit der Frage an mich heran, ob es zulässig sei, anlässlich der Kommunalwahlen auch städtische Bedienstete, die nicht Bürger dieser Stadt sind, zur Mitarbeit in den Wahlorganen heranzuziehen.

Ich habe der Stadt sinngemäß wie folgt geantwortet: Nach § 10 Abs. 1 Satz 3 KomWG werden die Mitglieder der Wahlvorstände aus Wahlberechtigten *und* Gemeindebediensteten bestellt. Damit ist dieser Personenkreis eindeutig bestimmt und – nach ordnungsgemäßer Bestellung – auch berechtigt, die mit dem Wahlablauf einhergehende Datenverarbeitung vorzunehmen.

Zu beachten ist allerdings, dass eine Pflicht zur Übernahme solch ehrenamtlicher Tätigkeit gemäß § 17 SächsGemO für Bedienstete, die keine Bürger der Gemeinde sind, nicht in Betracht kommt. Sie können auch nicht durch dienstliche Anweisung, sondern ausschließlich aufgrund ihres freien Willens zur Mitarbeit bewegt werden. Ein entsprechendes Einverständnis sollte dokumentiert werden.

Ich füge hier hinzu: Grundsätzlich sollte in jeder Kommune darauf geachtet werden, dass die Wahlorgane nicht stärker mit öffentlich Bediensteten besetzt werden als unbedingt erforderlich. Es wäre ein (weiteres) Alarmzeichen für die Demokratie, wenn neben einer geringen Wahlbeteiligung auch keine ausreichende Bereitschaft zur ehrenamtlichen Mitarbeit im Wahlmanagement mehr bestünde. Um „Engpässe“ nach Möglichkeit zu vermeiden, sollten die Vorbereitungen nicht erst in letzter Minute anlaufen. Wahltermine sind zumeist lange genug bekannt.

5.5.4 Tonbandaufzeichnungen von Stadtratssitzungen

Ein Stadtratsmitglied bat mich um eine datenschutzrechtliche Bewertung folgenden Sachverhalts: Während nicht-öffentlicher Ratssitzungen lasse der Bürgermeister ein Tonband mitlaufen, um die Protokollierung der Beschlüsse zu erleichtern. Den Stadtrat interessierte insbesondere die Frage, ob diese Handhabung zulässig sei, und ob er ihr unter Hinweis auf sein „Recht am eigenen Wort" widersprechen könne.

Ich habe ihm wie folgt geantwortet:

Die Sächsische Gemeindeordnung sieht eine generelle Befugnis des Bürgermeisters, Tonbandmitschnitte zu fertigen, nicht vor. Dieser leitet als Vorsitzender des Gemeinderates (§ 51 Abs. 1 Satz 1 SächsGemO) dessen Sitzungen und vollzieht die Beschlüsse. Dafür ist eine wortlautgetreue Dokumentation des Sitzungsablaufs nicht erforderlich. Zwar ist gemäß § 40 Abs. 1 Satz 1, 1. Halbsatz SächsGemO eine Niederschrift über die Sitzung anzufertigen, jedoch nur zu den „wesentlichen Inhalten der Verhandlungen". Wenn und soweit es eine ausdrückliche Befugnis zum Tonbandmitschnitt in der Geschäftsordnung nicht gibt, richtet sich die datenschutzrechtliche Bewertung nach allgemeinen rechtlichen Maßgaben.

Ich habe die Auffassung vertreten, dass der Bürgermeister zu Tonbandaufzeichnungen der Ratssitzungen auch ohne Einwilligung des einzelnen Betroffenen ermächtigt sei, und zwar aus folgendem Grund: Zwar trifft es zu, dass das privat gesprochene Wort nur auf Tonband aufgezeichnet werden darf, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt oder der Betroffene eingewilligt hat (vgl. BVerfG NJW 1973, 891; BGH NJW 1995, 1955). Diese engen Grenzen gelten aber nur für das nicht öffentlich gesprochene Wort. Das kommunale Wahlmandat bewirkt, dass das Ratsmitglied nicht privat, sondern öffentlich, nämlich als Träger eines amtlichen Mandats tätig wird. Anders formuliert: In den Ratssitzungen herrscht das Prinzip der Öffentlichkeit (mit gesetzlichen Einschränkungen), das Ratsmitglied handelt dort öffentlich. In der Sitzung gibt es keine Privatsphäre, um deren Schutz es beim Datenschutz geht. Diese Form der „Öffentlichkeit" gilt auch für nicht-öffentliche Ratssitzungen.

Das Mitglied des Gemeinderates ist insoweit eine öffentlich-rechtlich handelnde Person. Für Personen, die im unmittelbaren politischen Willensbildungsprozess stehen, gelten nicht die Datenschutzregeln wie für private Bürger. Sie müssen sich vor allem - hier durch Protokoll - ihre wortwörtlichen Aussagen zurechnen lassen. Dient die Tonbandaufzeichnung allein diesem Zweck, ist sie also nur ein technisches Hilfsmittel zur Herstellung der gesetzlich vorgesehenen Niederschrift, so ist sie zulässig.

Dringend zu fordern bleibt allerdings die unverzügliche Löschung der Mitschnitte,

spätestens nach der Protokollbeschlussfassung. Dass Mitschnitte nicht zweckentfremdet genutzt werden dürfen, habe ich in 7/5.5.8 dargelegt.

5.5.5 Bruch der Schweigepflicht durch ein Ratsmitglied

Der Vorsitzende einer Stadtratsfraktion gab belastende Daten aus der Stasi-Überprüfungsakte einer Stadträtin an die Presse weiter. Zuvor hatte der Bürgermeister den sog. Ältestenrat, den der Stadtrat als Kontrollkommission mit der Überprüfung seiner Mitglieder beauftragt hatte, in die Überprüfungsakten sämtlicher Ratsmitglieder Einsicht nehmen lassen und in nicht-öffentlicher Sitzung über den möglichen Belastungsfall unterrichtet. Der Fraktionsvorsitzende, der die Daten als Mitglied dieser Kommission erhalten hatte, forderte später die - „natürlich“ einer anderen Fraktion angehörige - Betroffene öffentlich zum Rücktritt auf und gab als Begründung hierfür das belastende Material gegenüber der Zeitung preis. In seiner auf den Vorwurf der Schweigepflichtverletzung bezogenen Stellungnahme erklärte mir der Fraktionsvorsitzende, sein Wissen habe er bereits 1989/90 bei seiner Tätigkeit als Mitglied diverser Auflösungskommissionen gewonnen. Jedoch wurde er in der Zeitung zuvor - korrekt - damit zitiert, dass aus dem Material, „was wir von der Gauck-Behörde erhalten haben“, hervorgehe, dass die Betroffene dem MfS über Teilnehmer einer Jugendtouristreise in den Westen, über deren Verhalten und deren Gesprächspartner berichtet habe.

Damit hat das Ratsmitglied in eklatanter Weise gegen die Vorschriften zum Umgang mit Stasi-Unterlagen sowie gegen seine Geheimhaltungspflicht aus § 37 Abs. 2 SächsGemO verstoßen. Ich habe daher das Verhalten dieses Ratsmitgliedes gegenüber der Stadt gemäß § 26 SächsDSG beanstandet.

Der Fraktionsvorsitzende hat den Bruch der Verschwiegenheitspflicht in der Zeitung selbst formuliert. Und selbst, wenn es zutreffend wäre, dass er sein Wissen von seiner früheren Tätigkeit her hat, so hätte er dieses Wissen dann nicht mehr preisgeben dürfen, sobald es - wie geschehen - Gegenstand seiner Befassung als Stadtrat im nicht-öffentlichen Raum geworden ist. Nach dem klaren Gesetzeswortlaut legt die Nichtöffentlichkeit eines Vorgangs „einen Deckel“ auch auf solche Wissensbereiche, die vor der nicht-öffentlichen Befassung bekannt waren. Ein Stadtrat muss auch über sein Vorwissen schweigen, wenn es Gegenstand einer vertraulichen Erörterung im Stadtrat geworden ist!

Die Stadt habe ich ferner dazu aufgefordert, die Zuständigkeit des Ältestenrates durch eine klare Satzungsvorschrift zu regeln oder aber den vorgedruckten Text, mit

dem die Stadträte in die Überprüfung ihrer Stasi-Akten einwilligen, ausdrücklich auf den Ältestenrat zu beziehen, denn bisher war nur die Einverständniserklärung zur Überprüfung an sich enthalten.

Der Fall zeigt, dass die gebotene Aufarbeitung des DDR-Unrechts zuweilen nicht nach dem gesetzlichen Verfahren vorgenommen, sondern in den Dienst des politischen Kalküls gestellt wird. Wir dürfen uns aber im Rechtsstaat nicht mit absolutistischen Methoden unseren politischen Vorteil oder gar unseren moralischen Anspruch sichern. Der damit verbundene Verstoß gegen das Persönlichkeitsrecht schadet der Idee der Aufarbeitung.

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Änderung der Sächsischen Frauenförderungsstatistikverordnung

Die Sächsische Frauenförderungsstatistikverordnung (SächsFFStatVO) vom 22. August 1995 ist, wie ich 4/5.7.2 dargelegt habe, seinerzeit in zum Teil rechtswidriger Weise ausgestaltet worden (vgl. auch 5/5.7.1). Mit der Änderungsverordnung vom 14. September 2001 (GVBl. S. 664) hat die Staatsministerin für Gleichstellung von Frau und Mann im Einvernehmen mit dem SMI erfreulicherweise einem Teil der von mir geltend gemachten Einwände Rechnung getragen - wohlgemerkt als Maßnahme der Deregulierung und Verwaltungsvereinfachung.
Die unnötige Einbeziehung der Staatsministerin in die Übermittlungskette (§ 3 Satz 5, § 4 Satz 1) hat man abgeschafft, leider aber nicht diejenige der Ministerien (§ 3 Satz 1 bis 3). Auch die Beschränkung des Erhebungsprogramms auf das der gesetzlichen Ermächtigungsgrundlage entsprechende Maß (4/5.7.2 unter a) ist ausgeblieben. Dies beides wäre ebenfalls Deregulierung gewesen. Während andere Statistiken, die eine einwandfreie gesetzliche Grundlage haben, aus Kostengründen ausgesetzt werden, wird hier eine Statistik zum Teil ohne die nötige gesetzliche Grundlage fortgeführt. Hier hat man eine Chance verpasst.
Im Übrigen musste ich von der Staatsministerin für Fragen der Gleichstellung von Frau und Mann verlangen, dass sie es in ihrem nächsten „Bericht über die Anwendung des Sächsischen Frauenförderungsgesetzes und die Situation von Frauen im öffentlichen Dienst im Freistaat Sachsen“ vermeidet, Tabellenfeldwerte zu veröffentlichen, die kleiner als drei sind. Tabellenwerte unter drei sind eben - da sind sich die Fachleute einig - nicht anonym, sondern personenbezogen, also keine Statistik. Es ist z. B. nicht

mehr für irgendwelche Erkenntniszwecke der Öffentlichkeit bzw. der Wissenschaft (vgl. § 1 Abs. 1 Satz 1 SächsStatG) dienlich, wenn man erfährt, welchen Geschlechtes der eine vom SMUL in die „Landeskommission für den Wettbewerb ‚Unser Dorf soll schöner werden'" entsandte Vertreter ist und wie es insoweit mit den vom SMWA und vom SMUL in den Verwaltungsrat der Sächsischen Dampfschifffahrtsgesellschaft Entsandten steht. Statt Seite 62 bis 83 des bisher veröffentlichten ersten Berichtes hätte die auf Seite 61 genannte Zahl von 24 Prozent Frauenanteil bei Entsendungen in Gremien dieser Art wohl ausgereicht; schon gegen einen Mittelweg, nämlich die Angabe aggregierter Daten für jedes Ministerium, wäre datenschutzrechtlich nichts einzuwenden - diese Daten passten auf eine halbe Seite.

5.7.2 Fragebögen für Hochschulmitarbeiter zwischen Forschung und amtlicher Statistik

Ein Petent beschwerte sich darüber, dass an einer Technischen Universität alle Beschäftigten mittels eines von der Hochschulverwaltung verteilten Fragebogens - wenn auch ohne eine Auskunftspflicht geltend zu machen - nach ihrer Einstellung zu Umweltfragen, nach umweltschutzerheblichen Verhaltensweisen am Arbeitsplatz (z. B. beim Verbrauch von elektrischem Strom oder Papier oder beim Umgang mit Abfall) oder auf dem Weg zur Arbeit (Wahl des Verkehrsmittels), aber auch etwa danach befragt wurden, ob sie ein Naturkostangebot in der Mensa wünschten.

Um Ausfüllung des Fragebogens bat auf dem Begleitschreiben der Rektor unter Angabe seiner Amtsbezeichnung und unter Verwendung des amtlichen Briefbogens mit Logo der TU. Die ausgefüllten Bögen sollten an ein „Projektbüro Öko-Audit" geschickt werden; der Rektor erklärte im Anschreiben, die *Universitätsleitung unterstütze* das Projekt, in dessen Rahmen die Befragung durchgeführt werde, und habe Frau Professorin X als Vorsitzende der „*Kommission Umwelt*", und Professor Y, Inhaber der Professur für das Fach Z, mit der Leitung des Projektes *beauftragt.*
Es ist im Verlauf der Angelegenheit dann auch folgerichtig der Rektor - und nicht der eine oder andere einzelne universitätsangehörige Forscher - gewesen, der mir gegenüber die Weigerung ausgesprochen hat, meiner Aufforderung zu entsprechen, die Erhebung einzustellen und bereits ausgefüllte Fragebögen zu vernichten: Erhebende und speichernde Stelle war also die TU als juristische Person.

Der Petent hat sich zu recht beschwert und dem im Fragebogen gegebenen Hinweis, die Teilnahme sei anonym und *die Datenschutzbestimmungen würden eingehalten* - einem vielen Laien sehr leicht in die Feder fließenden Hinweis (ja, diesem Hinweis kann man entnehmen, dass er von einem Laien - mag er sich auch Jurist nennen dürfen - stammt) -, nicht getraut.
Entgegen der Argumentation der Hochschulleitung war das Beschaffen der Daten

(etwas anderes mag für deren Auswertung gelten!) rechtlich die Durchführung einer amtlichen Statistik, und nicht Datenerhebung im Rahmen ‚freier' Forschung.

(1) Für die rechtliche Einordnung war - wie bei jedem Handeln im Rechtsverkehr - das objektive Erscheinungsbild der Handlung maßgeblich. Das gilt insbesondere auch für statistische Erhebungen (vgl. schon 4/5.7.3 auf S. 77). Das Erscheinungsbild war hier eindeutig: Die Befragungsaktion war ein Handeln eines (vom Staat ‚eingesetzten', geschaffenen) Trägers öffentlicher Gewalt. Und wie der Rektor das Erscheinungsbild gewählt hatte, das war der Hochschule zuzurechnen, denn der Rektor ist gemäß § 94 Abs. 2 Satz 1 SächsHG *der* Repräsentant der Hochschule.

(2) Die Hochschule - als Institution, als Träger öffentlicher Gewalt - konnte sich für die Datenerhebung nicht auf die Vorschrift des § 4 Abs. 1 Satz 1 SächsHG stützen, wonach *die Hochschule* - also die Institution - *ihrer Aufgabenstellung entsprechend der Pflege und Entwicklung der Wissenschaft durch Forschung* u. a. *dient.* Ein solcher sehr allgemein formulierter Rechtssatz kann die Grenze zwischen dem Bereich der Ausübung des Grundrechts der Freiheit wissenschaftlicher Forschung (Art. 5 Abs. 3 GG, Art. 21 SächsVerf) und der übrigen - verwaltenden - Tätigkeit der Hochschule *als Institution* nicht verschieben. § 4 Abs. 1 Satz 1 SächsHG besagt daher nicht etwa, dass die Hochschule selbst bzw. ihre Organe die Aufgabe der Forschung hätten. Die Hochschule bzw. ihre Organe können nämlich schon rein tatsächlich gar nicht forschen; das tut nur der einzelne Hochschul-Wissenschaftler, in manchen Fächern sind das auch überwiegend größere Forschergruppen, aber eben nicht die Hochschulorgane.

(3) Auf den Umstand, dass mit den Daten ja auch geforscht werden sollte, konnte sich die Hochschule nicht stützen: Das Besorgen von Daten, gewissermaßen als Rohstoff von Forschung, ist rechtlich dann keine Forschung mehr - sondern Verwaltung -, wenn es, wie hier, durch die Verwaltung bzw. ein Organ der Hochschule unter Inanspruchnahme von dessen Eigenschaft als Verwaltung bzw. Organ stattfindet, statt durch den Forscher, mag letzterer auch das Erhebungsprogramm ausgearbeitet haben und die Daten dann auswerten. Diese Grenzziehung ist auch anderweitig von juristischer Bedeutung: Beschaffung und Bereitstellung von Forschungsmitteln ist rechtlich keine Ausübung der Wissenschaftsfreiheit, sondern z. B. gewöhnlicher Kauf- oder Werkvertrag. Das gilt in gleicher Weise für *Daten* als ‚Rohstoff' der Forschung, trotz des Umstandes, dass zugleich die Art und Weise der Datenerhebung im Falle der Verwendung von Fragebögen schon Teil der wissenschaftlichen Arbeit ist. Denn jede Maßnahme zur bloßen Erhöhung des Rücklaufes durch Ausübung *amtlicher Autorität* gegenüber den Befragten ist nicht mehr Bestandteil bloßer forschender Tätigkeit, einschließlich der fachgerecht-geschickten Gestaltung von Fragebögen, und ist insbesondere auch nicht Ausübung fachlich-wissenschaftlicher Autorität. Im Regelfall wird dem Rektor eine fachliche Kompetenz für das wissenschaftliche

Vorhaben, dem eine solche ‚offizielle' Befragung gegebenenfalls dient, ja fehlen, weil er mit hoher Wahrscheinlichkeit gerade nicht zufällig Vertreter des betreffenden Wissenschaftszweiges ist, sondern eines anderen Faches.

(4) Die Verwaltungsspitze der Hochschule darf demnach ihre Amtsautorität gegenüber den Hochschulangehörigen, insbesondere gegenüber den Hochschulbediensteten, nicht dazu benutzen, bestimmte auf Befragung angewiesene Forschungsvorhaben zu unterstützen. (Rechtlich anders zu beurteilen wäre die Unterstützung durch einen an die allgemeine Bevölkerung gerichteten Aufruf, also an Menschen, hinsichtlich deren die Hochschulverwaltung ganz offenkundig keinerlei rechtliche Befugnisse hat.)

(5) Als amtliche Statistik einer öffentlichen Stelle des Freistaates Sachsen (vgl. § 1 Abs. 1 SächsHG, § 2 Abs. 1 Nr. 5 SächsStatG i. V. m. § 62 Abs. 2 i. V. m. § 61 Abs. 1 Satz 1 SächsHG) war die von der Universitätsleitung veranstaltete Erhebung den Regeln des Sächsischen Statistikgesetzes unterworfen. Gemäß § 2 Abs. 1 Nr. 5 SächsStatG darf eine Universität als juristische Person des öffentlichen Rechts nur sog. Sekundärstatistiken durchführen (d. h. Statistiken im Verwaltungsvollzug, § 7 Abs. 1 SächsStatG). Denn § 2 Abs. 1 Nr. 5 SächsStatG ermächtigt die TU nicht, eine Primärstatistik zu erstellen, also eine Statistik, bei der die Daten aufgrund einer statistischen Zielsetzung originär ermittelt werden. Betrachtet man § 2 Abs. 1 Nr. 4 und 5 im Zusammenhang, ist der Gesetzesinhalt eindeutig: Zwar fallen die staatlichen Hochschulen gemäß § 2 Abs. 1 Nr. 5 unter das SächsStatG; aber gemäß Nr. 4 fehlt es für sie an einer Ermächtigung, Primärstatistiken durchzuführen; dasselbe gilt etwa für Kammern. Es fehlt insbesondere an der Ermächtigung, die Durchführung von Statistiken durch Satzung anzuordnen (Unterschied zu § 8 SächsStatG, also der Regelung für Gemeinden).

Einer gesetzlichen Erlaubnis zur Durchführung der Statistik bedarf es in solchen Fällen auch nicht etwa deswegen nicht, weil die Ausfüllung des Erhebungsbogens nicht zur Pflicht gemacht, die Teilnahme an der Befragung vielmehr ausdrücklich für freiwillig erklärt wird. In Sachsen bedürfen, wie auch nach dem Statistikrecht des Bundes und vieler anderer - allerdings keineswegs aller - Bundesländer, auch auf freiwilliger Grundlage durchgeführte amtliche Statistiken der gesetzlichen Erlaubnis. Das geht aus § 6 Abs. 3 Satz 1, Abs. 6 Satz 2, § 11 Abs. 1 und § 17 Abs. 6 SächsStatG hervor.

(6) Eine gesetzliche Ermächtigung in einem anderen Gesetz, namentlich dem Hochschulgesetz, war nicht ersichtlich. Die Datenerhebung durch die TU ließ sich insbesondere auch nicht auf das Sächsische Datenschutzgesetz stützen, insbesondere § 4 Abs. 1 Nr. 2 SächsDSG, also die Einwilligung des Betroffenen, konnte nicht als Rechtsgrundlage herangezogen werden. Da es sich bei einer solchen Datensammlung - wie dargelegt - um eine amtliche Statistik handelt, ist das Sächsische Statistikgesetz

das speziellere Gesetz, das dem Sächsischen Datenschutzgesetz als dem allgemeineren Gesetz kraft Spezialitäts-Vorranges vorgeht. Wollte man das Sächsische Datenschutzgesetz ergänzend anwenden, wäre dies eine Umgehung des Sächsischen Statistikgesetzes. Das Sächsische Datenschutzgesetz stellt nämlich an die Erhebung der Daten inso-weit weniger strenge Anforderungen als das Sächsische Statistikgesetz. Es ist aber nicht im Sinne des Gesetzes, dass die strengen Anforderungen des Statistikgesetzes - keine Primärstatistiken durch Hochschulen, es sei denn auf besonderer gesetzlicher Grundlage - durch die Anwendung des Sächsischen Datenschutzgesetzes (Primär-statistiken durch Hochschulen bei Einwilligung der Betroffenen) umgangen werden könnten.

(7) Auch in einem weiteren Punkt ist das Statistikrecht strenger: Für seine Anwendbarkeit reicht schon ein ausgesprochen schwacher Personenbezug der Daten aus: Der Begriff der „Einzelangabe“ im Statistikrecht ist weiter als der datenschutzrechtliche Grundbegriff des „personenbezogenen Datums“ (vgl. § 3 Abs. 1 SächsDSG). Das Statistikrecht erfasst immer auch Datenerhebungen mit von vornherein äußerst hohem Anonymisierungsgrad; dies habe ich in meinem 5. TB unter 5.7.3 im Einzelnen ausgeführt. Abgesehen davon, war der Einwand der Hochschule, die erhobenen Daten seien nicht personenbezogen, unbegründet. Denn am Ende des Fragebogens wurde nach der Tätigkeitsart (Hochschullehrer, Arbeiter u. a.), der höchsten Ausbildung (Hauptschule, Habilitation u. a.) der Fakultät, in der der Befragte angestellt war, dem Alter (Schrittweite zehn Jahre) und der Dauer des Beschäftigungsverhältnisses mit der TU (z. B. weniger als drei, mehr als zehn Jahre) gefragt. Das ermöglichte es, aus der Kombination der jeweils angegebenen Merkmalsausprägungen ohne allzu großen Aufwand zumindest in vielen Fällen auf den konkreten TU-Mitarbeiter zu schließen; dies war nicht nur meine Einschätzung, sondern auch gerade diejenige des Petenten.

(8) Nach zähem Ringen, insbesondere dem Aussprechen einer Beanstandungsandrohung meinerseits, habe ich mich mit der TU auf folgenden Kompromiss geeinigt:

- Verzicht des Sächsischen Datenschutzbeauftragten auf eine förmliche Beanstandung, gemäß § 26 Abs. 2 SächsDSG, sowie auf das Verlangen nach Löschen der Daten (sofortige Vernichtung der Fragebögen) - kurz: Duldung der Fortsetzung des Forschungsvorhabens -, allerdings mit der Maßgabe einer teilweisen Löschung und teilweisen Zusammenfassung von Merkmalsausprägungen im Schlussteil der Erhebungsbögen vor der Auswertung der Daten;
- Abgabe einer Erklärung der Universität, vertreten durch den Rektor, wonach die Universität es in Zukunft unterlassen wird, durch ihren Rektor in dessen amtlicher Eigenschaft bei Bediensteten der Hochschule dafür zu werben, dass diese sich im Rahmen von Forschungsvorhaben der Universität mündlich oder schriftlich befragen lassen.

(9) Von der Universität geäußerte Befürchtungen, meine Rechtsauffassung enge die Forschung ein, beruhten auf einem Missverständnis: Unverändert bleibt es bei der von mir im 4. TB unter 5.7.3, S. 78 Mitte dargestellten Abgrenzung: Soweit bei der Datenerhebung nicht an die Eigenschaft der Betroffenen, Hochschulangehörige zu sein, angeknüpft wird, üben die hochschulangehörigen Forscher keine öffentliche Gewalt aus und sind daher die von ihnen mittels statistischer Methoden durchgeführten Untersuchungen keine amtliche Statistik. Um dieses anhand eines Beispiels zu konkretisieren: Selbstverständlich darf ein Professor der Psychologie die Versuchspersonen auch, etwa durch Aushang an Schwarzen Brettern, unter den Studenten suchen - aber eben nur ohne Einschaltung eines Organs der Universität; denn Universitäten und ihre Organe forschen, wie gesagt, eben nicht, sondern sie verwalten. Forschung betreiben die Wissenschaftler ganz unabhängig von einer etwaigen Inhaberschaft eines Amtes in der Universitäts-Selbstverwaltung.

Ich erwarte, dass sich die sächsischen Hochschulen künftig an diese Regel halten.

Vgl. ferner zur Abgrenzung zwischen Forschungstätigkeit und Verwaltungstätigkeit auch unten Abschnitt 13.1.

5.7.3 Schein-Statistik betreffend Dienst- und Arbeitsunfälle

Ein Staatsministerium hat sich an mich gewandt, weil es die Durchführung einer „Statistik“ betreffend Dienst- und Arbeitsunfälle der Beschäftigten nicht nur des Ministeriums, sondern auch der dem Ministerium nachgeordneten Behörden plante. Hierzu sollte die für Personalangelegenheiten zuständige Stelle, welche die Dienstunfallmeldungen und Unfallanzeigen der Beschäftigten der Behörde entgegennimmt bzw. selbst ausfüllt und an den Unfallversicherungsträger (§ 193 SGB VII) bzw. das Landesamt für Finanzen (vgl. § 45 Beamtenversorgungsgesetz) weiterleitet, die für die Unfallstatistik erforderlichen Daten in eine Datei einstellen und diese Datei an die *Fachkraft für Arbeitssicherheit* (nach dem Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit - ASiG) des Ministeriums übermitteln. Der geplante Datensatz war auf das beschränkt, was eine Fachkraft für Arbeitssicherheit benötigt, um Ursachen von Unfällen zu untersuchen, wie es nach § 6 Satz 2 Nr. 3 Buchst. b ASiG ihre Aufgabe ist.

Dem Vorhaben stand datenschutzrechtlich nichts entgegen.
Die Fachkraft für Arbeitssicherheit in einer Behörde hat die Aufgabe, Ursachen von Unfällen, die sich in der Behörde ereignen, zu untersuchen. Zu diesem Zweck darf die Fachkraft zwar keine Unfallanzeigen einsehen, sie darf aber diejenigen Daten aus der Unfallanzeige erhalten, deren Kenntnis zu ihrer Aufgabenerfüllung erforderlich ist.
Hier sollten die Daten nicht an die für die jeweilige Behörde zuständige Fachkraft übermittelt werden, sondern an die Fachkraft des Ministeriums. Die Fachkräfte

für Arbeitssicherheit stellen innerhalb des gesamten Geschäftsbereichs eines Ministeriums, soweit der Freistaat selbst Rechtsträger der Behörden ist, eine einheitliche „Organisation“ dar. Daher bedarf es für die Weitergabe der Daten zwischen den Fachkräften für Arbeitssicherheit keiner Übermittlungserlaubnis. Die Fachkraft des Ministeriums darf also alle diejenigen Daten erhalten, die auch die Fachkraft der ihm jeweils nachgeordneten staatlichen Behörde erhalten darf.
Das Vorhaben war auch nicht als sog. *Statistik im Verwaltungsvollzug* nach § 7 SächsStatG anzusehen, wie das Ministerium ursprünglich angenommen hatte. Denn es sollen einzelne Datensätze innerhalb des „Netzwerkes“ der Fachkräfte für Arbeitssicherheit im Bereich der staatlichen Behörden im Geschäftsbereich des betreffenden Ministeriums ausgewertet werden können: Es soll auch die Möglichkeit offenstehen, einzelnen Unfällen oder Unfallquellen nachgehen zu können, so dass die Datenverarbeitung eben nicht rein statistischen Zwecken dient, sondern dem Verwaltungsvollzug. (Eine Statistik im Verwaltungsvollzug hingegen erlaubte, eben dem andersartigen Zweck entsprechend, nicht ohne weiteres die Übermittlung nicht-aggregierter Daten, gemäß dem Gebot der frühestmöglichen statistikunschädlichen Aggregierung; vgl. dazu zuletzt 9/5.7.2 auf S. 56).

5.7.4 Beanstandung großer Teile der „Kommunalen Bürgerumfrage 2002“ der Landeshauptstadt Dresden

Trotz der von mir vorher (vgl. § 8 Abs. 3 SächsStatG) nachdrücklich geltend gemachten und ausführlich begründeten Einwände gegen große Teile dieser Statistik hat der Dresdner Stadtrat die entsprechende Satzung (vgl. § 8 Abs. 1 Satz 2 SächsStatG) beschlossen; daraufhin hat die Stadtverwaltung die Erhebung durchgeführt.

Ich habe dies gemäß § 26 SächsDSG beanstandet, obwohl die Stadt mir eine grundsätzliche Billigung der umstrittenen Teile ihres Vorhabens vorgelegt hatte, die sie sich vorher vorsorglich vom SMI besorgt hatte.

1. Meine Beanstandung betrifft zunächst Fragen, die die Stadtverwaltung deswegen nicht hätte stellen dürfen, weil die Thematik den gesetzlichen Aufgabenkreis der Gemeinden und ihre Fähigkeit, die Aufgabe auch zu lösen, nicht berührt. Die Gegenstände dieser Fragen gehen die Stadtverwaltung darum nichts an, weil die zu gewinnenden Daten, also die Ergebnisse der Statistik, von der Stadt nicht zur Wahrnehmung einer ihr in unserer Rechtsordnung übertragenen Aufgabe benötigt werden. Eine solche aus der Rechtsordnung zu entnehmende Zuständigkeit ist aber erforderlich, weil jedes *wesentliche* Handeln eines Trägers öffentlicher Gewalt einer gesetzlichen Grundlage bedarf (Grundrechtslehre; Wesentlichkeitsdoktrin des Bundesverfassungsgerichts). Aus diesem verfassungsrechtlichen Grund ist die Erhebung personenbezogener Daten im Wege der amtlichen Statistik - und zwar

auch dann, wenn eine Auskunftspflicht nicht vorgesehen ist (vgl. § 6 Abs. 6 und § 11 Abs. 1 SächsStatG) - im Falle der Kommunalstatistik gemäß § 8 Abs. 1 Satz 1, Abs. 2 SächsStatG nur insoweit erlaubt, als die Gemeinde die Ergebnisse der Statistik *zur Wahrnehmung ihrer Aufgaben benötigt*. Für den für alle Bestandteile des Erhebungsprogrammes, also alle Erhebungsmerkmale, erforderlichen objektiven Informationsbedarf (vgl. auch § 1 Abs. 1 Satz 1, § 6 Abs. 3 Satz 1 SächsStatG) reicht dabei die *Dienlichkeit* der Ergebnisse der Auswertungen aus (§ 9 Abs. 6 Satz 1 SächsStatG); ausführlich dazu bereits 6/5.7.5 unter 3, S. 80.

Die Stadtverwaltung kann sich nicht etwa mit Erfolg darauf berufen, dass es ihre Aufgabe sei, statistische Informationen auch über den durch ihre eigene Tätigkeit begründeten Eigenbedarf hinaus zu sammeln, weil es zu ihren legitimen Aufgaben gehöre, jeden Interessierten über die in allen möglichen Lebensbereichen auf dem Gemeindegebiet anzutreffenden Verhältnisse zu unterrichten - als Darstellung der Stadt nach außen (Stadtmarketing) oder auch als sog. *Stadtforschung*.
Die Bereitstellung von Informationen für jedermann als Selbstzweck kommt nicht als Wahrnehmung legitimer Aufgaben der Gemeinde in Frage. Insoweit immerhin stimmt allem Anschein nach auch das SMI mit mir überein.

Was aber zum Aufgabenkreis der Gemeinde gehört, meint das SMI anhand des in Art. 28 Abs. 2 GG definierten Umfangs der Selbstverwaltungsgarantie der Gemeinden bestimmen zu können. Dieses Recht, „alle Angelegenheiten der örtlichen Gemeinschaft im Rahmen der Gesetze in eigener Verantwortung zu regeln“, bedeute, dass den Gemeinden bei ihrer Aufgabenerfüllung Allzuständigkeit zuerkannt sei. Damit bestehe eine *Zuständigkeitsvermutung* zugunsten der Gemeinden, die alle ihnen *zweckmäßig* erscheinenden öffentlichen Aufgaben in Angriff nehmen dürfen. Die Gemeinden dürften daher nicht *von vornherein* auf die Erfüllung enumerativ zugewiesener Aufgaben beschränkt werden. Ihnen stehe auch ein Aufgabenfindungsrecht zu. Grenzen finde die Allzuständigkeit erst, „wenn die Angelegenheit den Bezug zur örtlichen Gemeinschaft verliert oder wenn aufgrund des allgemeinen Gesetzesvorbehalts eine bestimmte Aufgabe bereits einem anderen Aufgabenträger zugewiesen und damit der gemeindlichen Befassung entzogen ist“ - so das SMI.

Um die Meinungsverschiedenheit zwischen dem SMI und mir noch einmal zu verdeutlichen: Das Verwaltungshandeln, um dessentwillen durch die amtliche Befragung in das Grundrecht auf informationelle Selbstbestimmung eingegriffen werden soll, bedarf nach Art. 33 SächsVerf einer gesetzlichen Grundlage. Mit anderen Worten: Die Aufgabe, zu deren Wahrnehmung die Ergebnisse der Statistik gemäß § 8 Abs. 1 Satz 1, Abs. 2 SächsStatG dienlich sein müssen, muss gesetzlich vorgesehen sein. Das folgt aus dem Verfassungsgrundsatz des *Vorbehaltes des Gesetzes*, der Folgerung aus dem Rechtsstaatsgrundsatz, Art. 20 Abs. 3 GG, und

dem Demokratieprinzip, Art. 20 Abs. 2 GG, ist. Soweit Grundrechte betroffen sind, dürfen die Kommunen nicht alle Angelegenheiten der örtlichen Gemeinschaft, die nicht durch Gesetz bereits anderen Trägern öffentlicher Verwaltung übertragen sind, ohne weiteres an sich ziehen - eben weil auch sie *Obrigkeit* sind und ihre Grundrechtseingriffe einer gesetzlichen Legitimation bedürfen. Jedes wesentliche Handeln der Verwaltung, auch der Kommunalverwaltung, bedarf nach der Wesentlichkeitsdoktrin des Bundesverfassungsgerichts einer gesetzlichen Grundlage. Art. 28 Abs. 2 GG sichert den Gemeinden zwar einen grundsätzlich alle Angelegenheiten der örtlichen Gemeinschaft umfassenden Aufgabenbereich (BVerfGE 79, 127 [143]). Moderne Selbstverwaltung beruht aber nicht auf Immunitätsprivilegien im Stile mittelalterlicher Städtefreiheit, sie ist der gesetzlichen Einwirkung zugänglich (BVerfGE 23, 353 [365]) und steht damit unter Gesetzesvorbehalt.

Anders ausgedrückt, das sog. Aufgabenfindungsrecht der Gemeinden besteht nur innerhalb der „allgemeinen, für staatliche Aufgaben notwendig geltenden Grenzen“, insbesondere der durch den Vorbehalt des Gesetzes gesetzten Grenzen (Dreier, GG-Komm., Rdnr. 104 zu Art. 28).

Nun könnte man - auf den ersten Blick scharfsinnig - einwenden, dass dieser *Vorbehalt des Gesetzes* sich auf den notwendigen Aufgaben-Bezug der Kommunalstatistik nicht auswirke, weil ja die nötige gesetzgeberische Regelung, insbesondere die gesetzliche Erlaubnis eines Grundrechtseingriffes, schon durch die in § 8 Abs. 1 SächsStatG erteilte Erlaubnis, auf Satzungsgrundlage Kommunalstatistiken durchzuführen, vorliege, dem Vorbehalt des Gesetzes also schon Genüge getan sei. Diese Überlegung führte jedoch zu einem absurden Ergebnis: Die Vorschrift würde dann dazu missbraucht, dass Kommunen für alles, was sie als für sich in Frage kommende Aufgaben ansehen, personenbezogene Daten sammeln dürften; das Statistikrecht erlaubte damit die Verarbeitung personenbezogener Daten im Wege der amtlichen Statistik, also einen Grundrechtseingriff, auch für Zwecke einer Verwaltungstätigkeit, die selber dann gar nicht rechtmäßig ausgeübt werden dürfte. Eine entsprechende Auslegung des Gesetzes gäbe diesem also einen verfassungswidrigen Inhalt: Dieser verstieße gegen den Grundsatz der Verhältnismäßigkeit. Denn er erlaubte einen Grundrechtseingriff zur Verfolgung rechtswidriger, nämlich unerlaubter Zwecke.

Der Wortlaut der Vorschrift legt eine solche Auslegung auch keineswegs nahe; er bietet vielmehr viel eher eine Grundlage für die von mir vertretene verfassungskonforme Auslegung, wonach die Gemeinden dann, wenn etwas zu dem vorausgesetzten, von der Rechtsordnung vorgesehenen Bestand an ihnen zukommenden Aufgaben gehört, dafür auch personenbezogene Daten im Wege der amtlichen Statistik sammeln dürfen. Es heißt in § 8 Abs. 1 Satz 1 SächsStatG „zur

Wahrnehmung *ihrer Aufgaben*“ und in § 9 Abs. 6 SächsStatG „Wahrnehmung *der* Aufgaben der Gemeinde“, also in beiden Fällen nicht lediglich unbestimmter „*von Aufgaben der Gemeinde*“. Das lässt sich zwanglos dahingehend verstehen, dass vorausgesetzt wird, dass es sich gesichertermaßen um rechtmäßige Gemeinde-Aufgaben handelt.

Zwar ist die Übertragung von örtlichen Angelegenheiten auf andere Träger hoheitlicher Gewalt nur gestattet, wenn den Gemeinden ein Kernbereich von örtlichen Aufgaben unangetastet erhalten bleibt. Bei dessen Bestimmung muss der geschichtlichen Entwicklung und den verschiedenen historischen Erscheinungsformen der Selbstverwaltung Rechnung getragen werden (BVerfGE 22, 180 [205]). Das bedeutet aber nicht, dass es den Gemeinden freigestellt wäre, sich neue, „bürgernahe“ Betätigungsfelder („öffentlich-rechtliche Spielwiesen“) zu suchen, auf denen sie z. B. durch Datenerhebungen grundrechtsbezogene Eingriffe dem Einzelnen gegenüber vornehmen.

Angelegenheiten der örtlichen Gemeinden sind solche Aufgaben, die in der örtlichen Gemeinschaft wurzeln *oder* auf sie einen spezifischen Bezug haben *und von ihr eigenverantwortlich und selbständig bewältigt werden können* (BVerfGE 50, 195 [201]). Diese Pflicht, nämlich dass die Gemeinden zur Erfüllung der Aufgaben berechtigt und in der Lage sein müssen, hat das SMI nicht erkannt. Wenn die Gemeinde also beispielsweise danach fragt, ob und wieviele Zeitungen jemand liest, dann müsste sie einen (verwaltungsrechtlich durchsetzbaren) Einfluss auf das Leseverhalten haben, etwa das Zeitungsangebot verbessern dürfen. Dieses Recht hat die Gemeinde Dresden sicherlich nicht. Deshalb gehen sie diese Daten nichts an.

Das Argument, die stadteigene Pressearbeit je nach Ergebnis der Antwort auszurichten, leuchtet ebenfalls nicht ein. Denn das Pressegesetz zwingt zur Gleichbehandlung aller Medien; Vorzugsinformationen sind unerlaubt. Presseerklärungen oder Hintergrundgespräche müssen allen Medien, gleich welcher Schattierung angeboten werden, erst recht allen Dresdner Tageszeitungen gleichmäßig.

Beispiele für von mir aus diesem Grund als unzulässig beanstandete Fragen, weil die Gemeinde Dresden am Ergebnis der Befragung nichts ändern kann:

- Wie beurteilen Sie Ihre persönliche wirtschaftliche Lage?
- Haben Sie sich aus Angst vor Ungewissheit, mangels Eigenkapitals oder fehlender Kreditwürdigkeit bei den Banken nicht wirtschaftlich selbständig gemacht?
- Entspricht Ihre Arbeitstätigkeit Ihrer beruflichen Qualifikation, oder sind Sie

eigentlich höher qualifiziert oder haben Sie einen anderen Beruf gelernt?
- Wie hoch war der Elektroenergieverbrauch Ihres Haushaltes entsprechend Ihrer letzten Jahresabrechnung?
- Wieviel Geld hat Ihr Haushalt für Hobbys, Diskothekenbesuche, Kurzausflüge und den Besuch von Gastwirtschaften ausgegeben?
- Beziehen Sie Erziehungsgeld, BAföG-Leistungen oder Pflegegeld?
- Wollen Sie aus beruflichen Gründen, wegen Beendigung des Mietverhältnisses, wegen Unstimmigkeiten mit dem Vermieter oder aus familiären Gründen umziehen?
- Wollen Sie in ein anderes der neuen Bundesländer, in eines der alten Bundesländer oder ins Ausland umziehen?
- Welche der vier Dresdner Tageszeitungen lesen Sie?
- Leiden Sie unter Alleinsein oder unter Eintönigkeit im täglichen Leben, haben Sie Partnerschaftsprobleme oder Übergewicht, machen Ihnen der Alkohol oder Ihre persönliche Erbanlage zu schaffen, oder mehr das Arbeitsklima am Arbeitsplatz; wie ist Ihr Wohlbefinden insgesamt?
- Leben Sie mit einem Lebenspartner des anderen oder des gleichen Geschlechtes zusammen?

Man braucht meiner Auffassung nach kein Jurist zu sein, um auf Anhieb zu erkennen, dass eine Stadtverwaltung auch im Rahmen einer Statistik nach dergleichen nicht fragen darf. Hier wird nichts anderes als „Meinungsmache“ betrieben. Die Verwaltung der Stadt plustert sich auf und erweckt den - falschen - Eindruck, sie könne das persönliche Wohlergehen der Befragten auf den vorgenannten Gebieten positiv beeinflussen. Hier begegnet uns die Stadt als Betreuer, als Vormund.

2. Des Weiteren habe ich beanstandet, dass die Stadt von den Befragten hat wissen wollen, welche Verkehrspolitik sie betreiben solle (z. B. Vorrang für den öffentlichen Personennahverkehr - ja oder nein), für welche Personengruppen (z. B. Ausländer, Jugendliche) sie mehr oder weniger als bisher tun solle und wer für Ordnung und Sauberkeit im öffentlichen Raum der Stadt verantwortlich zu machen sei, eher die Anwohner oder die Stadtverwaltung.
   Derartige Fragen sind, wie ich schon in meinem 4. TB dargelegt habe (Abschnitt 5.7.6 i. V. m. 5.7.4) unzulässig: Es handelt sich insoweit um eine sog. *konsultative Volksbefragung*. Die Einwohnerschaft ist in amtlicher, rechtlich geregelter Weise, also nicht unverbindlich durch irgendwelche Privatleute, nach ihrer kommunalpolitischen Meinung gefragt worden. Zugleich soll Ihre Meinung rechtlich aber unverbindlich sein. Das ist ein Widerspruch gegen das Prinzip der Volkssouveränität, und wegen dieses Widerspruches sind konsultative Volksbefragungen aus verfassungsrechtlichen Gründen unzulässig, weil das organisierte, in rechtlich geregeltem Verfahren seine Meinung bekundende Volk

der Souverän, die höchste Macht ist. Ich habe den Eindruck gewinnen müssen, dass diese Grundsatzfrage manchen sprachlos macht. Die gestellten Fragen sind nicht vom Volk, sondern vom Stadtrat zu beantworten; (nur) dafür ist er da. Wenn die Stadt und das SMI meinen, hier handele es sich nicht um verbindliche Antworten, man wolle sich ja nur ein politisches Bild machen, dann müsste man das den Befragten nicht nur sagen, sondern auch Aufwand und Ertrag der Aktion bedenken.

3. Schließlich war es rechtswidrig, dass die Stadt auch die 16- und 17-Jährigen in die Datenerhebung einbezogen hat, ohne eine Einwilligung der Sorgeberechtigten zur Voraussetzung zu machen. Von diesen Jugendlichen hat sich die Stadt die Daten rechtswidrig besorgt. Denn die von den betroffenen Minderjährigen mit Absendung des ausgefüllten Fragebogens hinsichtlich der preisgegebenen Daten stillschweigend („konkludent“) erklärte Verfügung über ihr Grundrecht auf informationelle Selbstbestimmung ist rechtlich unwirksam gewesen. Nach den allgemeinen Regeln, welche die Rechtsprechung für die Einwilligung Minderjähriger in Eingriffe in ihre höchstpersönlichen Rechte aufgestellt hat, ist auch noch ab dem 15. Lebensjahr neben der Einwilligung des Minderjährigen diejenige der Sorgeberechtigten erforderlich (vgl. Soergel/Siebert/Zeuner, 12. Aufl. 1998, Rdnr. 231 zu § 823 BGB; Steffen in: Löffler, Presserecht, Komm. 4. Aufl. 1997, Rdnr. 125 zu § 6 LPG).
   Dies gilt dann umso mehr, wenn, wie es hier der Fall gewesen ist, auch Fragen gestellt werden, die sich auf Verhältnisse beziehen, an denen andere Haushaltsmitglieder - und damit in aller Regel insbesondere die Erziehungsberechtigten - teilhaben, namentlich die rechtlichen und tatsächlichen Wohnbedingungen bis hin zur monatlichen Hypothekenbelastung, aber auch die von der Familie gehaltene Tageszeitung.
   Überdies hat die Einbeziehung der 16- und 17-Jährigen im Hinblick auf die vorstehend unter (2) erörterte abstimmungsähnliche Wirkung der Datenerhebung zur Folge, dass die insoweit stattfindende konsultative Volksbefragung den Kreis der Befragten gegenüber demjenigen der in Gemeindeangelegenheiten Abstimmungsberechtigten um die 16- und 17-Jährigen erweitert, wie auch übrigens um diejenigen, die nicht Staatsangehörige eines Mitgliedsstaates der Europäischen Gemeinschaft sind. Eine offizielle - für die Verwaltung der Stadt im Ergebnis verbindliche - Meinungsbildung steht diesen Bevölkerungsgruppen auf amtlicher Ebene nicht zu.

4. Die Statistik wurde nicht anonym erhoben. Vielmehr können viele Personen, die geantwortet haben, persönlich identifiziert werden. Viele Einzelfragen (z. B. nach dem genauen Stadtteil, der Hausgröße, dem Familienstand, dem Beruf, dem Alter, der Kinderzahl) eröffnen diese ganz nahe liegende Möglichkeit: Wie viele 56-jährige Beamte des höheren Dienstes mit 5 Kindern wohnen in einem

Einfamilienhaus in Dresden-Gorbitz? Erst recht mit Zusatzwissen können viele Antwortbogen bestimmten Personen zugeordnet werden. Es ist rechtswidrig, hier Anonymität vorzugaukeln.

Deshalb habe ich öffentlich dazu aufgerufen, die Fragebögen freiwillig nicht zu beantworten, sondern in den Papierkorb zu werfen.

Ich hoffe, dass ich endlich bei meinen Bemühungen, Wildwuchs bei der Kommunalstatistik der großen Städte entgegenzuwirken, die Unterstützung der Kommunalaufsicht und anderer staatlicher Stellen bekomme.

5.8 Archivwesen

5.8.1 Archivrechtliche Schutzfristen bei Unterlagen über die Beschäftigung von Zwangsarbeitern im „Dritten Reich“

Ein Petent, der sich in seinem Ruhestand mit der Geschichte seines früheren Betriebes, d. h. einer zu SED-Zeiten verstaatlichten und später abgewickelten Unternehmensgruppe, beschäftigt, hat sich an mich gewandt, weil sein Antrag auf Verkürzung der für personenbezogenes Archivgut geltenden Schutzfrist vom Hauptstaatsarchiv abschlägig beschieden worden war.

Die betreffenden Akten sollten nach der Erwartung des Petenten Aufschlüsse über die Beschäftigung von Zwangsarbeitern während der NS-Zeit liefern.

Die Archiv-Behörde hatte ihre ablehnende Entscheidung damit begründet, dass es im Hinblick auf die von ihr nach § 10 Abs. 4 Satz 2, 1. Halbs. SächsArchivG zu treffende Abwägungsentscheidung zwar keineswegs am grundsätzlich hohen, ja herausragenden öffentlichen Interesse an der Erforschung der Zwangsarbeiter-Beschäftigung fehle, dass aber das spezielle Vorhaben des Petenten mangels Veröffentlichungs-Absicht und wegen des geplanten lediglich chronikartigen Inhaltes der abzufassenden Ausarbeitung nicht ein bestimmtes Forschungsvorhaben sei, das ein nach § 10 Abs. 4 Satz 2, 1. Halbs. SächsArchivG zusätzlich notwendiges öffentliches Interesse behaupten könne, welches in der erforderlichen Weise die schutzwürdigen Belange der betroffenen Personen überwiege.

Was die Bewertung der Erarbeitung bloßer chronikartiger Darstellungen im Hinblick auf § 10 Abs. 4 Satz 2, 1. Halbs. SächsArchivG betrifft, hatte sich die Behörde dabei - zu Recht - auf meine diesbezügliche Stellungnahme von 7/5.8.3 berufen. Die bloße Zusammenstellung des Stoffes bzw. die Aufbereitung von Quellen-Inhalten kann nur eine Vorstufe für die Gewinnung und Darstellung wissenschaftlicher

Ergebnisse sein. Außerdem ist die Veröffentlichung von Forschungs-Ergebnissen der Normalfall: Die Mitteilung, die prinzipiell jedermann zugänglich ist, ist wesentlicher Zweck wissenschaftlichen Forschens; dies gilt nicht nur für den von Berufs wegen im Wissenschaftsbetrieb Tätigen. Die Weitergabe an interessierte ehemalige Arbeitskollegen, wie sie im vorliegenden Falle stattfinden sollte, reicht nicht aus. Andererseits wird man heutzutage auch schon eine Präsentation der Ergebnisse im Internet als hinreichende Veröffentlichungsform anerkennen können.

Bloßes Interesse an alten Zeiten reicht eben als Grund für den Eingriff in das Grundrecht auf informationelle Selbstbestimmung nicht aus, der stattfindet, wenn ein Archiv dem Persönlichkeitsrechtsschutz dienende Schutzfristen verkürzt.

Ich habe versuchen müssen, bei dem Petenten um Verständnis dafür zu werben. Allerdings war auch in diesem Fall zu beachten, worauf ich bereits (7/5.8.3) vorsorglich hingewiesen habe: Für Amtsträger gelten, soweit es um die Ausübung ihrer Amtstätigkeit geht, die persönlichkeitsrechtsschützenden Schutzfristen nicht (§ 10 Abs. 2 Satz 3, 1. Halbs. SächsArchivG), natürlich auch nicht für Funktionsträger im NS-Staat.

Daraus folgt für Unterlagen, welche die Beschäftigung von Zwangsarbeitern betreffen: Es ist sorgfältig zu prüfen, ob nicht Vorgesetzte der Zwangsarbeiter sowie Organe und Inhaber der Unternehmen - also diejenigen, welche die Zwangsarbeiter oder Häftlinge kommandiert oder bewacht haben - insoweit im Rahmen der Kriegswirtschaft eine amtsträgerartige Tätigkeit ausgeübt haben, eben mit der Folge, dass insoweit gemäß § 10 Abs. 2 Satz 3 SächsArchivG eine Schutzfristverkürzung gar nicht erforderlich wäre. Diese Frage müsste in solchen Fällen konkret im Hinblick auf die jeweils untersuchten Unternehmen bzw. Betriebe geprüft werden. Die - unveröffentlichte - Entscheidung des Bundesarbeitsgerichtes vom 10. Mai 2000 (5 AZB 3/00), die zum Ergebnis einer rein zivilrechtlichen Beziehung zwischen den Zwangsarbeitern und den sie beschäftigenden Unternehmen gelangt (unter I 2 a der Gründe), lässt dafür meines Erachtens doch durchaus Raum. Interessant ist dabei, dass § 10 Abs. 2 Satz 3, 2. Halbs. über § 4 Abs. 2 Satz 2 SächsArchivG die Tätigkeit in der unmittelbaren oder mittelbaren DDR-Staatswirtschaft datenschutzrechtlich als Amtsträger-Tätigkeit einstuft.

5.8.2 Die sonstigen öffentlichen Archive nach § 15 SächsArchivG

Im Zusammenhang mit der Suche nach sozialrentenrechtlich wichtigen, die sechziger Jahre betreffenden Abrechnungsunterlagen und Verdienstnachweise der damaligen Leipziger Bezirksabrechnungsstelle für Zahnärzte ging es um die später von der

Kassenzahnärztlichen Vereinigung sichergestellten und nunmehr verwahrten alten Unterlagen.

Anders als kommunale Körperschaften (§ 13 SächsArchivG) und Hochschulen sowie Akademien (§ 14 SächsArchivG) können sonstige der Aufsicht des Freistaates Sachsen unterliegende juristische Personen des öffentlichen Rechts, namentlich Körperschaften wie im vorliegenden Falle die KZV, ein eigenes Archiv im Rechtssinne betreiben, vorausgesetzt, die Staatsregierung stimmt dem zu; auch unterstehen diese Archive im Unterschied zu denen nach §§ 13 f. SächsArchivG der *Fachaufsicht* der staatlichen Archive (§ 15 Satz 1 SächsArchivG).

Wie sich herausstellte, hat die KZV Sachsen die Unterlagen zwar mustergültig verwahrt, um ein Archiv im Rechtssinne hat es sich freilich nicht gehandelt. Denn die erforderliche Zustimmung der Staatsregierung war nie beantragt worden, bei der Archivverwaltung war die KZV Sachsen als anbietungspflichtige Stelle geführt worden - mit Recht: Nach § 15 Satz 2 SächsArchivG haben diese Stellen, wenn sie kein eigenes Archiv im Rechtssinne unterhalten, die für die Aufgabenerfüllung nicht mehr benötigten Unterlagen dem örtlich zuständigen staatlichen Archiv zur Übernahme anzubieten.

Die KZV hat daraufhin auch ausdrücklich davon abgesehen, ein Archiv im Rechtssinne unterhalten zu wollen, und entsprechend angekündigt, die von ihr nicht mehr benötigten Unterlagen unverzüglich dem Sächsischen Hauptstaatsarchiv anzubieten. Das halte ich unter Datenschutz- wie auch unter Kosten-Gesichtspunkten für sinnvoll.

Das SMI hat mir versprochen, auf die anderen unter § 15 SächsArchivG fallenden juristischen Personen des öffentlichen Rechts, z. B. die KZV, die Kammern und die Sozialversicherungsträger, ein gesteigertes Augenmerk zu richten.

Auch in dem Falle, dass ein unter § 15 SächsArchivG fallendes Archiv in absehbarer Zeit nicht existiert, sollte der Gesetzgeber bei Gelegenheit § 15 um eine dem § 14 Abs. 2 SächsArchivG entsprechende Regelung ergänzen. Denn bisher ist der Zugang zu diesen Daten nicht zweifelsfrei archivrechtlich geregelt. Wie man vielmehr das Auskunfts- und Einsichtsbegehren Betroffener statt nach Archivrecht nach den Voraussetzungen des allgemeinen datenschutzrechtlichen Auskunftsanspruchs (§ 17 SächsDSG) zu beurteilen hätte, so müsste man wohl auch den Datenzugang zu Forschungszwecken nach vom Archivrecht abweichenden, weniger sachgemäßen Regeln des allgemeinen Datenschutzrechts (vgl. im Einzelnen 6/5.8.4) beurteilen.

5.8.3 Anspruch auf latent-eigene Daten nach § 6 SächsArchivG

Ein Landratsamt hat sich im Nachhinein vergewissern wollen, ob das Kreisarchiv recht daran getan hatte, einem von seinem Nachbarn auf Bestellung einer Dienstbarkeit nach § 116 SachenRBerG verklagten Grundstückseigentümer Ablichtungen von Teilen der das Klägergrundstück betreffenden Bauakte aus dem Jahre 1988 zur Verfügung zu stellen.

Das Kreisarchiv hatte korrekt gehandelt.
Rechtsgrundlage der Überlassung der Kopien war allerdings nicht, wie angenommen worden war, § 9 Abs. 1 (i. V. m. § 13 Abs. 3 Satz 1) SächsArchivG. Denn diese Vorschrift gilt, was die Nutzung personenbezogenen Archivgutes durch *Dritte* betrifft, nur vorbehaltlich der allgemeinen Schutzfrist für personenbezogenes Archivgut gemäß § 10 Abs. 1 Satz 3 SächsArchivG.
Diese allgemeine Schutzfrist gilt jedoch naturgemäß dann nicht, wenn der Betroffene *selbst* die Auskunft über die im Archivgut *zu seiner Person* enthaltenen Daten begehrt. Das aber war hier der Fall gewesen. Wenn in dem Grundstück meines Nachbarn eine Abwasserleitung genehmigt und gebaut wurde und z. B. heute eine weitere Leitung in mein Grundstück gelegt werden soll, um die Leitung des Nachbarn zu entsorgen, so sind *meine* Rechtsverhältnisse mittelbar durch den früheren Leitungsbau im Nachbargrundstück berührt worden. Das betrifft mich. Deshalb gehen mich die früheren Bauakten meines Nachbarn etwas an; ich will sie sehen. In solchen Fällen handelt es sich um Daten mit - latentem - Doppel- bzw. Mehrfachbezug, um Daten insbesondere, die sich auf die Person des Interessenten beziehen, obwohl sein Name in den Unterlagen gar nicht vorkommt.
Denn: Die rechtlichen Verhältnisse des Nachbargrundstücks (hier: Genehmigung einer Abwasserleitung durch die staatliche Bauaufsicht 1988) bewirken gegebenenfalls die Belastung des Grundstücks des Interessenten (Verpflichtung zur Bestellung eines Leitungsrechtes). Das Eigentum des Interessenten vermittelt den Personenbezug der Angaben über sein Grundstück als möglicherweise im Verhältnis zum Nachbargrundstück *dienendes* Grundstück. Mit anderen Worten: Den Interessenten betreffende personenbezogene Daten im Sinne des § 6 SächsArchivG sind nicht nur die Angaben über das in seinem Eigentum stehende Grundstück, sondern gerade auch diejenigen das Nachbargrundstück betreffenden Angaben, die sich auf das Recht (hier: Eigentum) des Interessenten an dessen eigenem Grundstück auswirken können. § 6 Abs. 1 Satz 1 SächsArchivG ist insofern irreführend eng formuliert, als die Vorschrift vorauszusetzen scheint, dass der Name des Auskunftsberechtigten in den Unterlagen enthalten sein muss (das „Soweit“-Tatbestandsmerkmal in Abs. 3 Satz 1 derselben Vorschrift ist begründeterweise demgegenüber *weiter* formuliert).

§ 6 Abs. 1 Satz 1 SächsArchivG ist insoweit verfassungskonform und in Einklang mit

der grundlegenden Bestimmung des § 2 Abs. 3 SächsArchivG („berechtigte Belange betroffener Personen“) auszulegen.

Der Interessent hat deshalb einen Anspruch auf Auskunftserteilung und Herausgabe von Ablichtungen der Unterlagen gemäß § 6 Abs. 1 (und auch Abs. 3) SächsArchivG gehabt.

5.8.4 Archivierung von Unterlagen mit Stasi-Daten: Archivierung als immanenter Zusatzzweck

Einem behördlichen Datenschutzbeauftragten waren Zweifel gekommen, als er erfuhr, dass bei der Anbietung von Personalakten an das zuständige Archiv (fünf Jahre nach Beendigung des Beschäftigungsverhältnisses oder Tod) der Erklärungsbogen zur Tätigkeit für das MfS aus der Personalakte entnommen und vernichtet und die Auskünfte des BStU, einschließlich Anlagen, an den Bundesbeauftragten zurückgeschickt werden sollten. Zu einer solchen Verfahrensweise hatte sich die Behörde durch Belehrungen gehalten gesehen, die der BStU formelhaft in seinen „gemäß §§ 20, 21 Abs. 1 Nr. 6 StUG“ gemachten Mitteilungen (Stand 2001) zu erteilen pflegte.

Die Zweifel waren berechtigt - aus welchem Grunde, das ist für Personalunterlagen oben unter 5.1.1 in Abschnitt 3 dargelegt. Das Problem stellt sich jedoch nicht nur für Personalakten, d. h. nicht nur für Daten, die der BStU nach § 21 Abs. 1 Nr. 6 StUG, also zur Personalüberprüfung im öffentlichen Dienst, übersandt hat. Für die Akten in Rehabilitierungsverfahren (vgl. §§ 20 und 21, jeweils Abs. 1 Nr. 1, StUG) und für die Akten von Strafverfolgungsbehörden (§ 23 StUG), aber auch etwa für solche der Waffenrechtsbehörden (§ 20 Abs. 1 Nr. 8 StUG) oder die Rentenversicherungsträger (§ 20 Abs. 1 Nr. 9 StUG) kann nichts anderes gelten.

Aus folgenden Gründen sind diese Unterlagen entgegen mitunter geäußerten Auffassungen schon nach geltendem Recht nicht von den allgemeinen Anbietungspflichten, die gegenüber den Archivbehörden bestehen, und von deren Übernahmeberechtigungen ausgenommen:

(1) § 8 Abs. 1 StUG steht nicht entgegen. Die Vorschrift bezieht sich auf Unterlagen, welche die öffentliche Stelle originär, jedenfalls gerade nicht vom BStU im Rahmen von dessen Übermittlungstätigkeit, erhalten hat (auch wenn die „Soweit-Einschränkung“ am Ende von § 6 Abs. 1 Nr. 1 StUG als zu eng anzusehen sein mag, vgl. Stoltenberg, Rdnr. 4 zu § 6, Rdnr. 2 zu § 8 StUG). Abgesehen davon dürfte die

Behörde nach Abs. 2 Satz 1 der Vorschrift eine Kopie behalten, hinsichtlich deren dann keine Herausgabepflicht bestünde.

(2) Auch die durch § 29 StUG statuierte Bindung der Verwendung der vom BStU übermittelten Daten an den Zweck, zu dem diese Übermittlung stattgefunden hat, steht der Archivierung nicht entgegen.

Archivierung ist ein potentiell immer möglicher, immanenter Annex-Zweck jedes primären Datenverarbeitungszweckes. Darin unterscheidet dieser Zusatz-Zweck sich nicht von den bekannten Annex-Zwecken der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, Rechnungsprüfung und der Statistik im Verwaltungsvollzug (vgl. § 12 Abs. 3 Satz 1 SächsDSG). Allerdings ist Archivierung nicht ein ergänzender Zweck, kein Begleit-Zweck, sondern ein Anschluss-Zweck - und zwar der letzte, also derjenige, nach dem legitimerweise kein anderer mehr kommt: 6/5.8.3! Dabei gibt es freilich eine Übergangsphase, in der die schon archivierten Daten noch dem ursprünglichen Primärzweck zugeführt werden können (vgl. § 10 Abs. 3 Satz 2 SächsArchivG); auch wirken persönlichkeitsrechtsschützende Vorschriften, die für die Verarbeitung personenbezogener Daten zur Verfolgung des Primärzweckes gelten, in dieser ersten Phase („Übergangsphase“) der Archivierung fort (§ 5 Abs. 7, vor allem 2. Halbs., SächsArchivG).

(3) Selbst wenn das StUG eine Löschungspflicht enthielte, wäre sie gemäß § 10 Abs. 3 Satz 2 SächsArchivG für sächsische Behörden wohl nicht beachtlich, wie sich aus den 9/5.8.1 ausgeführten Gründen ergibt.

Man kommt auf diese Weise zwanglos zu dem einzig praktisch sinnvollen Ergebnis: Eine historische Erforschung der Personalüberprüfung, die im öffentlichen Dienst der neuen Bundesländer nach dem Sturz des kommunistischen Herrschaftssystems stattgefunden hat, oder auch eine Untersuchung der Ausführung der Rehabilitierungsgesetze, wird nicht dadurch unmöglich gemacht, dass aus den Akten der Behörden und Gerichte, die damit befasst gewesen sind, besonders wichtige Stücke haben herausgenommen werden müssen, so dass man die Folgerungen, die in den Urteilen und Bescheiden aus den verwerteten BStU-Unterlagen gezogen worden sind, nicht kritisch nachvollziehen könnte.

Dass die Forschungen Zugang zu diesen Unterlagen nur unter Wahrung der dem Persönlichkeitsrechtsschutz dienenden archivrechtlichen Vorschriften erhalten darf, bedarf eigentlich keiner Erwähnung.

Vgl. auch unten 9.4.1.

5.9 Polizei

5.9.1 Rechtswidriger Abgleich von Bewerberdaten im Polizeilichen Auskunftssystem Sachsen (PASS)

Durch die Eingabe eines Petenten wurde ich darauf aufmerksam, dass eine Polizeidirektion das Polizeiliche Auskunftssystem (PASS) nicht nur zur Bekämpfung von Straftaten nutzt. Mittels PASS überprüft sie auch Bewerber für den Polizeidienst, die alle sonstigen Einstellungsvoraussetzungen erfüllt haben, sowie Polizeibeamte, die befördert werden sollen.

Diese offenkundig rechtswidrige weil zweckwidrige Nutzung begründet die Polizeidirektion damit, dass die Erfüllung der polizeilichen Aufgaben nur Beamten anvertraut werden könne, die in besonderer Weise vertrauenswürdig seien. Dies klingt bei unkritischer Betrachtung zunächst vernünftig, ist aber ein klarer Gesetzesverstoß, da es keine Rechtsgrundlage für diese Art der Nutzung polizeilicher Informationssysteme gibt:
Denn die PASS-Daten der Bewerber dürfen weder nach den Vorgaben der PASS-Errichtungsanordnung noch nach § 13 Abs. 1 SächsDSG (i. V. m. § 35 SächsPolG) für die beabsichtigte Überprüfung genutzt werden. Nr. 2 der Errichtungsanordnung erlaubt, die PASS-Daten im Rahmen der Gefahrenabwehr, zur Verhütung von Straftaten und zur Strafverfolgung zu verwenden. Nicht gestattet ist die Nutzung für Aufgaben der behördeninternen Personalverwaltung. Auch nach § 13 Abs. 1 SächsDSG ist die Erforderlichkeit des Zugriffs auf PASS-Daten zu verneinen. Die Personalverwaltung kann die für die Einstellung notwendigen Daten bei der jeweils zuständigen Behörde einholen. Dies ist der gängige Weg, den alle Behörden einschließlich der Polizei zu beschreiten haben.

Besonders ins Gewicht fällt zudem, dass eine PASS-Abfrage zur Kenntnis einer Vielzahl personenbezogener Daten aus dem Bereich vollzugspolizeilicher Aufgaben führt, die für die anstehende Entscheidung des Personalreferats überhaupt keine Bedeutung haben. Zudem handelt es sich bei den Daten zu einem großen Teil um nicht gesicherte Erkenntnisse, denen lediglich Verdachtscharakter zukommt. Die Folgen missbräuchlicher Interpretation liegen auf der Hand. Die Daten in PASS können nur Anhaltspunkte für weiteres präventives oder repressives Handeln und Ermitteln der Ermittlungsbehörden bieten. Eine negative oder positive Entscheidung bei der Personalauswahl können sie nicht tragen

Es bleibt somit festzuhalten, dass die Polizei in Personalfragen nicht ihr fachliches Informationssystem in einen „Selbstbedienungsladen“ umfunktionieren darf.

Diese Haltung, auf bloße Verdachtsdaten zurückzugreifen ist für manchen Behördenmitarbeiter der Griff nach dem Vorzugswissen, also der Griff nach der Macht. Dem beugt der Datenschutz vor: Alle Informationen, die für eine grundrechtsberührende Entscheidung, z. B. zum gleichen Zugang zu einem öffentlichen Amt nach Eignung, Befähigung und Leistung, zu verarbeiten sind, müssen stichhaltig, also überprüft und klar aussagekräftig sein. Hier bietet sich der Auszug aus dem Bundeszentralregister an; die dort gespeicherten Daten sind aufgrund rechtsgültiger Entscheidung zustande gekommen, sie sind valide.

Aus diesen Gründen habe ich in meiner Stellungnahme gegenüber dem SMI deutlich gemacht, dass die Erhebung von Bewerberdaten mittels PASS zu unterbleiben hat.

Ich werde weiter über den Fortgang der Angelegenheit unterrichten.

5.9.2 Rechtswidrige erkennungsdienstliche Behandlung von Kindern

Darf ein zwölfjähriger Junge zur Vernehmung auf ein Polizeirevier geladen und dort von drei Seiten fotografiert, d. h. erkennungsdienstlich behandelt werden? Mit dieser Frage wandte sich ein Verwandter dieses Kindes an meine Dienststelle und bat, die Rechtmäßigkeit dieser Maßnahme zu überprüfen. Meine daraufhin durchgeführte Kontrolle ergab folgenden Sachverhalt:

Das Kind gehörte nach Zeugenbeobachtungen zu einer Gruppe von sieben Kindern und drei Jugendlichen, aus der heraus ein parkendes Auto mit Fußtritten beschädigt worden war. Der Zwölfjährige und ein weiteres Gruppenmitglied wurden sodann von den herbeigerufenen Polizeibediensteten noch am Tatort angetroffen und anschließend ihren Eltern übergeben. Aufgrund von Zeugenaussagen konnten vier weitere Gruppenmitglieder ähnlichen Alters (mit Namen und Anschrift) ermittelt werden. Da zunächst unklar war, wer überhaupt zur Gruppe gehörte und wer getreten oder nur zugeschaut hatte, ordnete die sachbearbeitende Polizeibedienstete an, dass von allen ermittelten Kindern und Jugendlichen jeweils Lichtbilder aufgenommen und diese jeweils als Wahlbildvorlage vorgelegt werden sollten.

Diesen Sachverhalt bewerte ich wie folgt: Die Aufnahme von Lichtbildern der zum Tatzeitpunkt strafunmündigen und bereits mit Name und Wohnanschrift identifizierten Kinder war rechtswidrig. Personen unter 14 Jahren (Kinder) können nicht Beschuldigte sein, § 19 StGB. Lichtbilder dürfen deshalb nicht nach § 81 b, 1. Alt. StPO aufgenommen werden. Gegen Kinder sind zur Strafverfolgung anderer Personen allenfalls Maßnahmen nach § 163 b Abs. 2 StPO wie gegen einen Unverdächtigen zulässig. Danach dürften sie unter besonderer Beachtung des Verhältnismäßigkeitsgrundsatzes *zur Identifizierung* auch erkennungsdienstlich behandelt

werden. Da vorliegend der Name und die Anschrift der Kinder jedoch bereits bekannt waren und die Lichtbilder somit nicht zum Zwecke der Identitätsfeststellung, sondern zur Strafverfolgung aufgenommen wurden, kommt § 163 b Abs. 2 StPO als Rechtsgrundlage für die Aufnahme von Lichtbildern der strafunmündigen Kinder nicht mehr in Betracht.

Wegen der Schwere des Verstoßes und weil das verantwortliche Polizeirevier nicht mit der gebotenen Klarheit bestätigte, dass sämtliche Lichtbilder der Kinder vernichtet wurden, musste ich diese Maßnahme nach § 26 Abs. 1 Satz 1 Nr. 1 SächsDSG beanstanden. Ferner habe ich die Verantwortlichen aufgefordert, sämtliche angefertigten Lichtbilder der betroffenen Strafunmündigen unabhängig von Aufbewahrungsort oder Form der Speicherung zu vernichten und die entsprechenden Daten zu löschen. Das SMI habe ich aufgefordert, den Polizeidienststellen per Erlass erneut die Voraussetzungen der erkennungsdienstlichen Behandlung von Kindern und Jugendlichen zu verdeutlichen.

Das Polizeirevier wurde zwischenzeitlich auch vom Generalstaatsanwalt aufgefordert, die unrechtmäßig erstellten Bilder zu vernichten.

5.9.3 Öffentlichkeitsarbeit der sächsischen Polizei

Bei der Presse- und Medienarbeit der Polizeibehörden werden manchmal höchst sensible personenbezogene Informationen veröffentlicht. Andererseits gehört eine aktuell und authentisch informierte Presse (mit diesem Begriff meine ich auch alle anderen Medien) zu den wichtigsten Säulen eines demokratischen Rechtsstaats. Die Aufgabe des SMI besteht deshalb darin, die vorgenannten divergierenden Verfassungsprinzipien, genauer, das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht einer freien informierten Presse, miteinander in eine praktische Konkordanz zu bringen, also einen angemessenen Ausgleich dahin zu führen, dass beide Grundrechte sich möglichst weit entfalten können, ohne einander zu beeinträchtigen.

Ich habe dem SMI in diesem Zusammenhang unter anderem folgende Probleme unterbreitet:

1. Delikte von Trägern öffentlicher Ämter:

   Bei Berichten über rein amtsbezogene Tätigkeit des Inhabers eines öffentlichen Amtes (Bürgermeister, Professor, Polizeibeamter, Datenschutzbeauftragter etc.) entsteht zwar zunächst keine Grundrechtslage, weil die (private) Persönlichkeit des Amtsträgers jedenfalls in Bezug auf sein Verhalten im Amt nicht betroffen erscheint. Das ändert sich jedoch in dem Moment, in dem neben den rein

amtlichen Vorgängen auch persönliches Fehlverhalten im Amt geschildert wird, das natürlich auf die geschützte Privatsphäre durchschlagen kann und „hinter dem Amt den Menschen treffen“ kann. Das ist in Ermittlungsverfahren immer der Fall. Deshalb ist das Grundrecht auf informationelle Selbstbestimmung in diesen Fällen immer betroffen, denn es schützt die Privatsphäre und das Persönlichkeitsrecht auch dann, wenn sie nur deshalb beeinträchtigt werden, weil der Betroffene einen vorwerfbaren Fehler bei seiner Amtsausübung gemacht zu haben verdächtig ist.

2. Sachleitung der Staatsanwaltschaft im strafrechtlichen Ermittlungsverfahren:

   Die Sachleitungsbefugnis in strafrechtlichen Ermittlungsverfahren steht der Staatsanwaltschaft zu. Es gibt keine weitergehende, etwa früher einsetzende Strafverfolgungspflicht der Polizei und es gibt keine Vorverlagerung von Verantwortlichkeit etwa zu Zwecken der Vorsorge für die Strafverfolgung allein bei der Polizei. Vielmehr kann die Polizei einen Strafverfolgungsauftrag nur aus einem Auftragsverhältnis zur eigentlichen Inhaberin der Sachleitungs-Kompetenz, nämlich der Staatsanwaltschaft, ableiten (Näheres dazu im Karlsruher Kommentar zur Strafprozessordnung, 4. Auflage München 1999, § 152 Rdnrn. 16 ff. sowie § 163 Rdnrn. 2 ff.). Daraus ergeben sich für die Beurteilung der Rechtsprobleme, die gemäß § 4 des Sächsischen Pressegesetzes und gemäß § 15 des Sächsischen Datenschutzgesetzes zu entscheiden sind, konkrete Folgerungen: Denn nur die Staatsanwaltschaft kann letztgültig in einem laufenden Ermittlungsverfahren entscheiden, ob durch die Auskunft an die Presse die sachgemäße Durchführung eines schwebenden Verfahrens vereitelt, erschwert, verzögert oder gefährdet werden könnte (siehe § 4 Abs. 2 Nr. 2 Sächsisches Pressegesetz); die Polizei ist nicht dazu befugt, dies abschließend zu beurteilen. Folglich hat sie bei der Staatsanwaltschaft zu fragen, ob sie im laufenden Ermittlungsverfahren Presseauskünfte erteilt.

3. Schutz des Persönlichkeitsrechts:

   Es bedarf einer rechtsförmlichen und tatsachenbezogenen Abwägung, ob einer Auskunft an die Presse Vorschriften über die Geheimhaltung, insbesondere Vorschriften über den Persönlichkeitsschutz, entgegenstehen (§ 4 PresseG). Die damit verbundene Ermessensentscheidung ist schwierig und dann, wenn Informationen aus dem Privatleben veröffentlicht werden sollen und dadurch der gute Ruf einer ohnehin in der Öffentlichkeit stehenden Person (Schauspieler, Journalist, Arzt, Rechtsanwalt, Politiker) gefährdet sein könnte, nur unter einer juristisch fundierten Abwägung möglich, die aktenkundig zu machen ist. Dabei ist zu bedenken, dass Worte sich meist nicht mit Geld wiedergutmachen lassen und dass schlechte und herabsetzende Botschaften, die sich am Ende nicht bestätigen, nicht aus der Welt geschafft werden können. In einem möglicherweise

stattfindenden Verwaltungsverfahren (und evtl. anschließenden Verwaltungs- oder gar Strafprozess) muss der Betroffene durch Akteneinsicht die Gründe für die Veröffentlichung seiner Daten in allen Einzelheiten nachvollziehen können. Merke: Auch die Pressestelle ist gemäß § 17 SächsDSG zur Auskunft an den Betroffenen verpflichtet.

Ferner zwingt die Unschuldsvermutung des Art. 6 Abs. 2 MRK alle Beteiligten dazu, mit größter Sorgfalt und Zurückhaltung an derartige Probleme heranzugehen. Die immer wieder leichtfertig dahin gesagte Forderung nach „offensiver Pressearbeit“ ist daher juristisch gefährlich und dem rechtsstaatlichen und langfristig zu bedenkenden Ansehen der Polizei eher abträglich.

Als Vorschrift über den Persönlichkeitsschutz im Sinne des § 4 Abs. 2 Nr. 1 SächsPresseG kommt insbesondere § 15 des Sächsischen Datenschutzgesetzes in Betracht:

a) § 15 Abs. 1 Nr. 1 SächsDSG sieht vor, dass die Übermittlung personenbezogener Daten aus dem Privatleben der Betroffenen an private Stellen (die Presse ist eine solche private Stelle) nur dann zulässig ist, wenn dies zur Erfüllung der dienstlichen Aufgaben der übermittelnden Polizeidienststelle erforderlich ist. In Betracht kommen hier Fahndungsaufrufe (siehe die dazu bestehenden Sondervorschriften) und z. B. der Appell an Zeugen, sich zu melden. Dabei ist immer zu beachten, dass der Verhältnismäßigkeitsgrundsatz (Geeignetheit, Erforderlichkeit und Zumutbarkeit des Eingriffs) beim Eingriff in das Persönlichkeitsrecht der Person, deren Daten veröffentlicht werden, eingehalten wird.

   Eine allgemeine Informationspflicht gegenüber der Öffentlichkeit gehört nicht zu den gesetzlichen Aufgaben der Polizei. Die kurzatmige Pflege des Ansehens der Polizei - etwa durch Nachrichten über Erfolge - ist nicht Gegenstand gesetzlicher Erlaubnistatbestände.

   Die weitere - kumulativ zu erfüllende - Voraussetzung für die Datenveröffentlichung ist es, dass die Nutzung der Daten nach § 12 Abs. 1 bis 4 SächsDSG zulässig wäre. Ich erspare mir es an dieser Stelle, die einzelnen Voraussetzungen zu erwähnen; sie sind dem Gesetz bei sorgfältiger Lektüre zu entnehmen.

b) § 15 Abs. 1 Nr. 2 SächsDSG enthält alternativ die gesetzliche Erlaubnis, die Presse zu informieren, der man grundsätzlich ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten nicht absprechen kann, weil sie sich auf die Rechtsprechung des Bundesverfassungsgerichts zu stützen vermag, nach

der der Informationszugang für Presse und Medien zu den konstituierenden Merkmalen einer freiheitlichen Demokratie gehört. Jedoch muss die zweite - kumulativ vorliegende! - Voraussetzung ebenfalls erfüllt sein, nämlich, dass der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat. Man ist eigentlich an dieser Stelle so weit, wie man es nach dem bloßen Wortlaut des Pressegesetzes wäre: Es ist folglich immer zu prüfen, ob der Persönlichkeitsrechtsschutz des Betroffenen es gebietet oder auch nur nahelegt, die Veröffentlichung seiner Daten zu unterlassen. Dies dürfte der Regelfall sein, weil die Rechtsprechung insofern aus der Sicht des Betroffenen argumentiert, der seine wohlverstandenen Rechte geltend machen möchte. Niemand will an den Pranger gestellt werden; niemand möchte vorverurteilt werden.

Ferner ist zu bedenken, dass gemäß § 15 Abs. 3 SächsDSG im Falle des Absatz 1 Nr. 2 der Betroffene vor der Übermittlung zu hören und im Falle der Übermittlung zu unterrichten ist. Das gilt nur dann nicht, wenn dem schwerwiegende öffentliche oder private Belange entgegenstehen. Solche sind bei der üblichen Pressearbeit der Polizei nicht ersichtlich.

4. Personenbeziehbarkeit:

Die Erfahrung zeigt, dass die Frage nach der Anonymisierung von Pressemeldungen fast immer fehlerhaft beantwortet wird: Formulierungen wie „Bürgermeister S. aus W." oder „Der 91-jährige Pirnaer" oder „Der 42-jährige Porschefahrer und Filialleiter eines Dresdner Unternehmens" oder „Anja S. (siehe Foto)" sind personenbezogene Angaben! Das ist immer dann der Fall, wenn eine bestimmte oder bestimmbare Person mit - u. U. nur mit großer Mühe heranziehbarem - Zusatzwissen identifiziert werden kann.

Deshalb sind auch bruchstückhafte oder unzureichend verfremdete Informationen als „personenbezogene Daten" geschützt, sofern sie den Weg zu einer Person weisen oder ermöglichen.

Will man anonymisieren, so hat dies so zu geschehen, dass es wirklich unmöglich ist, jemanden zu identifizieren.

5. Polizeiliche Gefahrenabwehr:

Hier gilt zwar, dass die Verfahrensherrschaft bei der jeweils zuständigen Polizeidienststelle liegt. Die materielle Rechtslage in Bezug auf die Schranken, die § 4 Abs. 2 SächsPresseG setzt, gilt aber in gleicher Weise. Hinzu kommt, dass die präventive Polizeiarbeit nur selten auf die Veröffentlichung personenbezogener

Daten angewiesen sein dürfte. Warnungen vor bestimmten Personen, wie etwa im Fall Schmökel, bestätigen diese Regel.

6. Verantwortung des Behördenleiters:

   Es verdient betont zu werden, dass nur der zuständige Behördenleiter oder ein ausdrücklich von ihm Beauftragter zu Auskünften an Presse und Medien berechtigt ist. Dabei ist nicht „jeder Behördenleiter" gemeint, sondern derjenige, der tatsächlich letztverantwortlich zuständig ist. Pressearbeit muss deshalb „hochgezont" werden, um sicherzustellen, dass keine Verletzung des § 203 Abs. 2, § 353 b StGB vorkommt. Das Spannungsverhältnis dieser Vorschriften zu § 4 des Pressegesetzes kann nur so gelöst werden, dass der letztverantwortliche Behördenleiter die Pressearbeit verantwortet und persönlich koordiniert. Nur er unterliegt den (beamtenrechtlichen) allgemeinen Geheimhaltungspflichten nicht. Aber auch für ihn gilt, dass er das Abwägungspotenzial der vorgenannten Vorschriften des Presse- und des Datenschutzrechts ausschöpfen muss.

7. Pflicht zur Gleichbehandlung:

   Ein Anspruch der Presse auf Spontanmitteilungen seitens der Polizei besteht unter keinem rechtlichen Gesichtspunkt. Erst recht sind Bevorzugungen bestimmter Journalisten oder Presseorgane oder Medien zu unterlassen. Ich halte die bevorzugende und „dauerhafte", andere Medienvertreter ausschließende, Zusammenarbeit mit einem bestimmten Pressevertreter - z. B. weil man ihn gut kennt - nur dann nicht für datenschutzrechtlich unproblematisch, wenn sachliche Gründe dafür (aktenkundig) bestehen. Die „bewährt positive Berichterstattung" ist kein solcher Grund.

Ich halte die Erarbeitung einer klaren Dienstanweisung für die Pressestellen der Staatsanwaltschaften und der Polizeibehörden - auch im Hinblick auf gerichtliche Verfahren zum Persönlichkeitsschutz, die sich nach einer Presseveröffentlichung ergeben könnten - für unerlässlich. Meine Unterstützung dabei habe ich dem Innenministerium angeboten.

Ein besonderes Problem ist die Teilnahme von - meist „handverlesenen" - Presse- und Medienvertretern an Echt-Einsätzen der Polizei und anderer Behörden. Neben der Informationspflicht der Behördenleiter gemäß § 4 des Sächsischen Pressegesetzes - seine Anwendung setzt grundsätzlich eine aktive Nachfrage der Medienvertreter voraus - beobachte ich mehr und mehr auch das aktive Herantreten der Behörden an die Presse im Wege der „Öffentlichkeitsarbeit". Hier ist der Grundrechtsschutz strikt zu beachten. So viel Verständnis es für politische Notwendigkeiten - die sich ja

von Zeit zu Zeit auch ändern - geben mag und so sehr es richtig ist, dass die innere Sicherheit zu einem großen Teil aus Psychologie und einer (jeweils modischen) Haltung der Gesellschaft zur Polizei besteht, so wichtig ist es aber auch, dass sich der notwendige Schutz aller Grundrechte - er ist ja das Ziel der inneren Sicherheit - auch in den Richtlinien über die Zusammenarbeit der gefahrenabwehrenden Behörden mit den Medien manifestiert.

Ich halte es deshalb für notwendig, dass der gebotene Schutz des Persönlichkeitsrechts derjenigen Personen, die das Objekt polizeilichen Handelns sind, auch konsequent aufrecht erhalten wird. Deshalb - und weil dies im Gesetz keine Stütze findet - kann ich die Teilnahme von Journalisten und anderen Medienvertretern an Echt-Einsätzen der Polizei oder der Feuerwehr oder z. B. auch bei Kontrollen des Sozialamtes „vor Ort“ nicht billigen. Die formalen Regeln des Pressegesetzes würden dann verlassen. Die gebotene Abwägung zwischen dem - sicherlich im Grundsatz berechtigten - Informationsinteresse der Medien einerseits und dem Schutz des Persönlichkeitsrechts der Betroffenen andererseits kann nämlich nicht im Vorhinein stattfinden, sondern muss sich an bereits erfolgten Geschehnissen und den daraus sich ergebenden Erkenntnissen vollziehen. Mit anderen Worten: Im Einsatz oder nach dem Einsatz erst wird deutlich, ob es schutzwürdige Interessen der Betroffenen an einer Geheimhaltung der Vorgänge gibt. Ganz einfach gesagt: Nicht alles, was die Polizei am Tatort antrifft, gehört in die Zeitung. Ist es aber dem Journalisten, der mitgenommen wurde bekannt, so kann man ihm nicht verbieten, es zu veröffentlichen.

Vor einem polizeilichen oder sonstigen behördlichen Einsatz ist es noch ungewiss, wie tief die notwendigen Eingriffe der Behördenmitarbeiter in das Persönlichkeitsrecht der Betroffenen sein werden. Die Eingriffstiefe ergibt sich vielmehr aus der angetroffenen Situation und aus dem Verlauf möglicher Eskalationen. Eine Abschätzung und Gewichtung ist daher erst während oder gar nach der getanen Arbeit möglich. Deshalb kann eine abgewogene Information zum konkreten polizeilichen Handeln immer erst nachträglich möglich sein.

Nur der sachliche und persönlichkeitsrechtsschonende Journalismus verdient Unterstützung. Gerade dies müsste Aufgabe auch der polizeilichen Medienarbeit sein. Jeder von uns hat in den letzten Jahrzehnten den Eindruck gewinnen müssen, dass auch Verwaltungsstellen und auch Strafverfolgungsbehörden sich manchmal darin überbieten, möglichst mediengerecht zu agieren. Wie wohltuend ist es da, wenn sachliche, abgeklärte und emotionsfreie Informationen erteilt und verarbeitet werden. Anders gesagt: Wer unbedingt auf der Welle des Zeitgeistes surfen will, darf dies als Privatmann tun. Dem Staat, den Präventions- und Repressionsbehörden steht dies jedenfalls nicht gut zu Gesicht.

Zu diesen Fragen habe ich einen Dialog mit dem SMI geführt, das mir erste Thesen

mitgeteilt hat, die ich als eine vernünftige Grundlage für die nötige Dienstanweisung ansehe:

1. Sofern die Polizei beabsichtigt, der Presse personenbezogene Daten aus laufenden Ermittlungsverfahren zu übermitteln, muss die Staatsanwaltschaft als Herrin des Ermittlungsverfahrens darüber entscheiden, ob durch die Auskunft an die Presse die sachgemäße Durchführung eines schwebenden Verfahrens vereitelt, erschwert, verzögert oder gefährdet werden könnte.

2. Rechtlich zulässig ist es, personenbezogene Daten an die Presse zu geben, soweit dies zur Erfüllung der dienstlichen Aufgaben der Polizei erforderlich ist. In Betracht kommen hier Fahndungsaufrufe und zum Beispiel der Appell an Zeugen, sich zu melden.

3. Wenn Informationen aus dem Privatleben weitergegeben werden sollen und dadurch eine Rufschädigung einer Person, die bereits in der Öffentlichkeit steht (Schauspieler usw.), eintreten könnte, muss seitens der Polizei zuvor abgewogen werden, ob der Betroffene ein schutzwürdiges Interesse am Unterbleiben der Übermittlungen hat. Insbesondere ist dabei darauf zu achten, dass keine Vorverurteilungen stattfinden.

4. Film- und Hörfunkaufnahmen, welche die Polizei der Presse gestattet, bedürfen grundsätzlich der vorherigen Einwilligung der Betroffenen. Falls sie ohne Einwilligung erstellt worden sind, weil noch keine Gelegenheit zur Einholung der Einwilligung bestand, muss die Einholung nachgeholt werden. Ansonsten müssen identifizierende Aufnahmen nachträglich unkenntlich gemacht werden. Eine Einwilligung ist nicht bei Film- und Hörfunkaufnahmen von Personen erforderlich, die - ständig oder vorübergehend - im Blickfeld der Öffentlichkeit stehen und damit der Zeitgeschichte angehören. Bei diesem Personenkreis überwiegt das Interesse der Allgemeinheit an Informationen gegenüber dem Persönlichkeitsrecht der Betroffenen.

5. Generell ist bei Anonymisierungen darauf zu achten, dass die Personenbeziehbarkeit vollständig unmöglich gemacht wird. Dies ist zum Beispiel bei Formulierungen wie „Bürgermeister S. aus D." oder „...der 42-jährige Porschefahrer und Filialleiter eines Dresdner Unternehmens" nicht der Fall.

5.9.4 Entwurf einer Handlungsanleitung des LKA zu DNA-Analysen zur Aufklärung von Straftaten

Mit einer umfangreichen Handlungsanleitung wollte das LKA Sachsen das Verfahren von DNA-Analysen zur Aufklärung von Straftaten landesweit festlegen. Meine

datenschutzrechtliche Bewertung ergab, dass die Handlungsanleitung in zwei zentralen Punkten nicht mit dem geltenden Recht vereinbar war, weil sie in unzulässiger Weise den Anwendern suggerierte, dass die Speicherung von personenbezogenen Daten in der beim BKA geführten DNA-Analyse-Datei auch auf der Grundlage von Einwilligungen zulässig sei:

1. *Speicherung von Daten Beschuldigter auf der Grundlage von Einwilligungen zum Zweck der Identitätsfeststellung in künftigen Strafverfahren.*

Bei Beschuldigten verbietet sich grundsätzlich eine auf einer Einwilligung basierende Speicherung von Daten in der DNA-Analyse-Datei zur künftigen Strafverfolgung. Die molekulargenetische Untersuchung zum Zweck der Identitätsfestellung in künftigen Strafverfahren ist in den §§ 81 g und 81 f StPO geregelt. Voraussetzung ist danach, dass „wegen der Art und Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstige Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sind". Ferner schreibt das Gesetz unmissverständlich vor, dass die Untersuchungen durch den Richter angeordnet werden. Für eine Einwilligungslösung ist insoweit kein Raum. Grundrechtsschützende Verfahrensvorschriften können in einem Rechtsstaat nicht über Einwilligungen zur Disposition gestellt werden. Die Prognoseentscheidung muss von einem unabhängigen Richter getroffen werden und kann nicht durch eine Entscheidung des Beschuldigten in Form der Erteilung einer Einwilligung ersetzt werden. Zur näheren Begründung verweise ich auf meinen 8. Tätigkeitsbericht (8.4), in dem ich über die von mir gegenüber dem SMJus ausgesprochene förmliche Beanstandung in Bezug auf die sächsische Praxis der DNA-Analyse zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen berichtet habe.

2. *Speicherung von Opferdaten auf der Grundlage von Einwilligungen zum Zweck der Strafverfolgung*

Die Handlungsanleitung sah darüber hinaus vor, Opferdaten zu Strafverfolgungszwecken in die DNA-Analyse-Datei einzustellen, was einen schweren Rechtsverstoß bedeutet hätte. In diese beim Bundeskriminalamt geführte Datei dürfen nach § 81 g StPO nur Daten von Beschuldigten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren eingestellt werden. Damit steht eindeutig fest, dass ausschließlich Daten von Beschuldigten in diese Datei gelangen dürfen. Schließlich verbietet sich die Speicherung der Opferdaten aber auch, weil diese Daten zu einem anderen als dem nach § 81 g StPO erlaubten Zweck, nämlich Identitätsfeststellung in künftigen Strafverfahren, eingestellt werden sollen.

Nach dem Entwurf der Handlungsanleitung sollten die Opferdaten in die Datei aufgenommen werden, um Täter in einem bereits anhängigen Strafverfahren

zu ermitteln. Die DNA-Analyse-Datei dient jedoch dem Zweck, die Identität in künftigen Strafverfahren festzustellen. Die von der Handlungsanweisung beabsichtigte Einstellung von Opferdaten hätte zur Konsequenz, dass die Opferdaten automatisch zum Zweck der Identitätsfeststellung im künftigen Strafverfahren genutzt würden. In der Datei würden die Opferdaten mit den Daten von Beschuldigten mit Negativprognose vermischt, mit der Folge, dass die Opferdaten automatisch mit jeder neu in die Datei eingestellten Spur verglichen würden. Dies ist von dem im Gesetzeswortlaut eindeutig zum Ausdruck kommenden Willen des Gesetzgebers nicht umfasst und damit unzulässig.

Davon abgesehen ist fraglich, ob die von der Handlungsanleitung angestrebte Maßnahme zum Zweck der Strafverfolgung wirklich erforderlich ist. Die jetzigen Möglichkeiten reichen aus, um Sexualstraftäter zu überführen. Im Zusammenhang mit dieser Frage ist auch zu untersuchen, welche Beschuldigten in der polizeilichen Praxis überhaupt auf Fremdspuren hin untersucht werden. Sofern Beschuldigte regelmäßig nur dann auf Fremdspuren untersucht würden, wenn sie einer Straftat gegen die sexuelle Selbstbestimmung verdächtig sind, wäre es möglicherweise auch jetzt schon mit vertretbarem Aufwand möglich, den Beschuldigten aufgrund kriminalistischer Erkenntnisse (Tatort, Tatzeit, Tathergang, Täterbeschreibung etc.) mit anderen Strafverfahren in Verbindung zu bringen. In diesem Fall könnten die Opferdaten nach §§ 81 c, 81 e StPO molekulargenetisch untersucht und mit den aufgefundenen Spuren verglichen werden.
Mit diesen Argumenten habe ich mich an die Staatsministerien des Innern und der Justiz gewandt. Zwar konnte ich erreichen, dass auf die Speicherung der Opferdaten verzichtet wird, jedoch nicht verhindern, dass die Speicherung von Daten Beschuldigter zum Zweck der Identitätsfeststellung in künftigen Strafverfahren auf einer mit dem geltenden Recht nicht vereinbaren „Einwilligungsgrundlage“ fortgeführt wird. Ich werde deshalb meine Bemühungen fortsetzen, dass DNA-Analysen für künftige Strafverfahren nur nach richterlicher Anordnung vorgenommen werden.

5.9.5 Übermittlung personenbezogener Daten aus dem Polizeilichen Auskunftssystem Sachsen (PASS) auf Ersuchen öffentlicher und privater Stellen

Im Zusammenhang mit der Problematik der Aufrechterhaltung von PASS-Speicherungen trotz bereits erfolgter Verfahrenseinstellung nach § 170 Abs. 2 StPO habe ich die Frage untersucht, inwieweit die Übermittlung personenbezogener Daten aus PASS an andere öffentliche und private Stellen rechtmäßig ist. Auf Nachfrage teilte mir das LKA Sachsen mit, dass es jährlich etwa 1.800 Anfragen zur Ermittlung des derzeitigen Aufenthalts bzw. einer ladungsfähigen Anschrift von Personen erhält, bei denen das Landesarbeitsamt Sachsen offene Forderungen eintreiben möchte. Vor

diesem Hintergrund gehe ich davon aus, dass auch zahlreiche weitere öffentliche und private Stellen das LKA um die Übermittlung personenbezogener Daten ersuchen.

Aus datenschutzrechtlicher Sicht halte ich es für bedenklich, dass die Beantwortung dieser Anfragen durch das LKA auch zur Übermittlung solcher personenbezogener Daten führen kann, die nach einer Verfahrenseinstellung nach § 170 Abs. 2 StPO bereits gelöscht sein müssten und die nur aufgrund der bisherigen Verfahrensweise der Polizei bei der Löschung von Daten noch im PASS gespeichert sind. Darin sehe ich einen nicht erforderlichen und damit unzulässigen Eingriff in das Persönlichkeitsrecht der Betroffenen.

Ich werde deshalb die Übermittlung personenbezogener Daten durch die Polizeibehörden an andere Stellen einer grundsätzlichen Kontrolle unterziehen.

5.9.6 Auswertung von Protokolldaten zu Zwecken der Gefahrenabwehr

Im Berichtszeitraum hatte ich mich erstmalig mit einem Fall der Nutzung von Protokolldaten zu polizeifachlichen Zwecken zu befassen. Weil Protokolldaten, d. h. personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, gemäß § 12 Abs. 4 SächsDSG grundsätzlich einer zweckfremden Nutzung entzogen sind, wurde mit § 43 Abs. 1 a SächsPolG nachträglich eine gesetzliche Privilegierung für die Polizei geschaffen: So dürfen Protokolldaten nach Anordnung durch den Leiter des Landeskriminalamtes oder einen von ihm beauftragten Beamten auch zur Gefahrenabwehr sowie zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung verwendet werden. Die Vorschrift stellt ferner sicher, dass der Sächsische Datenschutzbeauftragte von der Maßnahme unverzüglich zu unterrichten ist.

Demgemäß erhielt ich im vorliegenden Fall die Mitteilung des LKA, dass Protokolldaten aus dem polizeilichen Informationssystem PASS zu Zwecken der Gefahrenabwehr ausgewertet werden sollten. Im konkreten Fall war mir daran gelegen, dass die zweckändernde Nutzung nur dann vorgenommen werden sollte, wenn sie im Trefferfall auch zu tatsächlichen Folgemaßnahmen der Polizei führen würde. Denn wenn die Polizei, schon vor der Protokolldatenauswertung absehen könnte, dass diese zu keinen geeigneten polizeilichen Maßnahmen führen würde, wäre diese Maßnahme zur polizeilichen Aufgabenerfüllung nicht erforderlich und damit unzulässig gewesen.

Diese rechtlichen Voraussetzungen waren vorliegend durch die Fallkonstellation erfüllt: Eine Polizeidienststelle eines anderen Bundeslandes fragte beim LKA an, ob im sächsischen PASS zu einem Halter eines Kfz, das verdächtig oft an dortigen

Kinderspielplätzen festgestellt worden war, Abfragen vorgenommen wurden. Die Geeignetheit der Maßnahme war damit gegeben.

Die Auswertung der Protokolldaten führte jedoch zu keinem polizeilich verwertbaren Ergebnis.

5.9.7 Personenverwechslung im Polizeilichen Auskunftssystem Sachsen (PASS)

Ein Petent hatte sich an mich gewandt, nachdem er einer polizeilichen Kontrolle unterzogen worden war. Seiner Schilderung nach stützten die Polizeibeamten ihre Kontroll- und Durchsuchungsmaßnahmen auf eine Eintragung in PASS, die ihn als Tatverdächtigen eines im Jahr 1994 begangenen Fahrraddiebstahls auswies. Der Petent beschwerte sich ferner über die unfreundliche Art und die Unterstellung eines der ihn kontrollierenden Beamten, er sei örtlich als Fahrraddieb bekannt und sein Benehmen habe ihn (den Polizeibeamten) an eine Kontrolle im vorigen Jahr erinnert.

Meine datenschutzrechtliche Kontrolle ergab, dass der Petent infolge einer Personenverwechslung tatsächlich zu Unrecht als Fahrraddieb in PASS registriert war. Seine Daten wurden daraufhin unverzüglich gelöscht.

Ich nehme den Fall zum Anlass, nochmals einen besonders sorgfältigen Umgang mit diesem polizeilichen Informationssystem anzumahnen. Nachlässigkeiten, die regelmäßig zu unzulässigen Grundrechtseingriffen führen, dürfen nicht hingenommen werden.

5.10 Verfassungsschutz

In diesem Jahr nicht belegt.

5.11 Landessystemkonzept / Landesnetz

In diesem Jahr nicht belegt.

5.12 Ausländerwesen

In diesem Jahr nicht belegt.

5.13 Wahlrecht

In diesem Jahr nicht belegt.

5.14 Sonstiges

5.14.1 Personenbezogene Datenverarbeitung durch das „Büro Frau Biedenkopf“

Das im Jahre 1991 von der Staatskanzlei eingerichtete, inzwischen aufgelöste Büro der Ehefrau des Ministerpräsidenten („Büro Ingrid Biedenkopf“, im folgenden „Büro“) habe ich im Juli 2001 einer (angekündigten) Kontrolle unterzogen.

Meine Kontrolle ergab, dass die Verarbeitung der in Bürgeranliegen enthaltenen personenbezogenen Daten durch das Büro sich nicht auf gesetzliche Grundlagen und in der Regel auch nicht auf die Einwilligung aller Betroffenen stützen ließ; die Datenverarbeitung war daher in vielen Fällen rechtswidrig. Des Weiteren trat bei der Kontrolle zutage, dass staatliche und kommunale Behörden dem Büro unter Verstoß gegen die gesetzlichen Übermittlungsvorschriften oder unter Verstoß gegen besondere Amtsgeheimnisse rechtswidrig personenbezogene Daten übermittelt hatten.

Im Einzelnen:

Das Büro war als Teil der Staatskanzlei öffentliche Stelle nach § 2 Abs. 1 SächsDSG. Die Ehefrau des Ministerpräsidenten gehörte als Mitarbeiterin dieser öffentlichen Stelle an; ihrer Tätigkeit entsprach am ehesten das Institut des „beschränkten öffentlich-rechtlichen Dienstverhältnisses“ (wie z. B. ein Lehrbeauftragter an einer Universität). Das Büro verarbeitete personenbezogene Daten über Betroffene, Verwaltungsbedienstete und Dritte, indem es sich z. B. bei anderen Stellen über die den Eingaben zugrundeliegenden Fälle erkundigte (Daten erhob), den Vorgang im Büro aufbewahrte (Daten speicherte) und das Ergebnis der Prüfung durch Verwaltungsjuristen bewertete und mitteilte (Daten nutzte und übermittelte). Das wäre nur zulässig gewesen, wenn eine Rechtsvorschrift dies erlaubt oder soweit der Betroffene eingewilligt hätte, § 4 Abs. 1 SächsDSG.

Eine gesetzliche Zuständigkeit des Büros bestand nicht. Vielmehr hatte die Verwaltung sich und dem Büro die Zuständigkeit zur Bearbeitung von Bürgeranliegen mit dem Ziel zweckmäßiger Erledigung selbst gegeben. Sein Gewicht erhielt das Büro durch seinen Namen und den damit verbundenen Nimbus der Staatskanzlei.
Auch das Sächsische Datenschutzgesetz konnte keine Rechtsgrundlage für die Datenverarbeitung durch das Büro sein. Gemeinsame Voraussetzung aller

Befugnisse zur Datenverarbeitung nach dem Sächsischen Datenschutzgesetz ist die Erforderlichkeit zur Aufgabenerfüllung. Mit anderen Worten: Nur wenn das Büro vom Gesetzgeber eine Aufgabe zugewiesen bekommen hätte, könnten sich die Befugnisse zur Datenverarbeitung im erforderlichen, d. h. zwingend notwendigen Umfang aus dem Sächsischen Datenschutzgesetz herleiten lassen (Grundsätze der Gewaltenteilung und des Vorbehalts des Gesetzes).

Eine solche Zuständigkeitsbegründung durch das Parlament ist indes im Fall des Büros nicht ersichtlich. Das Haushaltsgesetz ist nach Auffassung aller namhaften Verfassungsjuristen keine Rechtsvorschrift, die öffentlich-rechtliche Aufgaben und Befugnisse begründen oder modifizieren kann.

Der Datenverarbeitung durch eine öffentliche Stelle aufgrund einer Einwilligung steht häufig der Grundsatz des Vorbehalts des Gesetzes entgegen. Nur dann, wenn eine Aufgabe einer bestimmten Stelle durch Gesetz zugewiesen ist, ist sie berechtigt, die zu deren Erfüllung geeigneten, erforderlichen und zumutbaren Daten zu erheben und weiterzuverarbeiten. Die Einwilligung mag zwar einen Grundrechtseingriff nicht entstehen lassen, dies allein legitimiert eine öffentliche Stelle aber noch nicht zur Verarbeitung der solcherart „freigegebenen“ Daten. Denn durch die Einwilligung kann eine unzuständige Stelle nicht ihre Zuständigkeit begründen. Das folgt allein schon daraus, dass „wesentliches“ Handeln öffentlicher Stellen demokratisch legitimiert sein muss (Wesentlichkeitsdoktrin des Bundesverfassungsgerichts).

Unabhängig davon ist bei der Einwilligung stets deren Tragweite zu beachten: Zwar wird derjenige, der dem Büro sein Anliegen schriftlich vorgetragen hatte, in der Regel damit einverstanden gewesen sein, dass das Büro die in seinem Anliegen enthaltenen Daten nutzte und anderen Stellen in den Grenzen des angestrebten Zwecks übermittelte. Mit der Eingabe wird dieses Einverständnis in der Regel also schlüssig erklärt worden sein. Trotzdem hätten in jedem Einzelfall die Grenzen des mutmaßlichen Einverständnisses sorgsam ermittelt werden müssen. Denn nicht jeder, der das Büro angeschrieben hatte, war wohl damit einverstanden, dass - ohne vorher gefragt zu werden - diese Informationen an andere Stellen übermittelt wurden, zumal wenn es sich um heikle, problematische, die Gesundheit oder die wirtschaftliche Existenz berührende Informationen handelte. Bei meiner Kontrolle habe ich nicht den Eindruck gewinnen können, dass die Bediensteten des Büros insofern die im Einzelfall gebotene Sorgfalt walten ließen. Hierfür eines von vielen Beispielen:

> Eine Bürgerin, die durch Konkurs ihres Arbeitgebers ihre Arbeitsstelle verloren hatte, trug die Umstände dieses Konkurses dem Büro schriftlich vor. Nachdem sie in einem ersten Antwortschreiben darauf aufmerksam gemacht worden war, dass es sich hierbei um eine private Angelegenheit handele, schrieb sie in einem zweiten Schreiben:

> „Etwas befremdlich finde ich allerdings, dass Sie mein Schreiben komplett an das ... amt weitergeleitet haben. Der Teil des Schreibens über die Angelegenheit „XY“ war doch sehr privater Natur und ich dachte, dass Sie diesen vertraulich behandeln würden. So war ich natürlich sehr überrascht, als mir der Dienststellenleiter des ... amts X, Zweigstelle Z mitteilte, dass er mein vollständiges Schreiben an Sie vorliegen habe (...).“

Hinzu kommt, dass allenfalls der Petent seine Einwilligung in die Verarbeitung der ihn betreffenden Informationen hat geben können. Aber Prozess- und Verfahrensgegner, Nachbarn, beschuldigte Behördenbedienstete, also alle anderen Personen, deren Daten vorkamen - also verarbeitet wurden - wurden von der bemühten und engagierten „Helferin in allen Lebenslagen“ nicht gefragt; mit deren Daten hätte das Büro sicher nicht umgehen dürfen.

Verstöße gegen den Datenschutz habe ich auch auf Seiten der vom Büro um Mitarbeit gebetenen öffentlichen Stellen (Staatsministerien, Regierungspräsidien, Städte und Landkreise, Universitäten) festgestellt. Nicht selten hatten diese Stellen - unabhängig davon, ob das Büro darum gebeten hatte - mehr Informationen über die Petenten oder über Dritte an das Büro übermittelt als zur Beantwortung erforderlich gewesen wäre. In den Fällen, in denen das Büro um Informationen bei anderen Stellen gebeten hatte, trug das Büro gemäß § 13 Abs. 2 Satz 2 SächsDSG die Verantwortung für die Zulässigkeit der Übermittlung. Wurde mehr übermittelt als angefordert, traf diese Verantwortung die übermittelnde Stelle (§ 13 Abs. 2 Satz 1 SächsDSG). Dabei war auch gegen besondere Amtsgeheimnisse, z. B. das Sozialgeheimnis, verstoßen worden. In einem der ca. 500 von mir kontrollierten Fälle hatte ein hoher Beamter einen wohl eigens erstellten „internen Vermerk“ mit einer Fülle von Sozialdaten an die Ehefrau des Ministerpräsidenten übersandt.

In einem anderen Fall wandte sich eine Petentin X mit der Bitte an das Büro, ihr die Anerkennung als Kriegsopfer zu ermöglichen. Nebenbei erwähnte sie, dass sie eine Rente in Höhe von nur ... DM erhalte. Nachdem die Ehefrau des Ministerpräsidenten versprochen hatte, sich kundig zu machen, erschien in den Unterlagen folgender Vermerk über ein Telefongespräch mit einem hohen Beamten:

> „(...) Beim Sozialamt existiert eine sog. Seniorenliste, auf der alle Altersrentner registriert sind. Dort taucht der Name von Herrn X, aber nicht von Frau X auf. Deshalb vermutet das SMS, dass Frau X Erwerbsunfähigkeitsrente erhält und es sich bei dem registrierten Herrn X möglicherweise um den Ehemann handelt (...).“

Mit der Übermittlung des Datums, dass ein Herr X auf der „Seniorenliste“ als Bezieher von Altersrente registriert ist, verletzte das Ministerium das Sozialgeheimnis, § 35 SGB I, wonach jeder Anspruch darauf hat, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden. Die Voraussetzungen, unter denen Sozialdaten befugt übermittelt und damit offenbart werden dürfen, §§ 67 d ff. SGB X, wurden nicht beachtet. Dies verstieß gegen den Sozialdatenschutz.

Eine Fülle weiterer Beispiele rechtswidriger Datenverarbeitung musste ich feststellen.

Insgesamt ergab die Kontrolle, dass bei der Verarbeitung personenbezogener Daten durch das Büro datenschutzrechtliche Vorschriften nicht beachtet worden sind. Ich habe deshalb gegenüber der Sächsischen Staatskanzlei eine Beanstandung aussprechen müssen. Wegen der grundsätzlichen Bedeutung der schwerwiegenden Verstöße gegen datenschutzrechtliche Vorschriften habe ich den Sächsischen Landtag nach § 27 Abs. 2 SächsDSG über die Angelegenheit unterrichtet (DS 3/4795).

Merke: So gut die Absicht auch sein mag, die Gesetze sind zu beachten. Der Zweck heiligt nämlich nicht die Mittel.

5.14.2 Prüfkriterien für rechtmäßige Videoüberwachungen

Immer häufiger setzen öffentliche Stellen zur Wahrnehmung ihres Hausrechts und zur Vermeidung von Straftaten Videotechnik ein. Bei Kontrollen dieser Videoüberwachungsanlagen musste ich in den meisten Fällen erhebliche Mängel feststellen.

Aus diesem Grunde halte ich es für unerlässlich, dass sich öffentliche Stellen vor jedem Einsatz dieser Technik, der immer auch in das Recht auf informationelle Selbstbestimmung eingreift, folgende Fragen stellen:

- Wer ist Inhaber des (öffentlichen) Hausrechts? Wer trägt die Verantwortung für die Video-Daten-Verarbeitung?

- Welche Gefahren sind wirklich vorhanden und greifbar?

- Ist der Videoeinsatz überhaupt geeignet, etwas zu bewirken, z. B. Störer frühzeitig festzustellen und Gefahren wirklich abzuwehren? Nach meiner Erfahrung wird diese Frage nur selten ehrlich und realistisch beantwortet.

  Kann die öffentliche Stelle diese Fragen mit positivem Ergebnis beantworten, muss sie die weiteren Zulässigkeitsvoraussetzungen beachten:

- Dokumentation der eingesetzten Videoüberwachungstechnik (entsprechend dem Datei- und Geräteverzeichnis nach § 10 SächsDSG); das sind präzise die Standorte, die jeweiligen Aufnahmebereiche und die eingesetzten Aufzeichnungs- und Speicherungsverfahren.

- Maßnahmen zur Gewährleistung des Datenschutzes bei der Videoüberwachung entsprechend dem Datenschutz- und Sicherheitskonzept nach § 9 SächsDSG; hierzu gehören auch bei Aufzeichnungen die Festlegung der Speicherungsdauer (48 Stunden dürften in der Regel ausreichend sein).

- Deutliche Hinweise auf die Videoüberwachung, z. B. durch Schilder mit Angabe des Überwachungszweckes und eines Ansprechpartners der für die Datenverarbeitung verantwortlichen Stelle (vgl. Art. 10 der EG-Datenschutzrichtlinie vom 14. Oktober 1995).

- Sofern eine private Stelle mit der Durchführung der Videoüberwachung beauftragt wird, ist ein entsprechender Vertrag über die Auftragsdatenverarbeitung abzuschließen (vgl. § 7 SächsDSG); in diesem Vertrag müssen die Kontrollrechte des Sächsischen Datenschutzbeauftragten garantiert sein.

- Erfasst die Videoüberwachung auch Bedienstete der betreibenden öffentlichen Stelle, liegt eine Personaldatenverarbeitung vor. Deshalb sind zusätzlich folgende Punkte zu beachten:

- Abschluss einer Dienstvereinbarung der Dienststellenleitung mit dem Personalrat über die Videoüberwachung nach § 31 Abs. 1 SächsDSG.

- Herstellen des Benehmens mit dem Sächsischen Datenschutzbeauftragten gemäß § 31 Abs. 7 SächsDSG.

Ich fordere alle öffentlichen Stellen des Freistaates Sachsen auf, diese Kriterien vor jedem Videoeinsatz zu beachten.

6 Finanzen

Ausstellung einer weiteren Lohnsteuerkarte beim Arbeitgeberwechsel

Ein Petent sah den Datenschutz bei Arbeitnehmern durch die gegenwärtige Lohnsteuerkartenpraxis verletzt. Er kritisierte, dass bei einem Arbeitgeberwechsel während des laufenden Kalenderjahres auf der Rückseite der Lohnsteuerkarte der bisherige Arbeitgeber den bezogenen Arbeitslohn einzutragen habe. Auf diese Weise erhalte der neue Arbeitgeber Kenntnis von schützenswerten Daten aus einem Dienstverhältnis. Der Petent sah in der Ausgabe einer zweiten Lohnsteuerkarte eine Möglichkeit, Abhilfe zu schaffen.

Ich habe dem Petenten wie folgt geantwortet:

Die Datenschutzbeauftragten des Bundes und der Länder bemühen sich seit mehr als zehn Jahren bei dem für Steuerangelegenheiten zuständigen BMF um eine Änderung des derzeitigen Verfahrens. Übereinstimmend vertreten sie die Auffassung, dass es im Hinblick auf das Recht auf informationelle Selbstbestimmung einem Arbeitnehmer überlassen bleiben sollte, ob er beim Wechsel des Arbeitgebers während des Kalenderjahres dem neuen Arbeitgeber seine bisherige Lohnsteuerkarte vorlegt und damit seine Einkünfte offenlegt oder sich eine weitere Lohnsteuerkarte ausstellen lässt. Eine solche Verfahrensänderung jedoch würde eine Änderung des Einkommensteuergesetzes (§§ 39 b ff. EStG) voraussetzen. Dies hat das BMF bis heute abgelehnt.

Im Juli 2001 hat der Bundesbeauftragte für den Datenschutz erneut vorgeschlagen, die jetzige Regelung über die Ausstellung von Ersatz-Lohnsteuerkarten zugunsten der Arbeitnehmer, die ihren Arbeitgeber wechseln, dahingehend zu erweitern, dass auf der Ersatz-Lohnsteuerkarte nicht mehr wie bisher die Steuerklasse VI (§ 39 c Abs. 1 EStG), sondern die für die monatliche Besteuerung maßgebende Steuerklasse eingetragen wird.

Das BMF hat gegen diese Lösung eine Reihe von Einwendungen erhoben, insbesondere den Verwaltungsaufwand und das Missbrauchsrisiko. Ein weiteres Argument ist, dass sich das jetzige Verfahren mit der Einführung einer *elektronischen Lohnsteuerkarte* in absehbarer Zeit ohnehin erledige.

Wie zu erfahren war, wird das neue Verfahren derzeit in Pilot-Projekten getestet und soll bis spätestens 2005 bundesweit eingesetzt werden. Es bietet dem Arbeitgeber die Möglichkeit, die bisher auf der Lohnsteuerkarten-Rückseite zu bescheinigenden Daten elektronisch an die Finanzverwaltung zu übermitteln. Damit liefert jeder

Arbeitgeber nur die Daten für den Zeitraum, in dem der Arbeitnehmer bei ihm beschäftigt war. Diese Daten werden sodann im Rahmen der Veranlagung des Arbeitnehmers beim Finanzamt, das die Daten des Arbeitnehmers aggregiert, ausgewertet. Die Lohnsteuerbescheinigung für den Arbeitnehmer ist dann nicht mehr die Lohnsteuerkarte, sondern eine Bescheinigung des Arbeitgebers über die an die Finanzverwaltung gelieferten Daten. Folglich entfällt damit auch die Verpflichtung des Arbeitnehmers, dem neuen Arbeitgeber die Lohnsteuerkarte auszuhändigen (§ 39 Abs.1 EStG).

Da jedoch für einen Arbeitgeber kein Zwang besteht, sich an dem Verfahren zu beteiligen, besteht das datenschutzrechtliche Problem weiter. Die Datenschutzbeauftragten werden sich im Zuge der für das elektronische Verfahren notwendigen Gesetzesänderung noch einmal für eine Änderung des *nicht elektronischen* Verfahrens einsetzen. Allerdings versprechen weitere Bemühungen in dieser Richtung angesichts der ablehnenden Haltung des BMF wenig Erfolg.

7 Kultus

7.1 Datenschutz in der Schule

In diesem Jahr nicht belegt.

7.2 Kirchlicher Datenschutz

In diesem Jahr nicht belegt.

8 Justiz

8.1 Entwurf eines Straftäter-Unterbringungsgesetzes

Im Berichtszeitraum brachte die Mehrheitsfraktion im Sächsischen Landtag den Entwurf eines „Gesetzes über die Unterbringung besonders rückfallgefährdeter Straftäter“ (Straftäter-Unterbringungsgesetz - Drucksache 3/5343) ein.

Mit dem Entwurf sollte - wie in Bayern, Baden-Württemberg und Hessen - die Rechtsgrundlage dafür geschaffen werden, als „besonders gefährlich eingeschätzte Strafgefangene“ nachträglich zum Zwecke der Gefahrenabwehr wie in einer Sicherungsverwahrung unterbringen zu dürfen - was letztlich bedeuten würde, dass der Landesgesetzgeber seinen Zuständigkeitsbereich verlässt und auf dem Gebiet des Strafrechts gesetzliche Regelungen schafft. Weil die Ausführung des geplanten Gesetzes die umfangreiche Sammlung von - häufig äußerst sensiblen - Informationen über Gefangene während ihrer Haftzeit bedingen würde, habe ich mich mit folgender Argumentation an den Sächsischen Landtag gewandt:

1. Das Institut der Sicherungsverwahrung, dem ich den Gesetzentwurf trotz seiner anderslautenden Begründung wegen seiner tatsächlichen Anlehnung an Motive und Ausgestaltung der strafrechtlichen Sicherungsverwahrung zuordne, ist ausschließlich bundesrechtlich zu regeln; dies ergibt sich aus Art. 74 Abs. 1 Nr. 1 GG. Die Unterbringung gefährlicher Straftäter zum Zwecke der Gefahrenabwehr, §§ 63, 64, 66 StGB, sowie der maßgebliche Zeitpunkt für die Gefährlichkeitsprognose - der Zeitpunkt der der Haft zugrunde liegenden Verurteilung - sind im Strafgesetzbuch geregelt. Insoweit fehlt dem Freistaat Sachsen hier die Gesetzgebungskompetenz. An dieser Stelle könnte der Leser die Frage stellen: „Hat denn die Frage der Gesetzgebungskompetenz überhaupt etwas mit dem Datenschutz zu tun? Wieso nimmt sich der Datenschutzbeauftragte das Recht heraus, sich zu dieser Frage zu äußern?“

   Diese Fragen wurden - insbesondere von einzelnen Mitarbeitern der Staatsregierung, gelegentlich auch von einzelnen Abgeordneten - in der Vergangenheit dann aufgeworfen, wenn mein Votum unangenehm oder gar störend erschien. Datenschutz ist Verfassungsrecht; es geht dabei um den Schutz der Privatsphäre gegen obrigkeitliche Ausforschung. Das Allgemeininteresse, das Gemeinwohl, das und wie es in unseren Rechtsvorschriften zum Ausdruck kommt, muss mit dem und gegen das Grundrecht auf informationelle Selbstbestimmung abgewogen und - entsprechend der Rechtsordnung - in einen angemessenen Ausgleich gebracht werden.

Dies geht häufig aber nicht ohne einen Blick auf die Rechtsordnung als Gesamtsystem. Wer bei schwierigen Auslegungs- und Abwägungsfragen den juristischen Blick verengt und seinen „Scharfsinn“ auf die Einzelsituation und die Einzelvorschrift fokussiert, wird nicht selten zu einem ungerechten Ergebnis gelangen, weil er sich juristische Scheuklappen angelegt hat.

Verfassungsrecht meint immer das Recht des Gesamtkontextes der Verfassung; die Auslegung einer Rechtsvorschrift bedarf - wenn ihr Wortlaut, wie so oft, nicht ganz klar ist - des Blickes auf das Rechtsgebiet insgesamt und seine Regelungsgrundsätze; die richtige Anwendung des Grundsatzes der Verhältnismäßigkeit zwingt zum Blick über den Tellerrand.

Hinzu kommt: Wer die gerechte Lösung eines Problems sucht, muss die Wirklichkeit in den Blick nehmen: Nicht jede Lösung, die schnell und klar ist, ist die richtige, sondern diejenige, die alle - meist hochkomplexen - Einflüsse und Auswirkungen bedenkt.
Will man also eine Stellungnahme zu einem Gesetzgebungsvorhaben abgeben, so gehört dazu die Gesetzgebungskompetenz ebenso wie der Einfluss des Gesetzes auf den Alltag der Datenverarbeitung.

Ich bin in diesen Fragen mit meinen Amtskollegen einer Meinung.

2. Für unzulässig halte ich auch, dass dem Entwurf zufolge künftig Bedienstete der Vollzugsbehörden - Psychologen, Sozialarbeiter, kommunale Bedienstete der Jugendhilfe etc. - Erkenntnisse über den Strafgefangenen, die sie zum Zweck der Erreichung der Vollzugsziele (§ 2 StVollzG) gewonnen haben, nun zu einem allgemeinen polizeilichen Zweck erheben, speichern, verarbeiten und danach an das anordnende Gericht übermitteln dürfen sollen. Zwar erlaubt § 180 Abs. 2 StVollzG solche zweckändernden Übermittlungen auch zulasten des Gefangenen grundsätzlich, wenn es „zur Abwehr ... einer Gefahr für die öffentliche Sicherheit“ erforderlich ist. Zuvor Erheben, d. h. zweckgerichtet beschaffen, darf die Vollzugsbehörde nach § 179 StVollzG jedoch grundsätzlich nur Daten, „soweit deren Kenntnis für den hier nach dem Strafvollzugsgesetz aufgegebenen Vollzug der Freiheitsstrafe erforderlich ist“. Mit anderen Worten: Die Vollzugsbehörde darf sich keine anderen als die nach Strafvollzugsrecht zulässigen Informationen über den Gefangenen beschaffen. Andere Daten dürften ohne ausdrückliche gesetzliche Befugnis nicht erhoben, gespeichert, verarbeitet und demgemäß auch nicht übermittelt werden. Eine solche bereichsspezifische gesetzliche Datenerhebungsbefugnis zu allgemeinen polizeilichen Zwecken war im Entwurf jedoch nicht enthalten. So ließ der Entwurf ungeklärt,

- welche in der Vollzugsanstalt vorhandenen Informationen, die aus bundesrechtlicher

Sicht für den konkreten Vollzug zweckgebunden sind, nun für andere Zwecke erhoben, gespeichert und verarbeitet werden dürfen,
- wie sich der Betroffene gegen solche Einzelinformationen und die daraus möglichen Feststellungen, z. B. in Bezug auf ihren sachlichen Wahrheitsgehalt, rechtsstaatlich zur Wehr setzen kann,
- wie sich der Betroffene gegen Feststellungen der Vollzugsbehörde im Antrag auf weitere Unterbringung wehren können sollte,
- ob polizeirechtliche oder ob vollzugsrechtliche Grundsätze bei der Erhebung und weiteren Verarbeitung der - ausschließlich heiklen - Antragstatsachen gelten sollten.

3. Für bedenklich halte ich des Weiteren die vom Entwurf vorgesehene Bestimmung, wonach „das Gericht ... alle Umstände zu ermitteln (hat), die für die Entscheidung von Bedeutung sind. Vor der Unterbringung (hat) das Gericht zur Gefährlichkeit des Betroffenen die Gutachten von zwei Sachverständigen einzuholen.“ Dem Entwurf zufolge sollte einer dieser beiden Sachverständigen „ein sachverständiger Mitarbeiter der Justizvollzugsanstalt, in die der Betroffene eingewiesen ist“ sein dürfen. Mithin würde dieselbe Person, nämlich der in der Justizvollzugsanstalt beschäftigte Sozialarbeiter, sowohl auf die Stellung des Antrages auf weitere Unterbringung hinwirken, als auch eine sachverständige Äußerung vor Gericht abgeben dürfen. Dass sich hieraus schon während der Haftzeit ein enormer Zuwachs an „Macht“ des Sozialarbeiters über den Gefangenen ergeben wird, liegt auf der Hand. Außerdem wäre ein solcher Gutachter per se befangen, weil vorbefasst. Eine solche Regelung lehne ich deshalb kategorisch ab.

Ich habe die Hoffnung, dass der Sächsische Landtag meine Kritik berücksichtigt.

8.2 Datensammlungen von Richtern

Immer wieder erfahre ich etwas über die Angewohnheit einiger Richter, ihre Entscheidungsentwürfe oder Ausfertigungen derselben elektronisch im PC oder in Papierform zu speichern. Diese Datensammlungen sind der Abfassung künftiger vergleichbarer Verfahrensentscheidungen dienlich. Sie können sich aber auch als Datensammlung ohne Rechtsgrundlage erweisen und bis hin zu Persönlichkeitsbildern oder Verhaltensprofilen entwickeln. Es kommt also darauf an, datenschutzgerechte Verfahren für diese Datensammlungen zu finden, sofern diese nicht anonymisiert geführt werden.

Bei der rechtlichen Bewertung der Problematik ist Folgendes zu beachten: Gemäß § 25 DRiG ist der Richter zwar unabhängig, aber natürlich dem Gesetz unterworfen.

Die Vorschriften des Sächsischen Datenschutzgesetzes gelten daher auch für die Richterschaft, unabhängig davon, dass sie in ihrer rechtsprechenden Tätigkeit meiner Kontrolle entzogen sind. Wenn ich somit auch nicht die konkrete Datenverarbeitung der Richterschaft kontrollieren kann, so gehört es doch gemäß § 27 Abs. 4 SächsDSG zu meinen Befugnissen, jeder öffentlichen Stelle Empfehlungen zur Verbesserung des Datenschutzes zu geben und sie in Fragen des Datenschutzes zu beraten.

Deshalb habe ich mich an die Präsidenten der höchsten Gerichte im Freistaat Sachsen sowie an das Sächsische Staatsministerium der Justiz gewandt, damit eine datenschutzgerechte Gestaltung und Nutzung der richterlichen Datensammlungen erreicht wird.

Als wichtigen ersten Erfolg meiner Initiative kann ich verzeichnen, dass die Leitung des Oberlandesgerichts zusammen mit meiner Behörde eine „Gemeinsame Empfehlung ... zur datenschutzrechtlichen Behandlung von Sammlungen personenbezogener Daten im Bereich der ordentlichen Gerichtsbarkeit“ erarbeitet und in Kraft gesetzt hat.

Die Empfehlung wendet sich an Richter und richterliche Kollegien, Rechtsreferendare, Rechtspflegeranwärter, Justizsekretäranwärter und Gerichtsvollzieher.
Die Empfehlung schafft Kategorien gerichtlicher personenbezogener Datensammlungen und orientiert sich hierbei an dem Grad der möglichen Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung durch die Datennutzung:

- Datenschutzrechtlich wenig problematisch sind die aufgrund der Verwaltungsvorschrift über die Aktenordnung für die Geschäftsstellen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften (VwVAktO) obligatorisch zu führenden Geschäftsvorgänge. Der Umgang mit diesem Schriftgut ist behördenintern klar geregelt.

- Auch sind die von der Gerichtsverwaltung geführten systematischen Entscheidungssammlungen und der Zugriff auf diese datenschutzrechtlich unbedenklich, soweit in diesen Sammlungen ausschließlich anonymisierte Entscheidungen Eingang finden. In vielen Ländern der Welt und auch bei den Gerichten der europäischen Gemeinschaften ist es üblich, die Entscheidungen nach dem Namen des Klägers zu bezeichnen, zu ordnen und zugänglich zu machen. Dahinter steckt der richtige und sympatische Gedanke, dass jeder, der die Gerichte anruft, sich und sein Rechtsanliegen veröffentlicht. Die Öffentlichkeit ist ja nichts Böses, sondern soll ein breites Forum für eine offene und gerechte Streitkultur eröffnen. Da haben wir in Deutschland noch Nachholbedarf...

- Problematisch sind allerdings die Sammlungen personenbezogener Daten, die in Dienstzimmern aufbewahrt werden: Bei diesen von Richtern geführten

Entscheidungssammlungen wird empfohlen, Entscheidungen nach Möglichkeit nur in weitgehend anonymisierter Form, jedenfalls aber mit geschwärztem oder mittels moderner Telekommunikationstechnik anonymisiertem Rubrum zu sammeln. Über die Zugangsberechtigung zu derartigen Entscheidungssammlungen - auch gegenüber anderen Richtern - oder über die Weitergabe solcher Sammlungen im Rahmen von Dezernatsnachfolgen oder eines Wechsels in der Besetzung des richterlichen Kollegiums sollten der Empfehlung gemäß die eine Entscheidungssammlung führenden Richter in eigener Verantwortlichkeit unter Beachtung datenschutzrechtlicher Grundsätze (Zweckbindung, Geeignetheit, Erforderlichkeit) und gesetzlicher Regelungen befinden.

- Schließlich wird Richtern empfohlen, außerhalb des dienstlichen Bereichs in besonderer Weise auf die Wahrung datenschutzrechtlicher Belange zu achten. So sollten sie etwa Entscheidungssammlungen - aber auch Verfahrensakten etc. - nach Möglichkeit nur in dem zur Wahrnehmung der Rechtsprechungsaufgaben für notwendig erachteten Umfang außerhalb des dienstlichen Bereichs (z. B. nach Hause) verbringen und sich ihrer gesteigerten Verantwortlichkeit für außerhalb des dienstlichen Bereichs befindliche dienstliche Unterlagen - einschließlich „privatpersönlicher“ Entscheidungssammlungen - stets bewusst sein.

- Mit Ausscheiden aus dem Dienstverhältnis - einschließlich der Versetzung in ein nicht-richterliches Amt - wird Richtern empfohlen, lediglich noch anonymisierte Entscheidungssammlungen fortzuführen und sämtliche außerhalb des dienstlichen Bereichs vorhandene Speicherungen in Einrichtungen der elektronischen Datenverarbeitung in einer Weise zu löschen, die eine Rekonstruktion - auch mit besonderem technischen Aufwand - zuverlässig ausschließt.

Mit dieser gemeinsamen Empfehlung des OLG-Präsidenten und des Sächsischen Datenschutzbeauftragten ist eine datenschutzrechtlich vorbildliche Lösung gefunden worden. Sie beachtet - sorgsam austariert - das Spannungsverhältnis zwischen richterlicher Dienstaufsicht und richterlicher Unabhängigkeit. Ich habe deshalb die Hoffnung, dass die Empfehlung in ihren wesentlichen Zügen von den übrigen Gerichtsbarkeiten übernommen wird.

8.3 Zulassungsverfahren zur Rechtsanwaltschaft

Seit 1. Januar 2002 ist die Rechtsanwaltskammer Sachsen für die Entscheidung über die Zulassung zur Anwaltschaft, den Widerruf, den Wechsel der Zulassung und der sonstigen bislang dem OLG Dresden obliegenden Entscheidungen nach der Bundesrechtsanwaltsordnung (BRAO) zuständig. Zulassungsbehörde war bislang das OLG Dresden.

In Vorbereitung auf ihre neuen Aufgaben hat mich die Rechtsanwaltskammer Sachsen frühzeitig in die Gestaltung der Antragsformulare für die jeweiligen Verfahren eingebunden. In den sachorientiert geführten Beratungen, an denen auch das SMJus beteiligt war, konnte ich eine in allen Belangen datenschutzgerechte Gestaltung der Antragsunterlagen erreichen. Hauptgegenstand war hierbei die verfassungskonforme Begrenzung des Fragerahmens auf das Wesentliche, denn die BRAO enthält leider in ihren Vorschriften zur Rechtsanwaltszulassung zahlreiche generalklauselartige Formulierungen.

8.4 Ermittlungen des SMJus wegen der Entziehung eines verliehenen Ordens

Die Staatskanzlei nahm eilfertig Presseberichte über die (strafrechtliche) Verurteilung einer Person, der der Bundespräsident einen Orden verliehen hatte, zum Anlass das SMJus zu ersuchen, die Voraussetzungen für die Entziehung des Ordens zu prüfen. Daraufhin bat das SMJus die Generalstaatsanwaltschaft um Übersendung einer Urteilsausfertigung. Diesen Auftrag erfüllte die Generalstaatsanwaltschaft weisungsgemäß, so dass endlich die Staatskanzlei vom SMJus eine Urteilsausfertigung erhielt.

Diese Beschaffung personenbezogener Daten war rechtswidrig, weil sie nicht auf eine gesetzliche Grundlage gestützt werden konnte:

Zwar regelt § 4 Abs. 1 Ordensgesetz die Entziehung eines Ordens wegen Ordensunwürdigkeit aufgrund des „Begehens einer entehrenden Straftat“. Insoweit befugt ist einzig und allein der Verleihungsberechtigte, nämlich der Bundespräsident. Weder das SMJus noch die Sächsische Staatskanzlei waren somit zur Prüfung der Voraussetzungen einer Entziehung des Ordens zuständig.

Für die datenschutzrechtliche Bewertung des Falles waren ferner folgende Erwägungen von Bedeutung: § 4 Abs. 2 i. V. m. Abs. 3 OrdenG regelt abschließend und speziell die Datennutzung und -übermittlung durch „Strafverfolgungs- oder Strafvollstreckungsbehörden“ an den Verleihungsberechtigten. Voraussetzung ist, dass ein Gericht „(...) auf eine Freiheitsstrafe (...)“ oder „die Aberkennung der Fähigkeit, öffentliche Ämter zu bekleiden“ erkannt hat. Beides war hier ersichtlich nicht der Fall. Denn die Presse hatte nicht über eine Freiheitsstrafe, sondern über eine Geldstrafe berichtet. Dafür, dass das Gericht der verurteilten Person die Fähigkeit, öffentliche Ämter zu bekleiden, aberkannt hatte, fehlte jeder Anhaltspunkt. Schließlich ist das SMJus weder Strafverfolgungs- noch Strafvollstreckungsbehörde im Sinne des Ordensgesetzes, erst recht nicht die Staatskanzlei.

Das SMJus hat seine zunächst vertretene Auffassung, dass es im Verleihungsverfahren nicht nur zur Vorschlagsberechtigung, sondern auch zur Anregung gegenüber dem Bundespräsidenten, den Orden wieder zu entziehen, berechtigt sei, aufgegeben. „Für die Zukunft“ werde es sich meiner Auffassung anschließen. Aus diesem Grunde konnte ich von einer förmlichen Beanstandung absehen.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

Wechselseitiger Kfz-Zulassungsservice durch zwei benachbarte Zulassungsstellen an Sonnabenden

Bürgerfreundliches Verhalten beweist sich nicht zuletzt an den behördlichen Öffnungszeiten. Längere Öffnungszeiten bewirken einen gewissen Aufwand, besonders in personeller Hinsicht. Eine kreisfreie Stadt und ein Landkreis beabsichtigten daher, ihre beiden Kfz-Zulassungsstellen an Sonnabenden wechselseitig zu öffnen und Kunden aus dem jeweils anderen Zuständigkeitsbereich mitzubetreuen. Konkret sollten die Bewohner des Landkreises an dem einen Sonnabend die Zulassungsstelle der Stadt benutzen können und umgekehrt am darauf folgenden Sonnabend die Bürger der Stadt die Zulassungsstelle des Kreises.

§ 68 Abs. 2 Satz 2 StVZO lautet: „Anträge können mit Zustimmung der örtlich zuständigen Behörde von einer gleichgeordneten auswärtigen Behörde behandelt und erledigt werden.“

Da sowohl das SMWA als auch das SMI in dieser Vorschrift zu Recht eine gesetzliche Grundlage für ein derartiges Verfahren gesehen haben, bestehen hinsichtlich der örtlichen Zuständigkeit keinerlei Bedenken. Ich habe beide Seiten jedoch darauf hingewiesen, dass der Datenschutz nach § 9 SächsDSG uneingeschränkt zu gewährleisten ist. Ich habe mir vorbehalten, zu gegebener Zeit eine datenschutzrechtliche Kontrolle dieses Projektes durchzuführen.

In diesem Zusammenhang habe ich beide Kommunen auf das „Aachener Modell“ hingewiesen, wo sich eine kreisfreie Stadt und ein Landkreis auf eine einzige (gemeinsame) Kfz-Zulassungsstelle verständigt haben. So weit wollte man in diesem Fall aber nicht gehen.

9.2 Gewerberecht

Nochmals: Aufbewahrungsfristen von Gewerbeanzeigen nach § 14 GewO

Die in 9/9.2 behandelte Frage, ob die in Sachsen geltende 20-jährige Aufbewahrungsfrist für Gewerbeanzeigen (gerechnet ab dem Zeitpunkt der Gewerbe*ab*meldung) mit § 14 GewO vereinbar ist, ist inzwischen auf einer Tagung des Bund-Länder-Ausschusses „Gewerberecht“ behandelt worden. Dort wurde meiner Interpretation der Vorschrift widersprochen. Diese Interpretation entspräche nicht dem Konzept der Gewerbeordnung im Hinblick auf die Beurteilung der Zuverlässigkeit. Das SMWA hat mir mitgeteilt, es habe Einigkeit darüber bestanden, dass eine sofortige Vernichtung der Daten nach Abmeldung nicht zwingend sein könne, und zur Begründung Folgendes ausgeführt:

„Insbesondere durch die Vorschrift des § 146 Abs. 2 Nr. 1 GewO, wonach ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 14 Abs. 1 bis 3 GewO eine Anzeige nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet, wird dieses Ergebnis bestätigt. Denn würde man nach der Anzeige der Gewerbeaufgabe sofort die in Rede stehenden Daten vernichten, so wäre es der Behörde praktisch unmöglich nachzuprüfen, ob die angezeigte Gewerbeaufgabe tatsächlich erfolgt ist oder ob das Gewerbe ohne Anzeige weitergeführt wird. Weiterhin handelt gemäß § 1 Abs. 1 Nr. 2 des Gesetzes zur Bekämpfung der Schwarzarbeit ordnungswidrig, wer Dienst- oder Werkleistungen in erheblichem Umfang erbringt, obwohl er der Verpflichtung zur Anzeige vom Beginn des selbständigen Betriebes eines stehenden Gewerbes (§ 14 GewO) nicht nachgekommen ist. Mithin würde bei sofortiger Vernichtung der Gewerbedaten die ohnehin schwierige Beweisführung den Behörden nahezu unmöglich gemacht, so dass diese Form der Schwarzarbeit praktisch nicht mehr zu ahnden wäre. Angesichts des vorgesehenen Bußgeldrahmens von bis zu zweihundertausend Deutsche Mark erscheint dieses Resultat in der Tat nicht vertretbar.“

Das überzeugt mich. Deshalb habe ich einer 5-jährigen Aufbewahrungsfrist zugestimmt. Das SMWA hat mit einem Rundschreiben an die drei Regierungspräsidenten diesen Fünfjahreszeitraum ab Gewerbeabmeldung als verbindlich festgelegt.

9.3 Industrie- und Handelskammern; Handwerkskammern

In diesem Jahr nicht belegt.

9.4 Offene Vermögensfragen

9.4.1 Probleme im Zusammenhang mit der Konzentration auf die ÄRoV Chemnitz, Dresden und Leipzig

Durch das SächsAGVermG (§ 1 Abs. 1 und 2) sind mit Wirkung zum 1. Januar 2001 die Aufgaben der ÄRoV jeweils für das gesamte Gebiet der drei Regierungsbezirke auf ein Amt, und zwar auf die Kreisfreien Städte Chemnitz, Dresden und Leipzig, übertragen worden. Deshalb waren gemäß § 1 Abs. 4 SächsAGVermG die noch anhängigen Verfahren nunmehr von diesen Ämtern zu bearbeiten.

Diese Neuregelung hat, was die Speicherung und Übermittlung personenbezogener Daten betrifft, einige Fragen aufgeworfen. Vor allem: Was wird mit den Akten der bereits abgeschlossenen Verfahren? Wer erteilt auf welcher Grundlage Auskünfte zu angemeldeten oder beschiedenen Anträgen bzw. zu von diesen betroffenen oder auch gerade nicht betroffenen (Negativattest) Vermögensgegenständen?
Ich habe zu diesen Fragen gegenüber dem LARoV wie folgt Stellung genommen:

(1) Verbleib der zu den nicht unter § 1 Abs. 4 SächsAGVermG fallenden Verfahren gehörenden Akten:

(1.1) Die seit dem 1. Januar 2001 gemäß § 1 Abs. 2 SächsAGVermG nicht mehr für die Ausführung des Vermögensgesetzes zuständigen Landkreise und Kreisfreien Städte haben keine Restzuständigkeit mehr zur Ausführung von unter § 1 Abs. 1 SächsAGVermG fallenden Rechtsvorschriften. Sie dürfen demnach insbesondere auch keine Auskünfte aus den in Ausführung dieser Gesetze entstandenen (oder dazu aus DDR-Beständen übernommenen) Unterlagen erteilen und dürfen diese Daten auch nicht etwa deswegen speichern, weil eine solche Speicherung für die Ausführung der betreffenden Rechtsvorschriften erforderlich ist. Die gesamte Funktion ist auf die gemäß § 1 Abs. 2 SächsAGVermG nunmehr zuständigen Ämter übergegangen.

Das Gegenteil lässt sich meiner Meinung nach aus § 1 Abs. 4 SächsAGVermG nicht entnehmen.
Weder der Wortlaut noch die Stellung der Vorschrift bieten Anhaltspunkte dafür, dass Abs. 4 die in Abs. 2 i. V. m. Abs. 1 ausgesprochene Übertragung des Gesetzesvollzuges einschränkt auf die anhängigen Verfahren. Als Klarstellung der Wirkung der Zuständigkeitsübertragung auf die einzelnen Verwaltungsverfahren, einschließlich der Fortsetzung in gerichtlichen Verfahren, ist die Vorschrift durchaus sinnvoll.
Auch die praktischen Folgen sprechen für meine Auslegung: Beschränkte § 1 Abs. 4 SächsAGVermG Abs. 2 auf die noch anhängigen Verwaltungsverfahren (unter Ausschluss der bloßen Auskunfts-Verfahren), hätte das zur Folge, dass die bei den

Rechtsträgern der Alt-ÄRoV verbleibenden Aufgaben des Gesetzesvollzuges durch besondere Behörden, sozusagen Rest-Auskunfts-ÄRoV, wahrzunehmen wären, die sachlich für alle von § 1 Abs. 4 SächsAGVermG nicht erfassten Verfahren zuständig wären. Mithin gäbe es nach dem 1. Januar 2001 weiterhin die alten ÄRoV als Behörden mit einer Zuständigkeit, die gegenüber der früheren ausschließlich durch § 1 Abs. 4 SächsAGVermG eingeschränkt wäre. Kurz: Es gäbe eine gespaltene sachliche Zuständigkeit und es gäbe zweierlei Arten von ÄRoV. Eine solche Zuständigkeitsverteilung wäre so außergewöhnlich, dass sie einer sehr klaren, Zweifel ausschließenden Regelung im Gesetz bedürfte - an der es aber eben fehlt.

Demnach müssten eigentlich alle zu den Beständen der seit dem 1. Januar 2001 nicht mehr zuständigen und de jure nicht mehr bestehenden ÄRoV (nachfolgend kurz „Alt-ÄRoV“) gehörenden Akten von den drei gemäß § 1 Abs. 2 SächsAGVermG nunmehr zuständigen ÄRoV (nachfolgend: übernehmende ÄRoV) übernommen werden.

Auch die Zuständigkeit für die Anbietung gegenüber dem zuständigen Archiv und für die Übernahme durch dieses gemäß § 13 Abs. 3 Satz 1 SächsArchivG i. V. m. § 5 Abs. 5 bis 8 SächsArchivG ist hinsichtlich dieser Akten mit dem 1. Januar 2001 auf die drei übernehmenden ÄRoV bzw. die von deren Rechtsträgern unterhaltenen Archive übergegangen.

(1.2) Verschiedene Gründe sprechen dafür, dass sämtliche Akten zu Verwaltungsverfahren der ÄRoV bis auf Weiteres noch aufbewahrt werden müssen:

Das BARoV verlangt - darauf hatte mich das LARoV hingewiesen - eine längerfristige Aufbewahrung aller Entschädigungsbescheide; die KfW macht wegen Grundpfandrechten, die staatliche Darlehensforderungen gesichert haben, Auskunftsrechte im Hinblick auf abgeschlossene Verwaltungsverfahren noch langfristig geltend; die Lastenausgleichsämter werden noch länger wegen Rückforderung von Lastenausgleichsleistungen nachfragen; es gibt noch Petitionsverfahren zu bereits bestandskräftig abgeschlossenen Verwaltungsverfahren. Auch ist noch nicht abzusehen, wie sich die Rechtsprechung des Bundesverwaltungsgerichts zu Wiederaufgreifensgründen entwickeln wird, etwa im Falle des Wegfalles von Restitutions-Ausschlussgründen, zumindest im Falle des § 5 Abs. 1 b VermG. Schließlich gibt es wohl noch Auskunftsrechte von TLG und BVVG bzw. OFDen zu abgeschlossenen Verwaltungsverfahren.

(1.3) Wie man hören kann, sind die Beteiligten bei der Regelung des Kostenausgleiches gemäß § 2 SächsAGVermG davon ausgegangen, dass für die drei übernehmenden ÄRoV Kostenbelastungen durch die Aufbewahrung der zu den abgeschlossenen Verfahren gehörenden Akten nicht entstehen. (Angeblich soll ein Landkreis, der Träger eines Alt-ARoV gewesen ist, die Verfassungswidrigkeit der Kostenregelung

des Gesetzes in einem beim SächsVerfGH anhängigen Rechtsstreit geltend gemacht haben.)

(1.4) In Anbetracht der besonderen Schwierigkeiten, welche die Regelung der offenen Vermögensfragen im Zusammenhang mit der Wiedervereinigung Deutschlands mit sich gebracht haben und, wie sich vorliegend zeigt, weiterhin mit sich bringen, halte ich es für vertretbar, dass die bei den Rechtsträgern der Alt-ÄRoV noch vorhandenen Unterlagen, die dort sozusagen vom „ARoV in Liquidation“ verwahrt und verwaltet werden, bei diesen Rechtsträgern verbleiben. Da diese aber nicht mehr über ÄRoV verfügen, sind die Unterlagen gemäß § 5 Abs. 6 SächsArchivG i. V. m. § 13 Abs. 3 Satz 1 SächsArchivG von den Kommunalarchiven zu übernehmen, obwohl sie ausnahmslos noch aufzubewahren sind.

Ich vermute, dass dies auch archivfachlich die vorzugswürdige Regelung ist. Es wird erwogen, dass auch die Akten der von den drei übernehmenden ÄRoV noch fortzuführenden Verfahren nach Verfahrensabschluss an den jeweiligen Rechtsträger des Alt-ARoV zurückgegeben werden sollen, in dessen Zuständigkeit das Verfahren vorher begonnen hat. Auf diese Weise würde der Zusammenhang zwischen Belegenheit des Vermögensgegenstandes und räumlicher Zuständigkeit des Archives gewahrt. Dafür wird es vermutlich einer gesonderten rechtlichen Grundlage bedürfen, die in einer Ergänzung des SächsAGVermG bestehen könnte.

Praktische Folge einer solchen Archivierung wäre, dass Bedienstete, die aufgrund früherer Beschäftigung im Alt-ARoV heutzutage für die Nutzung der Unterlagen noch zuständig sind, Bedienstete im Kommunalarchiv sein müssten.

Was die im Archivrecht üblicherweise wohl nicht vorgesehene Herausgabe von Originalunterlagen an befugte Stellen betrifft, könnte ich mir vorstellen, dass im Falle der gerade auf § 5 Abs. 6 SächsArchivG gestützten Archivierung - und auch vermutlich überhaupt in denjenigen Fällen, in denen es um den Beweiswert der Unterlagen in Rechtsstreitigkeiten geht, vgl. § 2 Abs. 3, 2. Fall SächsArchivG - dies ausnahmsweise auch anders gehandhabt werden kann. Und zwar auch dann, wenn sich das Archiv durch ein Auskunftsverlangen inhaltlich überfordert sieht: Dann müsste die Akte zur Auskunftserteilung dem übernehmenden ARoV überlassen werden können.

(2) Weitergabe von Stammdaten aus dem Bestand der Alt-ÄRoV an das jeweils übernehmende ARoV:

Wie dargelegt, ist die gesamte Erfüllung der Aufgaben der Alt-ÄRoV gemäß § 1 Abs. 2 SächsAGVermG mit Beginn des Jahres 2001 auf das jeweilige übernehmende ARoV übergegangen.

Weil das ARoV zur Aufgabenerfüllung (und zusätzlich auch für Anfragen der GVO-Behörde) unverändert eine Übersicht über Verfahrensstände zu den verschiedenen Vermögenswerten, insbesondere Grundstücken, benötigt, entspricht die Weitergabe der Stammdaten-Dateien (verwaltet mit den Programmen EVA bzw. OVIT) an die übernehmenden ÄRoV dem Aufgabenübergang. Es handelt sich insoweit nicht um eine Übermittlung im Rechtssinne, sondern um eine Datenweitergabe gemäß Funktionsübergang.

Insoweit bestehen gegen die Verwendung des bei den ÄRoV verbreiteten EDV-Programmes „OV-Archiv“ keine Einwände.

Die fortgesetzte Speicherung und Nutzung der Stammdaten mit dem Stand, der sich bei Übergang der Zuständigkeit auf das jeweils übernehmende ARoV ergeben hat, ist im Rahmen der - von den Archiven der Rechtsträger der Alt-ÄRoV wie dargelegt zu übernehmenden - Aufgabenerfüllung ebenfalls zulässig.
Dabei ist es sicherlich auch datenschutzrechtlich unbedenklich und vermutlich sinnvoll, wenn mit Hilfe neuerer Software sichergestellt wird, dass diese Stammdaten auch in Zukunft auf neueren Rechnern genutzt werden können.

(3) Übermittlung neuerer (geänderter) Stammdaten durch das übernehmende ARoV an den Rechtsträger des Alt-ARoV?

Die vom Programm „OV-Archiv“ unterstützte Übermittlung neuerer, also gegenüber dem Datenstand zum 1. Januar 2001 geänderter Stammdaten an den Rechtsträger des Alt-ARoV - also das Archiv der betreffenden kommunalen Gebietskörperschaft - wäre unzulässig. Eine Rechtsgrundlage für eine solche Datenübermittlung ist nicht erkennbar. Insbesondere bedürfen die Archive für Auskünfte aus den Unterlagen der Alt-ÄRoV solcher geänderten Daten nicht.

Die Rechtsträger der Alt-ÄRoV sind unverändert GVO-Behörde für ihr Gebiet. Daher müssen sie als GVO-Behörde - unverändert - GVO-Genehmigungsbescheide auf der Grundlage von Daten erlassen, die ausschließlich durch den Verlauf von bei den ÄRoV anhängigen oder nach einer solchen Anhängigkeit bestandskräftig entschiedenen Verfahren stammen (vgl. § 1 Abs. 2 GVO). Diese Daten hat sich die GVO-Behörde - unverändert getragen von den Landkreisen und kreisfreien Städten (§ 8 GVO) - vom jeweils zuständigen ARoV übermitteln zu lassen. Die möglicherweise vielfach anzutreffende fehlende organisatorische Trennung zwischen ARoV und GVO-Behörde darf über diesen Sachverhalt nicht hinwegtäuschen.

Daraus folgt: Die Landkreise und Kreisfreien Städte, die nicht mehr Träger eines ARoV sind, haben die für die Erteilung der Genehmigung gemäß § 4 GVO benötigten Daten aus dem Vollzug des Vermögensgesetzes beim nunmehr zuständigen -

übernehmenden - ARoV anzufordern. Dieses muss, sofern es nicht alle Altunterlagen bekommen hat, beim Archiv eben derjenigen kommunalen Gebietskörperschaft anfragen, die als Träger eines Alt-ARoVs in ihrer Archivbehörde die Unterlagen behalten hat.

Für eine Verkürzung dieses Datenweges - beispielsweise aus dem Kreisarchiv eines Landkreises an das ARoV der Stadt Chemnitz und wieder zurück an das Landratsamt in dessen Eigenschaft als GVO-Behörde - könnte man möglicherweise den datenschutzrechtlichen Gesichtspunkt der Datensparsamkeit geltend machen. Unter dem Gesichtspunkt der Geeignetheit der Datenverarbeitung sollte jedoch maßgeblich sein, dass die GVO-Behörde nicht lediglich einer Auskunft über einen abgeschlossenen Vorgang bedarf, sondern einer Angabe über die vermögensrechtliche Lage, wie sie sich aufgrund der gesamten Tätigkeit der zuständigen Vermögensämter (ARoV oder LARoV) darstellt. Daher benötigt die GVO-Behörde eine Auskunft des örtlich zuständigen ARoV, kann sie sich nicht mit der Auskunft des Alt-ARoV zufriedengeben.

Der Vollständigkeit halber sei in diesem Zusammenhang angemerkt, dass selbstverständlich auch nicht die GVO-Behörde die Funktion eines ARoV i. L. übernehmen und in eigener Zuständigkeit Akten des nicht mehr existierenden ARoV aufbewahren darf.

Das LARoV hat keine Einwände gegen meine Rechtsauffassung geltend gemacht.

9.4.2 Auskunftsersuchen gegenüber den ÄRoV und LÄRoV zur Ermittlung von Verstößen gegen das Rechtsberatungsgesetz

Ein sog. gewerblicher Erbenermittler war wegen unerlaubter Rechtsberatung von einem Rechtsanwalt auf Unterlassung verklagt worden und hatte sich in einem gerichtlichen Vergleich gegenüber dem Anwalt dazu verpflichtet, nicht in Rückübertragungsverfahren nach dem Vermögensgesetz als Bevollmächtigter von Antragstellern gegenüber den zuständigen Behörden (ÄRoV, LÄRoV) aufzutreten. Der Rechtsanwalt wollte nun von den ÄRoV sowie LÄRoV wissen, ob der Erbenermittler dort - seiner Verpflichtung zuwiderhandelnd - tätig geworden sei. Hierzu hat der Anwalt den Ämtern eine Kopie des Vergleiches sowie einen von ihm selbst entwickelten Vordruck übersandt. Die Behörde sollte angeben, ob ihr solche rechtsberatenden Tätigkeiten des Erbenermittlers bekannt sind, gegebenenfalls sollte das Aktenzeichen des Verfahrens angegeben werden. In einem Freitextfeld sollten sonstige Bemerkungen eingetragen werden.
Einige Ämter hatten Bedenken, ob die Auskunft an den Rechtsanwalt zulässig sei.

Da jedenfalls die Angabe des Aktenzeichens ein personenbezogenes Datum ist, benötigte die Behörde für die Weitergabe dieses Datums eine Rechtsgrundlage. Diese Rechtsgrundlage bietet für sächsische Behörden § 15 Abs. 1 Nr. 2 SächsDSG.

Der Rechtsanwalt hatte ein berechtigtes Interesse an der Kenntnis der zu übermittelten Daten glaubhaft dargelegt. Der Erbenermittler hatte sich gegenüber dem Rechtsanwalt verpflichtet, bestimmte rechtsberatende Tätigkeiten nicht auszuüben. Um prüfen zu können, ob der Erbenermittler sich an seine Verpflichtungen hält, benötigte der Rechtsanwalt die erfragten Angaben, insbesondere auch das Aktenzeichen. Für nicht erforderlich habe ich allerdings das Freitextfeld „Sonstiges“ erachtet, da insbesondere nicht klar war, was die Behörde hier angeben sollte.
Der Betroffene, das ist derjenige, über den das Datum eine Information enthält, darf kein schutzwürdiges Interesse am Unterbleiben der Übermittlung haben. Durch die Angabe des Aktenzeichens kann mit Zusatzwissen ein Bezug zu verschiedenen Personen hergestellt werden, nämlich zu allen Beteiligten des Verfahrens sowie unter Umständen zu weiteren Personen. Ein schutzwürdiges Interesse dieser Personen am Unterbleiben der Übermittlung des Aktenzeichens an den Rechtsanwalt war nicht ersichtlich. Der Rechtsanwalt benötigte das Aktenzeichen zu Beweiszwecken bei der Geltendmachung von Unterlassungsansprüchen. Durch die Verwendung des Aktenzeichens zu solchen Zwecken konnten schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Das Risiko der Mandanten, durch Maßnahmen, die auf dem Rechtsberatungsgesetz beruhen, den bisherigen Bevollmächtigten zu verlieren und Geld für einen neuen Bevollmächtigten ausgeben zu müssen, wird mit dem Rechtsberatungsgesetz als für die Erreichung des Gesetzeszweckes erforderlich in Kauf genommen; dies Risiko begründet daher keine Schutzwürdigkeit im Sinne des § 15 Abs. 1 Nr. 2 SächsDSG.
§ 15 Abs. 3 SächsDSG sieht die Anhörung der Betroffenen vor der Übermittlung vor. Von diesem Anhörungserfordernis wird abgesehen, wenn dem schwerwiegende öffentliche oder private Belange entgegenstehen. Eine Anhörung sämtlicher Betroffener hätte die Durchsetzung der Unterlassungsansprüche erheblich verzögert. Zum Schutz der von einer mutmaßlichen unerlaubten Rechtsberatung durch den Erbenermittler betroffenen Verfahrensbeteiligten sowie zum Schutz des Rechtsanwalts vor rechtswidrigen Wettbewerbsbeeinträchtigungen war eine schnelle Durchsetzung der Unterlassungsansprüche erforderlich, die eine Anhörung der Betroffenen zur Übermittlung des Aktenzeichens entbehrlich machte. Hinzu kam, dass die Anhörung notwendig mit einer Übermittlung von Daten über den Prozessgegner des Rechtsanwaltes, also den gewerblichen Erbenermittler, verbunden gewesen wäre, die für diesen vermutlich zusätzlich von Nachteil gewesen wäre.

Im Ergebnis habe ich also die Datenübermittlung zu Fällen, in denen nach Einschätzung der Behörde ein Verstoß gegen den Vergleich vorlag, für zulässig erachtet.

9.5 Sonstiges

In diesem Jahr nicht belegt.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1 Aufbewahrungsfristen von Patientendaten

Ein Krankenhaus fragte nach den für Patientendaten vorgeschriebenen Aufbewahrungsfristen. Unter Bezugnahme auf meine Antwort in 9/10.1.1 und 9/10.1.8 habe ich ihm mitgeteilt, dass das Sächsische Krankenhausgesetz keine Aufbewahrungsfristen vorsieht, sich in anderen Rechtsvorschriften jedoch folgende Angaben finden:

- für ärztliche Aufzeichnungen, Behandlungsdaten gemäß § 10 Abs. 3 der Berufsordnung der Sächsischen Landesärztekammer (Ausnahmen für längere Aufbewahrungsfristen sind möglich, z. B. bei Latenzzeiten gewisser Krankheiten)	10 Jahre
- Aufzeichnungen über Untersuchungen mit radioaktiven oder ionisierenden Stoffen (§ 43 Abs. 3 StrlSchV)	10 Jahre
- Aufzeichnungen über die Behandlung mit den o. g. Stoffen (§ 43 Abs. 3 StrlSchV)	30 Jahre
- Aufzeichnungen zu Röntgenbehandlungen (§ 28 Abs. 4 Satz 1 Nr. 1 RöV)	30 Jahre
- Aufzeichnungen zur Röntgendiagnostik (§ 28 Abs. 4 Satz 1 Nr. 2 RöV)	10 Jahre
- Aufzeichnungen über die Behandlung Geschlechtskranker (§ 10 Abs. 1 Satz 2 GeschlKrG i. V. m. § 2 Abs. 3 zweite DVO zum GeschlKrG)	5 Jahre
- Aufzeichnungen über die Anwendung von Blutprodukten und von gentechnisch hergestellten Plasmaproteinen zur Behandlung von Hämastasestörungen (§ 14 Abs. 3 TFG)	15 Jahre

Bei unterschiedlichen Fristen gilt stets die längste Aufbewahrungsfrist.

Da vertragliche Schadensersatzansprüche des Patienten (§§ 199 Abs. 2 und 852 BGB n.F.) erst nach 30 Jahren verjähren, empfehle ich für Patientenakten (Krankenblätter, Dokumentation der Behandlung) eine 30-jährige Aufbewahrungsfrist.

Hinsichtlich der Aufbewahrung von Verwaltungsakten vertrete ich folgende Auffassung:
Gemäß § 33 Abs. 6 SächsKHG gehört es zu den datenschutzrechtlichen Pflichten des Krankenhauses, personenbezogene Daten, die für die weitere Aufgabenerfüllung nicht mehr erforderlich sind, zu vernichten (zur archivrechtlichen Anbietungspflicht vor der Vernichtung siehe 9/10.1.1 Nr. 3). Die Verwaltungsakten enthalten die Patientendaten, die zur verwaltungsmäßigen Abwicklung des Behandlungsverhältnisses, insbesondere zur Leistungsabrechnung, erforderlich sind. Diese Aufgabe ist spätestens dann erfüllt, wenn der Patient entlassen ist und der Sozialleistungsträger die Kosten erstattet hat. Nach einem Urteil des Bundessozialgerichts vom 17. Juni 1999 (Das Krankenhaus 2000, S. 39) verjähren Zahlungsansprüche eines Krankenhauses innerhalb von vier Jahren. Dieser Zeitraum kann als Grundlage für eine Aufbewahrungsfrist von Verwaltungsakten dienen. Spätestens 6 Jahre nach Ablauf des Kalenderjahrs, in dem die letzten abrechnungsfähigen Leistungen erbracht worden sind, sind sie meiner Auffassung nach zu vernichten. Diese Frist ist ausreichend bemessen, um eventuelle Rückfragen klären zu können.

10.1.2 Krankenhausseelsorge / Anstaltsseelsorge und Datenschutz

Nach Art. 140 des Grundgesetzes und Art. 109 Abs. 4 der Sächsischen Verfassung sind die Bestimmungen der Art. 136, 137, 138, 139 und 141 der Deutschen Verfassung vom 11. August 1919 (das ist die Weimarer Reichsverfassung) Bestandteil des Grundgesetzes und der Sächsischen Verfassung. Art. 141 Weimarer Reichsverfassung lautet: „Soweit das Bedürfnis nach Gottesdienst und Seelsorge im Heer, in Krankenhäusern, Strafanstalten oder sonstigen öffentlichen Anstalten besteht, sind die Religionsgesellschaften zur Vornahme religiöser Handlungen zuzulassen, wobei jeder Zwang fernzuhalten ist.“

Diese Vorschrift ist im Kontext zu lesen mit Art. 4 Abs. 2 des Grundgesetzes und Art. 19 Abs. 2 der Sächsischen Verfassung: „Die ungestörte Religionsausübung wird gewährleistet.“

Aus den vorgenannten Vorschriften ergibt sich eine Verpflichtung des Staates zur Grundrechts-Ermöglichung auch unter den Bedingungen von Krankenhaus- und Anstaltsverhältnissen. Weil Anstaltsinsassen und Patienten tatsächlich gehindert sind, ihre Religion dort, wo sie sich befinden, auszuüben, muss der Staat positive

Vorkehrungen treffen, um ihnen die Ausübung des Grundrechts zu ermöglichen. Dies ist in dem Begriff „gewährleistet“ zum Ausdruck gebracht.

Campenhausen schreibt in seinem Staatskirchenrecht, 3. Auflage München 1996 auf Seite 227 zur „Bedürfnisklausel“: „Es ist vom Vorliegen des Bedürfnisses auszugehen, solange sich Angehörige einer Religionsgemeinschaft in der Anstalt befinden und nicht aufgrund ihrer Bekenntnisfreiheit eine religiöse Betreuung abgelehnt haben. Ein Bedürfnis nach religiösen Handlungen liegt daher nicht erst dann vor, wenn ein Einzelner in der jeweiligen Anstalt ein solches äußert. Das Bedürfnis ist vielmehr in erster Linie durch die Anstaltsleitung festzustellen. Die Prüfung durch die Anstaltsleitung ist nur auf die Feststellung der objektiven Umstände beschränkt, bietet daher keinerlei Raum für etwaige Ermessensentscheidungen.“

Das gilt natürlich ebenso für Krankenhäuser. Sie haben den Bedarf durch Befragung ihrer Patienten festzustellen. Dabei wäre es weder geeignet noch erforderlich, Einzelfragen zur religiösen Überzeugung oder einem speziellen Wunsch nach seelsorgerischer Betreuung zu stellen. Diese Daten sind höchst-persönlicher, ja intimer Art und stehen zudem unter dem besonderen Schutz nach Art. 8 der Europäischen Datenschutzrichtlinie. Hinzu kommt, dass der Zeitpunkt der Krankenhausaufnahme der denkbar ungünstigste ist; die Patienten haben dann andere Sorgen. Der konkrete Wunsch nach Seelsorge wird meist auch erst später entstehen. Die Mitgliedschaft in einer öffentlich-rechtlich anerkannten Kirche ist hingegen ein relativ oberflächliches Datum. Seine Erhebung ist zur Ermittlung des - abstrakten - Bedürfnisses i. S. des Art. 141 Weimaer Reichsverfassung datenschutzrechtlich unproblematisch.

Das Bundesverfassungsgericht (BVerfGE 46, 266 ff.) und das Bundesverwaltungsgericht (DÖV 76, 273 f.) sagen deutlich, dass die Befragung von Patienten städtischer Krankenhäuser nach ihrer Religionszugehörigkeit der Erleichterung des Rechts der Religionsgesellschaften auf seelsorgerische Betreuung in Krankenhäusern dient und mit der Verfassung vereinbar ist und nicht gegen das Grundrecht auf sog. negative Bekenntnisfreiheit der Befragten verstößt, wenn die Beantwortung freigestellt ist.

§ 13 des Evangelischen Kirchenvertrages Sachsen vom 24. März 1994 sowie Art. 12 des Vertrages zwischen dem Heiligen Stuhl und dem Freistaat Sachsen vom 2. Juli 1996 sehen - wortgleich - vor, dass die Seelsorge in staatlichen Krankenhäusern und entsprechenden Einrichtungen des Freistaates Sachsen „gewährleistet“ wird. Diese verbindliche (gesetzliche!) Norm des „Gewährleistens“ schließt es ein, dass staatlicherseits alle notwendigen Voraussetzungen dafür geschaffen werden, dass eine praktisch sinnvolle Durchführung der Krankenhausseelsorge ermöglicht wird, deren konkrete Organisation ureigene Aufgabe der Kirchen ist.

Jeder, der Mitglied einer öffentlich-rechtlichen Kirche und gleichzeitig Patient im Krankenhaus ist, muss dem jeweils zuständigen Krankenhausseelsorger bekannt werden. Gleiches gilt für Anstalten, Justizvollzugsanstalten etc. Es ist Aufgabe deren Leitung, dies sicherzustellen. Namen, Geburtsjahr, Anschriften, Einlieferungstag und Zimmer-Nummer sind also von der Verwaltung unverzüglich dem jeweils in Betracht kommenden Seelsorger mitzuteilen.

Die entsprechende Datenerhebungsbefugnis und Datenübermittlungsbefugnis ergibt sich direkt aus den o. g. staatskirchenrechtlichen Vorschriften.

Die Seelsorge in privaten oder auch kirchlichen Anstalten dürfte - wegen der Drittwirkung der Verfassungslage - zu den Nebenpflichten des Behandlungsvertrages gehören. Es ist die Nebenpflicht des Krankenhauses, die Religionsausübung dadurch sicherzustellen, dass der Patient nach seiner Konfession befragt und dies dann der jeweils zuständigen Krankenhausseelsorge übermittelt wird.

Im Interesse einer möglichst gleichmäßigen Behandlung der Patienten in dieser Angelegenheit bitte ich die Staatsregierung, informell auf die anderen Träger von Krankenhäusern dahin einzuwirken, dass die für staatliche Krankenhäuser geltenden Grundsätze dort analog angewandt werden.

Seelsorge ist eine aufsuchende („den Schafen nachgehende“) Tätigkeit. Dem Krankenhaus- oder Anstaltsseelsorger werden mit der Übermittlung der Daten über die Kirchenmitgliedschaft von Patienten erste (aber nicht: einzige!) Anhaltspunkte für das Ansprechen der „Seelen“ gegeben. Auch über den Kreis dieser Betroffenen hinaus muss es den Seelsorgern möglich gemacht werden, konkrete Bedürfnisse nach Seelsorge zu ermitteln, also alle Kranken persönlich und ohne Zuhörer anzusprechen. Ferner muss es jedem Patienten möglich sein, ihrerseits auf die Seelsorger zuzugehen und ein vertrauliches Gespräch zu führen.

Aus alledem folgt z. B. für Krankenhäuser, sinngemäß auch für Justizvollzugsanstalten u. ä.:

1. Es ist die verfassungsrechtliche (oder daraus abgeleitet: vertragliche) Pflicht der jeweiligen Krankenhausleitung, den Patienten nach seiner Konfession zu befragen und die entsprechenden personenbezogenen Informationen der Krankenhausseelsorge mitzuteilen. Es versteht sich, dass die Beantwortung der Frage freiwillig erfolgt.

2. Unabhängig von diesen Mitteilungen ist es den Krankenhausseelsorgern zu gestatten, die Patienten - und zwar unabhängig von ihrer Konfessionszugehörigkeit - aufzusuchen und zu befragen, ob sie Seelsorge wünschen.

3. Die Befragung der Patienten durch die Krankenhausleitung, ob sie eine Seelsorge wünschen, gehört nicht zu den Pflichten der Krankenhausleitung; die entsprechende Datenerhebung erfolgt ohne Rechtsgrundlage.

4. Den Patienten ist darüber hinaus in allen Krankenhäusern die Möglichkeit zu eröffnen, selbst von sich heraus auf die Krankenhausseelsorge zuzugehen.

10.1.3 Reichweite der Aufsichtsrechte des SMS gegenüber unteren Behörden in kommunaler Trägerschaft

In einer Stellungnahme zu einem Forschungsvorhaben hatte ich das SMS gebeten, in seiner Funktion als oberste Landesgesundheitsbehörde die Gesundheitsämter der Landkreise und kreisfreien Städte anzuweisen, eine bestimmte Datenübermittlung an das Forschungsinstitut nicht vorzunehmen.
Das SMS hat die Auffassung vertreten, dass es die Befugnis zu einer solchen Anweisung nicht habe.

Eine solche Weisungsbefugnis ergibt sich nicht kraft bloßer Rechtsaufsicht. Rechtsaufsicht kann nur nacheilend tätig werden, sofern nicht zusätzlich präventive Aufsichtsmittel wie Genehmigungs- oder Anzeigevorbehalte *gesetzlich vorgesehen* sind. Bloße, d. h. nicht mit solchen Erweiterungen versehene Rechtsaufsicht ermöglichte also dem SMS nicht, z. B. für Vorgehen der Gesundheitsämter Weisungen zu erteilen, wenn solche Weisungen nicht eigens in einem Bundes- oder Landesgesetz vorgesehen sind.

Jedoch hat das SMS über die Rechtsaufsicht hinaus auch die Fachaufsicht. Denn gemäß § 3 Abs. 1 SächsGDG nehmen die Landkreise und kreisfreien Städte die Aufgaben und Befugnisse der Gesundheitsämter als übertragene Aufgaben wahr. Die Aufgaben der Landkreise und kreisfreien Städte als unterer Verwaltungsbehörden (§ 2 Abs. 1 Nr. 3 SächsGDG) stellen somit sog. Pflichtaufgaben nach Weisung im Sinne des § 2 Abs. 3 SächsGemO dar. Zwar hat der Gesetzgeber im Sächsischen Gesundheitsdienstegesetz ein Weisungsrecht nicht ausdrücklich normiert. Aber die Vorschrift des Sächsischen Gesundheitsdienstegesetzes hat nach damaligem Recht für die Begründung eines Weisungsrechts ausgereicht (vgl. Quecke/Schmid Rdnr. 55, a. Anf., Rdnr. 57 zu § 2 SächsGemO; Vietmeier DVBl. 1993, 190). Art. 85 Abs. 3 SächsVerf und § 2 Abs. 3 Satz 2 SächsGemO bzw. § 2 Abs. 3 Satz 2 SächsLKrO sind erst später in Kraft getreten.
Dementsprechend führt die Kommentierung von Quecke/Schmid a.a.O. Rdnr. 55 § 4 SächsGDG als Beispiel für die Übertragung einer *Weisungsaufgabe* in der Weise auf, dass es keinen Unterschied zum Beispiel zu § 2 Abs. 2 SächsMG gibt - einer Regelung, die als nachkonstitutionelle genau den Umfang des Weisungsrechts angibt und damit die Anforderungen des Art. 85 Abs. 3 SächsVerf erfüllt.

Kurz: Die Pflichtaufgabe gemäß § 4 SächsGDG ist nicht mit Erlass der Sächsischen Verfassung bzw. der Sächsischen Landkreisordnung und der Sächsischen Gemeindeordnung weisungsfrei geworden (obwohl es nach heutigem sächsischem Recht fachaufsichtlich weisungsfreie Pflichtaufgaben geben kann).

Die Fachaufsicht aber berechtigt zu Weisungen (Gern, Sächsisches Kommunalrecht, Rdnr. 943), seien es Verwaltungsvorschriften oder Einzelweisungen (Quecke/Schmid Rdnr. 63 zu § 2 SächsGemO).

Das SMS stimmt mir im Ergebnis zu. Es bestehe ein fachaufsichtliches Weisungsrecht. Zur Klarstellung sei beabsichtigt, dieses Weisungsrecht bei einer Novellierung des Sächsischen Gesundheitsdienstegesetzes ausdrücklich zu normieren.
Die von mir erbetene Anweisung gegenüber den Gesundheitsämtern hat das SMS vorgenommen.

10.2 Sozialwesen

10.2.1 Überlegungen zu einer Übertragung des Einzuges von Forderungen von Sozialleistungsträgern gegen Dritte (§ 116 SGB X) auf Private

Ist jemand geschädigt worden und hat deshalb einen Anspruch auf Schadensersatz gegen den Schädiger, so geht dieser Anspruch gemäß § 116 SGB X auf den Versicherungsträger über, soweit der Versicherungsträger wegen des Schadensereignisses Sozialleistungen erbringen musste. Einige Versicherungsträger haben vor, diese Schadensersatzforderungen nicht mehr selber geltend zu machen, sondern die Geltendmachung und Einziehung der Forderungen auf private Dritte zu übertragen.

Im Ergebnis bin ich der Auffassung, dass die Übertragung dieser Aufgabe eine Funktionsübertragung wäre, die vom Gesetz nicht vorgesehen ist. Die damit verbundene Weitergabe von Sozialdaten wäre rechtswidrig. Dies gälte auch, falls man unterhalb der Schwelle der Abtretung (Factoring) bliebe und sich mit einer bloßen Einziehungsermächtigung oder auch nur Bevollmächtigung begnügte.

Auch die (verkaufsweise) Abtretung einer bereits titulierten Forderung wäre rechtswidrig, weil nämlich auch damit die Übermittlung von Sozialdaten im Sinne von § 67 Abs. 1 Satz 1 SGB X verbunden wäre. Aus § 71 Abs. 1 Satz 2 SGB X lässt sich meiner Meinung nach nichts Gegenteiliges folgern.

§ 116 SGB X regelt selbstverständlich gesetzliche Aufgaben der Sozialleistungsträger und damit auch der Krankenkassen - eben gerade als allgemeine Vorschrift, die

nicht sinnvoll in SGB IV, erst recht nicht in SGB V eingeordnet worden wäre. Aus der Möglichkeit, gemäß § 110 Abs. 2 SGB VII den Haftungsausschluss des Absatzes 1 dieser Vorschrift - und damit einen wesentlichen Zweck der gesetzlichen Unfallversicherung - auszudehnen, lässt sich nichts Gegenteiliges ableiten.

Ich habe das SMS über meinen ablehnenden Rechtsstandpunkt zu diesem sog. Outsourcing im Krankenversicherungsbereich unterrichtet.

10.2.2 Speicherung personenbezogener Daten im Rahmen eines Feststellungsverfahrens nach § 69 SGB IX

Aufgrund einer Eingabe stellte sich die Frage, ob ein Gericht personenbezogene Daten speichern darf, die es durch eine Vernehmung von Zeugen im Rahmen eines Feststellungsverfahrens nach § 69 SGB IX erhoben hat. Zu klären war in diesem Zusammenhang, ob das Gericht damit rechtsprechend oder in einer Justizverwaltungsangelegenheit tätig war - nur im letzten Fall bin ich für die Kontrolle zuständig.

Ein Sozialamt hat im Rahmen der Nachprüfung der Schwerbehinderteneigenschaft die den Schwerbehinderten behandelnde Ärztin um Erstattung eines Befundberichts gebeten. Da die Ärztin diesen nicht abgegeben hat, hat das Sozialamt das Sozialgericht um Vernehmung der Ärztin gebeten. Gemäß § 22 Abs. 1 Satz 1 SGB X kann die Behörde das zuständige Sozial- oder Verwaltungsgericht um Vernehmung ersuchen, wenn ein Zeuge oder Sachverständiger die Aussage oder Erstattung des Gutachtens verweigern, ohne dazu berechtigt zu sein. § 22 SGB X soll die Zeugenaussage und die Gutachtenerstellung erzwingen, soweit Zeugen und Sachverständige sie nicht erbringen, obwohl sie nach § 21 Abs. 3 SGB X hierzu verpflichtet sind. Da die Behörde selbst keinen Verwaltungszwang anwenden kann, eröffnet ihr das Gesetz die Möglichkeit, Zeugen und Sachverständige durch das Gericht vernehmen zu lassen, das seinerseits die in den Verfahrensordnungen vorgesehenen Zwangsmittel einzusetzen berechtigt ist.

Führt das Gericht nun auf Ersuchen der Behörde die Vernehmung des Zeugen oder sachverständigen Zeugen durch, so protokolliert es diese Aussage. Ob in dieser Niederschrift und in der zu dem Verfahren beim Gericht geführten Akte unzulässigerweise personenbezogene Daten des Behinderten gespeichert werden, darf ich nicht prüfen. Denn gemäß § 24 Abs. 2 SächsDSG unterliegen die Gerichte meiner Kontrolle nur, soweit sie in Justizverwaltungsangelegenheiten tätig werden. Dies ist der Fall z. B. bei der Personalverwaltung oder bei der Ausübung der Aufsicht über Rechtsanwälte, Notare und Gerichtsvollzieher. Nicht dazu gehört die Rechtsprechung, die in richterlicher Unabhängigkeit ausgeübt wird. Justizverwaltungsangelegenheiten sind also weder Urteile noch Beschlüsse noch deren Inhalt einschließlich der Wortwahl, noch alle einer solchen Entscheidung vorausgehenden

gerichtlichen Maßnahmen (Karlsruher Kommentar - Kissel, EGGVG, § 23, Rdnr. 12) - wie die Durchführung einer Beweisaufnahme, die Vernehmung von Zeugen.
Das gilt auch im Fall des § 22 SGB X, also der Vernehmung auf Ersuchen einer Behörde, die selbst ja öffentlich-rechtliche Verwaltungstätigkeit nach dem SGB ausübt (vgl. § 1 SGB X). Dass Ursache der Zeugenvernehmung die Verwaltungstätigkeit einer Behörde ist, hat keinen Einfluss auf die Ausführung durch die Gerichte. Denn gemäß § 205 Sozialgerichtsgesetz bzw. § 180 Verwaltungsgerichtsordnung findet die Vernehmung von Zeugen und Sachverständigen in diesem Fall vor dem dafür im Geschäftsverteilungsplan bestimmten Richter statt, wobei die Vorschriften der jeweiligen Prozessordnung voll umfänglich Anwendung finden (vgl. Vogelgesang in Hauck/Haines, SGB X/1,2 K § 22 Rdnr. 8, von Wulffen, SGB X, § 22 Rdnr. 8, Obermayer, VwVfG, § 65 Rdnr. 53). Die Geschäftsverteilung bzw. der Geschäftsverteilungsplan dient der Bestimmung des gesetzlichen Richters im Sinne von Art. 101 Abs. 1 Satz 2 GG (vgl. Kopp/Schenke, VwGO, § 4, Rdnr. 7). Bei der Durchführung der Beweisaufnahme ist der gesetzliche Richter gemäß Art. 97 Abs. 1 GG unabhängig und nur dem Gesetz unterworfen, die Zeugenvernehmung auch im Rahmen des § 22 SGB X ist also eine unmittelbar dem Gericht zugewiesene Rechtsprechungsaufgabe. Als solche unterliegt sie nicht meiner Kontrolle.

Auch die Datenübermittlung durch das Gericht, wenn dieses die Niederschrift der Zeugenvernehmung der Behörde zuleitet, unterliegt nicht meiner Kontrolle. Wenn die Behörde die Niederschrift dann zu den Akten des Antragstellers nimmt, verarbeitet sie personenbezogene Daten - die Erhebung, Speicherung und Nutzung der von den Gerichten übermittelten Daten ist gemäß § 11 Abs. 1, § 12 Abs. 1 SächsDSG zulässig. Denn die Kenntnis des ärztlichen Befundes ist für die Entscheidung der Behörde - die Feststellung des Vorliegens einer Behinderung und den Grad der Behinderung (§ 69 Abs. 1 SGB IX) - erforderlich.

10.2.3 Auskunftsverweigerung eines Unfallversicherungsträgers zum Bearbeitungsstand eines Versicherungsfalles unter Berufung auf die Verletzung des Sozialdatenschutzes

Ein Feuerwehrmann war bei einer Übung durch einen Unfall ums Leben gekommen. Die Witwe hatte gegenüber dem Unfallversicherungsträger Leistungen an Hinterbliebene beantragt. Nachdem ein halbes Jahr lang keine Leistungen erfolgt waren, hat sich der Träger der Freiwilligen Feuerwehr, eine Stadtverwaltung, beim Unfallversicherungsträger nach dem Stand des Verfahrens erkundigt. Der Unfallversicherungsträger hat die Auskunft verweigert unter Hinweis darauf, dass die Stadt nicht am Verwaltungsverfahren beteiligt sei.
Die Stadt hat mich gefragt, ob diese Weigerung zu Recht erfolgt sei.
Ich habe der Stadt mitgeteilt, dass ein gesetzlicher Anspruch auf Auskunft nicht

bestünde. Die Stadt könne aber auf Grundlage einer Einwilligung der Witwe des Feuerwehrmannes Auskunft erhalten.

Im Einzelnen ergibt sich das aus Folgendem:
Der Unfallversicherungsträger ist gemäß § 67 Abs. 1 SGB X i. V. m. §§ 35, 12, 22 SGB I an die Vorschriften zum Schutz der Sozialdaten gemäß §§ 67 ff. SGB X gebunden. Für ihn gilt das sog. Sozialgeheimnis gemäß § 35 SGB I.

Aufgrund dessen käme ein Auskunftsanspruch der Stadt im Rahmen der Amtshilfe nach §§ 4 ff. VwVfG (nicht anwendbar sind die Amtshilfe-Regelungen des SGB X, vgl. Hauck/Haines Rdnr. 6 zu § 3 SGB X) nur in Betracht, wenn es für die gewünschte Datenübermittlung eine ausdrückliche Übermittlungsbefugnis nach dem SGB gäbe. Denn gemäß § 5 Abs. 2 Nr. 1 VwVfG darf die um Amtshilfe - hier in Gestalt der sog. Informationshilfe - ersuchte Behörde Hilfe nicht leisten, wenn sie hierzu aus rechtlichen Gründen nicht in der Lage ist, weil die Weitergabe der betreffenden Information verboten ist. Die datenschutzrechtlichen Regelungen gehen den allgemeinen Grundsätzen der Amtshilfe somit vor (vgl. Kopp/Ramsauer Rdnrn. 19, 24 zu § 5 VwVfG). Kurzformel: Datenschutz ist amtshilfefest.

Das in § 25 SGB X geregelte Recht auf Akteneinsicht kommt nicht als Grundlage eines Anspruchs auf Erteilung der gewünschten Auskunft durch den Unfallversicherungsträger an die Stadt in Betracht, denn die Vorschrift regelt nur das Recht der Beteiligten des sozialrechtlichen Verwaltungsverfahrens auf Einsicht in die das Verfahren betreffenden Akten.

Auch die Information, welchen Stand das vom Versicherungsträger durchgeführte Verwaltungsverfahren hat, unterliegt dem Sozialdatenschutz. Gemäß § 67 Abs. 1 SGB X sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hier handelt es sich um eine Angabe über Verhältnisse der Hinterbliebenen, aber auch des Verstorbenen; für letztere gilt nach Maßgabe des § 35 Abs. 5 SGB I ebenfalls das Sozialgeheimnis.

Gemäß § 67 d SGB X ist eine Übermittlung von Sozialdaten - hier also durch den Versicherungsträger an die Stadt - nur zulässig, soweit das SGB die Übermittlung ausdrücklich erlaubt.

Mangels einer anderen Übermittlungserlaubnis käme eine Übermittlung nur auf der Grundlage einer Einwilligung des Betroffenen in Frage. Diese Möglichkeit folgt aus § 67 b Abs. 1 i. V. m. § 67 Abs. 6 SGB X. Betroffen ist die Witwe, möglicherweise auch Kinder des Verstorbenen, weil sie Verfahrensbeteiligte sind. Betroffen ist möglicherweise auch der Verstorbene; eine Einwilligung der Hinterbliebenen gälte auch für ihn, weil weder eine Verletzung seines postmortalen Persönlichkeitsrechtes

noch ein Interessengegensatz unter den Hinterbliebenen insoweit ersichtlich ist (vgl. Schroeder-Printzen Rdnr. 4, Hauck/Haines Rdnr. 60, jeweils zu § 67 b SGB X).

Mit Hilfe einer ausdrücklichen schriftlichen Erklärung der Witwe, zugleich auch im Namen minderjähriger Kinder, dass sie darin einwillige, dass die Stadt vom Unfallversicherungsträger Auskunft zum Verfahrensstand bekomme, wäre der Versicherungsträger insoweit von seiner Schweigepflicht entbunden. Darin läge zugleich eine Einwilligung in die Erhebung der Daten durch die Stadt.

10.2.4 Verhältnismäßigkeit der Datenerhebung bei einem Antrag auf Gewährung von Sozialhilfe

Ein Sozialamt verlangt bei jedem Erstantrag auf laufende Hilfe zum Lebensunterhalt (§ 11 ff. BSHG), dass der Antragsteller der Erteilung von Bankauskünften zustimmt; hierzu legt es ihm ein Formblatt „Befreiung vom Bankgeheimnis und Ermächtigung zur Auskunftserteilung aus Anlass von einkommens- und vermögensabhängigen Leistungen“ vor. Ein Petent hat sich an mich gewandt und gefragt, ob er der Erteilung einer Auskunft durch die kontoführende Bank zustimmen müsse, obwohl er im Antrag seine Einkommens- und Vermögensverhältnisse offengelegt und sämtliche Kontoauszüge der letzten drei Monate vor Antragstellung vorgelegt hatte. Durch dieses Verlangen des Sozialamtes glaubte sich der Petent verdächtigt, falsche Angaben über sein Einkommen und Vermögen gemacht zu haben.

Dieses vorbehaltlose Verlangen des Sozialamtes ist rechtswidrig. Zwar hat, wer Sozialleistungen beantragt, alle Tatsachen anzugeben, die für die Leistung erheblich sind (§ 60 Abs. 1 Nr. 1, 1. Halbsatz SGB I). Die Hilfe zum Lebensunterhalt ist dem zu gewähren, der seinen notwendigen Lebensunterhalt nicht oder nicht ausreichend aus eigenen Mitteln und Kräften, vor allem aus seinem *Einkommen* und *Vermögen*, beschaffen kann (§ 11 Abs. 1 Satz 1 BSHG). Der Antragsteller muss also sein Einkommen und Vermögen offenlegen - kann er die Angaben selbst nicht machen, so hat er auf Verlangen des Trägers der Sozialhilfe der Erteilung der erforderlichen Auskunft durch einen auskunftsfähigen Dritten zuzustimmen (§ 60 Abs. 1 Satz 1 Nr. 1, 2. Halbsatz SGB I).

Hat jedoch der Antragsteller Angaben zu seinem Einkommen und Vermögen gemacht, anhand deren seine Bedürftigkeit und Leistungsberechtigung festgestellt werden können, so sind Bankauskünfte gerade nicht erforderlich. Wenn schon die Auskunftserteilung nicht erforderlich ist, sind es die Zustimmung und das entsprechende Verlangen des Trägers der Sozialhilfe, diese zu erklären, erst recht nicht. Zwar hat das Sozialamt den Sachverhalt von Amts wegen zu ermitteln (§ 20 SGB X) und sich dabei der Beweismittel zu bedienen, die es nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält (§ 21 Abs. 1 SGB X).

Jedoch bedarf es weiterer Ermittlungen, die letztlich der Überprüfung (dem Beweis) dienen, nicht, wenn der Antragsteller selbst Angaben vollständig gemacht hat. „Ein pauschaler Allgemeinverdacht gegenüber dem von einem Hilfesuchenden abgegebenen Erklärungen und Angaben ist nicht ausreichend, um dem Hilfesuchenden eine besondere Beweisführung aufzugeben. Ohne Vorliegen konkreter Anhaltspunkte ist das Verlangen, der Einholung von Bankauskünften zuzustimmen, aber eine überflüssige Ermittlungstätigkeit des Sozialhilfeträgers und somit nicht *erforderlich* im Sinne von § 60 Abs. 1 Nr. 1 SGB X (HessVGH Beschluss vom 7. Februar 1995, Aktenzeichen 9. TG 3113/94, DVBl. 1995, Seite 702, rechte Spalte).

Zulässig ist das Verlangen also im gesetzlich vorgesehenen Fall, nämlich dann, wenn der Antragsteller selbst nicht in der Lage ist, Angaben zu machen und Kontoauszüge beizubringen. In diesem Fall kann er durch die Erteilung einer Bankauskunft für den nötigen Ersatz sorgen. Hiervon zu unterscheiden ist der Fall, dass der Antragsteller offenkundig mangelnde oder unvollständige Angaben macht, indem er auf den Kontoauszügen Schwärzungen vornimmt oder diese - was anhand der Nummerierung erkennbar ist - nur unvollständig vorlegt. Dann hätte der Antragsteller seine gemäß § 60 Abs. 1 SGB I bestehende Mitwirkungspflicht nicht erfüllt. Denn er ist zur Beibringung der vollständigen und insbesondere - von Einzelfällen einmal abgesehen - vollständig ungeschwärzten Kontoauszüge verpflichtet. (Hierzu habe ich mich in meinem 9. TB unter 10.2.6 ausführlich geäußert.) In diesem Fall könnte der Antragsteller die Angaben machen, er *will* es nur nicht. Das Sozialamt hat sich deshalb darauf zu beschränken, den Antragsteller aufzufordern, die erkennbar fehlenden Informationen nachzuliefern und ihn auf die Folgen hinzuweisen, die sein Unterlassen hat (§ 67 a Abs. 3 Satz 3 SGB X, § 66 Abs. 1 SGB V).

Verhältnismäßig - also zulässig - erscheint das Verlangen nach Zustimmung zur Erteilung von Bankauskünften dann, wenn Verdachtsgründe dafür bestehen, dass der Antragsteller wahrheitswidrige Angaben über sein Einkommen und Vermögen gemacht hat. Das ist z. B. dann der Fall, wenn das Sozialamt - aus welchen Gründen auch immer - Anhaltspunkte dafür hat, dass der Antragsteller bei der Bank, deren Kontoauszüge er vorgelegt hat, oder bei einer anderen Bank weitere Konten führt, über die Einkünfte verbucht werden.
Erhebt sich ein solcher Verdacht, so muss das Sozialamt dies dem Betroffenen mitteilen und *deshalb* (zweckgebunden!) die Zustimmung zur Bankauskunft verlangen.

Ich habe dem betreffenden Sozialamt sowie dem SMS meine Rechtsauffassung mitgeteilt und darüber hinaus das Sozialamt aufgefordert, seine Vorgehensweise zu ändern. Das Sozialamt hat daraufhin erklärt, dass es zukünftig die Zustimmung zur Erteilung von Bankauskünften nicht mehr vorbehaltlos, sondern nur noch in Ausnahmefällen einholen werde - welche Fälle das sind, könne und müsse nicht weiter konkretisiert werden.

Auch das SMS teilt meine Rechtsauffassung, dass das vorbehaltlose Verlangen, der Einholung einer Bankauskunft zuzustimmen, rechtswidrig ist. Es meint jedoch, dass die Erteilung der Bankauskunft auch dann zulässig sei, wenn der Antragsteller offenkundig unvollständige Angaben macht. Von den Angaben, die der Leistungsberechtigte im Rahmen seiner Mitwirkungspflichten erbringen muss, seien die Angaben zu unterscheiden, zu deren Einholung der Antragsteller freiwillig seine Zustimmung erklärt. Das SMS übersieht, dass nicht entschieden werden kann zwischen freiwilligen Angaben und Pflichtangaben. Denn alle für die Bestimmung der Bedürftigkeit und Leistungsberechtigung relevanten Angaben betreffen das Einkommen und Vermögen des Antragstellers; bezüglich *aller* Angaben besteht die Mitwirkungspflicht gemäß § 60 Abs. 1 SGB I.

Auch habe ich Zweifel daran, dass der Antragsteller seine Zustimmung *freiwillig* erklären wird. Denn wenn er bewusst unvollständige Angaben macht, also nur einen Teil seiner Kontoauszüge vorlegt bzw. Schwärzungen vornimmt, so lässt dies doch erkennen, dass er gewisse Angaben zwar machen *kann*, jedoch nicht machen *will*. Wenn er aber diese Angaben nicht machen will, so will er - so scheint es mir - auch nicht, dass das Sozialamt bei seiner Bank Auskünfte einholt. Erteilt er dennoch seine Zustimmung hierzu, so tut er dies nicht aus freiem Willen, sondern weil er Konsequenzen befürchtet, nämlich die abschlägige Bescheidung seines Antrags. Stimmt er der Erteilung der Bankauskunft also zu, erfüllt er seine Mitwirkungs*pflicht*.

Hat das Sozialamt ihn zuvor - wie von mir gefordert (vgl. oben) - zur Nachlieferung der fehlenden Informationen aufgefordert und auf die Folgen eines Unterlassens hingewiesen und kommt der Antragsteller dieser Aufforderung nach, indem er der Einholung von Bankauskünften zustimmt, dann kann das Sozialamt selbst die Auskünfte einholen. Denn dann hatte der Antragsteller die Wahl, auf welche Weise er seine Mitwirkungspflicht erfüllt. Hätte das Sozialamt von ihm die Zustimmung verlangt, hätte es ihm die Möglichkeit des Nachreichens von Kontoauszügen abgeschnitten - was mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren wäre.

10.2.5 Von den Trägern der Sozialhilfe verwendeter Fragebogen zur Auskunft über Einkommens- und Vermögensverhältnisse

Durch eine Eingabe habe ich erfahren, dass ein Sozialamt die Verwandten eines Sozialhilfeempfängers zu deren Einkommen und Vermögen befragt. Zu diesem Zweck übersendet es ihnen einen „Fragebogen zur Auskunft über Einkommens- und Vermögensverhältnisse“. Hintergrund dieser Vorgehensweise ist Folgender: Gemäß

§ 1601 BGB sind Verwandte in gerader Linie (Eltern, Großeltern, Kinder, Enkel) verpflichtet, einander Unterhalt zu gewähren. Gegenüber diesem Unterhaltsanspruch ist die Sozialhilfe grundsätzlich nachrangig (§ 2 Abs. 1 BSHG). Wird einem Bedürftigen bereits Sozialhilfe gewährt, so wird der Nachrang der Sozialhilfe dadurch wieder hergestellt, dass der dem Hilfeempfänger gegen seinen Verwandten zustehende Anspruch Kraft Gesetzes auf den Träger der Sozialhilfe übergeht - das regelt § 91 BSHG. Zusammen mit dem nach bürgerlichem Recht bestehenden Unterhaltsanspruch geht auch der unterhaltsrechtliche Auskunftsanspruch nach § 1605 BGB über (§ 91 Abs. 1 Satz 1 BSHG). Nach dieser Vorschrift sind Verwandte in gerader Linie einander verpflichtet, auf Verlangen über ihre Einkünfte und ihr Vermögen Auskunft zu erteilen, soweit dies zur Feststellung eines Unterhaltsanspruchs oder einer Unterhaltsverpflichtung erforderlich ist. Über die Höhe der Einkünfte sind auf Verlangen Belege vorzulegen.

Mit § 91 Abs. 1 Satz 1 BSHG i. V. m. § 1605 Abs. 1 BGB existiert also eine Rechtsvorschrift im Sinne des § 4 Abs. 1 Nr. 1 SächsDSG, die die Verarbeitung personenbezogener Daten erlaubt. Aus datenschutzrechtlicher Sicht bestehen daher keine Bedenken gegen die Vorgehensweise des Sozialamtes im allgemeinen. Bedenken habe ich jedoch gegen die Zulässigkeit einiger Fragen, die das Sozialamt formularmäßig stellt. Sie sind meines Erachtens nicht *erforderlich* zur Feststellung des Bestehens eines Unterhaltsanspruchs des Hilfeempfängers gegen seinen Verwandten.

Erfragt wird unter anderem, ob der - möglicherweise unterhaltsverpflichtete - Verwandte Eigentümer eines Grundstückes ist. Zum Beweis seiner Angaben soll er einen Grundbuchauszug und einen notariellen Vertrag vorlegen. Gegen die Frage und das Verlangen nach Vorlage des Grundbuchauszuges habe ich nichts einzuwenden, das Verlangen nach Vorlage eines notariellen Vertrages ist jedoch unzulässig, weil *nicht erforderlich*. Der notarielle Vertrag über das Grundgeschäft (denkbar sind: Kaufvertrag oder Schenkung) ist zum Nachweis des Eigentums *gar nicht geeignet*, denn das Eigentum an einem Grundstück geht erst mit Eintragung der Rechtsänderung in das Grundbuch auf den Erwerber über (§ 873 Abs. 1 BGB). Im Übrigen ist das Verlangen nach Vorlage des notariellen Vertrages *unverhältnismäßig* im engeren Sinne, denn sowohl ein Kaufvertrag als auch ein Schenkungsvertrag enthalten weitaus mehr Daten, als erforderlich sind, um die Verpflichtung zur Übereignung nachzuweisen.

Ebenfalls erfragt werden die Bankverbindungen des Verwandten. Diese Frage ist ebenso unzulässig wie die Frage nach den Namen vorhandener Schuldner und die Frage nach Kennzeichen und Neuwert des PKW, dessen Eigentümer der Verwandte ist. Auch diese Angaben sind nicht erforderlich, denn sie beschränken sich nicht auf die Feststellung des Vorhandenseins von Vermögenswerten - Bankguthaben, Forderungen gegen Dritte, PKW -, sondern gehen darüber hinaus: Die Angabe

der kontoführenden Bank, des Namens des Schuldners und des Kennzeichens des PKWs soll letztlich der Überprüfung der Angaben des Verwandten durch Nachfrage bei der Bank, dem Schuldner und der Kfz-Zulassungsstelle ermöglichen. Eine solche Datenerhebung bei Dritten ist jedoch unzulässig, da sie sich weder auf eine wirksame Einwilligung des Betroffenen (§ 4 Abs. 1 Nr. 2 SächsDSG) noch auf eine sie erlaubende Rechtsvorschrift (§ 4 Abs. 1 Nr. 1 SächsDSG) stützen lässt. Einer Auskunftserteilung durch die Bank steht zudem das Bankgeheimnis entgegen.

Das Sozialamt und das SMS, das ich um Stellungnahme gebeten habe, haben meinen Rechtsstandpunkt insoweit akzeptiert; das Sozialamt hat den Fragebogen entsprechend meinen Vorgaben geändert.

Unterschiedliche Rechtsauffassungen bestanden zunächst auch hinsichtlich der Zulässigkeit der Frage nach den Einkommens- und Vermögensverhältnissen des Ehegatten des Verwandten - Bruttoeinkommen und finanzielle Belastungen des Ehegatten sollen detailliert angegeben werden. Gegen die Zulässigkeit dieser Frage habe ich zunächst Bedenken geäußert, da mir unverständlich blieb, ob und inwieweit Einkommen und Vermögen des Ehegatten eines unterhaltspflichtigen Verwandten relevant sind für die Feststellung des Bestehens der Unterhaltspflicht. In Folge der Diskussion der Rechtsstandpunkte bin ich jedoch zu dem Ergebnis gelangt, dass diese Frage zulässig ist: Voraussetzung des Unterhaltsanspruchs des Hilfeempfängers gegen seinen Verwandten ist dessen Leistungsfähigkeit (§ 1603 BGB). Bei der Bestimmung derselben sind vorrangige Unterhaltsansprüche, wie die des Ehegatten des Verwandten zu berücksichtigen. Diese Rangfolge normiert § 1609 Abs. 1 i. V. m. Abs. 2 BGB, wonach der Ehegatte minderjährigen unverheirateten Kindern gleichsteht, die anderen Kindern und anderen Verwandten vorgehen. Es muss also zunächst der Unterhaltsanspruch des einen Ehegatten gegen den anderen, der mit dem Hilfeempfänger verwandt ist, berechnet werden.

In den Fällen des Getrenntlebens und nach der Scheidung ist das einfach: Der unterhaltsverpflichtete Ehegatte ist zur Zahlung einer Geldrente verpflichtet (§ 1361 Abs. 4 BGB und § 1585 Abs. 1 BGB). Für die Feststellung der Leistungsfähigkeit des Verwandten gegenüber dem Hilfeempfänger genügt in solchen Fällen die Angabe der Höhe der Unterhaltsverpflichtung gegenüber seinem Ehegatten. *Nicht erforderlich* wären dagegen Angaben über Einkommen und Vermögen des Ehegatten.

Anders stellt sich die Rechtslage dar, wenn die Ehegatten nicht getrennt leben oder geschieden sind, die eheliche Lebensgemeinschaft vielmehr fortbesteht. Die Verpflichtung zum Unterhalt ergibt sich in diesen Fällen aus §§ 1360, 1360 a BGB. Bei Bestehen der ehelichen Lebensgemeinschaft ist die Zahlung einer Geldrente aber grundsätzlich ausgeschlossen (Palandt/Brudermüller, Bürgerliches Gesetzbuch, § 1360 a Rdnr. 5). Vielmehr ist der Unterhalt „in der Weise zu leisten, die durch die

eheliche Lebensgemeinschaft geboten ist“ (§ 1360 a Abs. 2 BGB). „Die Ehegatten sind einander verpflichtet, die zum gemeinsamen Unterhalt der Familie erforderlichen Mittel für einen angemessenen Zeitraum im Voraus zur Verfügung zu stellen“ (§ 1360 a Abs. 2 BGB). Die Unterhaltspflicht wird also grundsätzlich durch Naturalleistungen erfüllt.

Der Anspruch eines Ehegatten auf Leistung von Naturalunterhalt ist umso geringer, je größer sein Einkommen und Vermögen ist. Je geringer der Unterhaltsanspruch des Ehegatten ist, desto größer ist die Leistungsfähigkeit des Verwandten, so dass er unter Umständen auch dem Hilfeempfänger gegenüber zum Unterhalt verpflichtet ist.

Im Einzelnen: Die Leistungsfähigkeit des dem Sozialhilfeempfänger gegenüber möglicherweise unterhaltspflichtigen Verwandten beurteilt sich gemäß § 76 BSHG nach seinem Einkommen. Dabei ist das anrechenbare Einkommen nach § 76 Abs. 2 und Abs. 2 a BSHG zu bereinigen. Hinsichtlich der Berechnung (Berichtigung des Einkommens) kann die Bundesregierung gemäß § 76 Abs. 3 BSHG durch Rechtsverordnung Näheres bestimmen. Da die Bundesregierung bisher von dieser Möglichkeit des Erlasses einer Rechtsverordnung keinen Gebrauch gemacht hat, können für die Berechnung des Einkommens die Empfehlungen des *Deutschen Vereins für öffentliche und private Fürsorge e. V.* zum früheren Mehrbedarfszuschlag für Erwerbstätige zugrunde gelegt werden (Müller, Der Rückgriff gegen Angehörige von Sozialhilfeempfängern, 1996, S. 117).

Entsprechend den Empfehlungen des Vereins werden - ohne ins Detail zu gehen - für den Verwandten sowie für seinen Ehegatten und seine Kinder verschiedene Regelsätze angerechnet. Weiterhin werden prozentuale Zuschläge sowie die Kosten der Unterkunft und andere Kosten hinzugerechnet, so dass sich am Ende ein Garantiebetrag ergibt, der bei dem Verwandten verbleiben muss. Erst wenn sein Einkommen den Garantiebetrag übersteigt, kann er überhaupt in Anspruch genommen werden.

Setzt sich das Familieneinkommen aus Erwerbseinkommen des Verwandten und seines Ehegatten zusammen, so wird ebenso ein Garantiebetrag berechnet, der bei der Familie verbleiben muss. Entsprechend der Höhe des Einkommens der Ehegatten wird nun der jeweils auf sie entfallende Anteil an dem Garantiebetrag errechnet. Macht der Anteil des Verwandten 50 % des Familieneinkommens aus, so beträgt sein Anteil am Garantiebetrag ebenfalls 50 %. Ist er am Familieneinkommen mit 70 % beteiligt, so beträgt sein Anteil am Garantiebetrag ebenfalls 70 %. Nur wenn sein Einkommen seinen Anteil am Garantiebetrag überschreitet, ist er in der Höhe des über dem Garantiebetrag hinausgehenden Betrages dem Sozialhilfeempfänger gegenüber zum Unterhalt verpflichtet.

Die Höhe des Einkommens seines Ehegatten wirkt sich also auf seine Leistungs-

fähigkeit wie folgt aus: Erzielt auch der Ehegatte ein Einkommen, reduziert sich der Garantiebetrag, der beim Verwandten verbleiben muss. Statt 100 % im Falle der alleinigen Erwerbstätigkeit reduziert er sich je nach Höhe des Einkommens des Ehegatten auf beispielsweise 50 % oder 70 %. Damit vergrößert sich der Differenzbetrag zwischen seinem Gesamteinkommen und dem Garantiebetrag. Ihm steht ein höherer Geldbetrag zur Verfügung, mit dem er u. U. auch dem Sozialhilfeempfänger gegenüber zum Unterhalt verpflichtet ist.

Da also der Differenzbetrag und damit das als Unterhalt einsetzbare Einkommen von der Höhe des Einkommens des Ehegatten abhängig ist, sind auch die Angaben zum Einkommen und Vermögen des Ehegatten für die Berechnung des Unterhaltsanspruchs des Sozialhilfeempfänger *erforderlich*.

So schön kann Jura sein. Will sagen: Auch hier erlebt der Leser ein Beispiel für die Komplexität der Rechtsordnung im Sozialdatenschutz.

10.2.6 Übermittlung von Sozialdaten durch das Sozialamt an das SMS zur Weiterübermittlung an den Petitionsausschuss des Landtages

Der Petitionsausschuss des Landtages hat über das SMS Akten, die beim Sozialamt geführt werden, angefordert, um eine Petition zu bearbeiten. Das Sozialamt, gegen dessen ablehnenden Bescheid sich die Petition wendet, hat sowohl die Vorlage der Akten als auch die Auskunftserteilung verweigert, da eine Befugnis zur Übermittlung von Sozialdaten an das SMS oder an den Petitionsausschuss nicht gegeben sei. Diese Rechtsgrundlage könne sich gemäß § 67 d SGB X nur aus Vorschriften des Sozialgesetzbuches ergeben, und dort sei eben keine Rechtsgrundlage vorhanden.

Da irrt sich das Sozialamt gewaltig, denn es darf dem Landtag über das SMS die Sozialdaten, die zur Erledigung der Petition erforderlich sind, übermitteln. Rechtsgrundlage ist § 67 d Abs. 1 i. V. m. § 69 Abs. 5 SGB X. Nach § 69 Abs. 5 SGBX X ist eine Übermittlung von Sozialdaten zulässig für die Erfüllung der gesetzlichen Aufgaben aller Stellen, auf die § 67 c Abs. 3 Satz 1 SGB X Anwendung findet. Das sind solche Stellen, deren Aufgabe in der Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen besteht. Der Petitionsausschuss des Landtages nimmt solche Aufsichts- und Kontrollbefugnisse auf normenklarer Rechtsgrundlage wahr:
Petitionen, die an den Landtag gerichtet sind, sind in angemessener Frist zu bescheiden. Das ist ausdrücklich in Art. 35 Satz 2 SächsVerf geregelt. Die Erledigung der Petition durch begründeten Bescheid setzt eine sachliche Prüfung des Anliegens des Petenten voraus (vgl. Sachs, Kommentar zum GG, Art. 17 Rdnr. 13). Anliegen des Petenten ist ein „petitum“, d. h. ein außerhalb der förmlichen Rechtsbehelfe

und -mittel geltend gemachtes Begehren, das darauf abzielt, eine öffentliche Stelle zu einem bestimmten Verhalten zu veranlassen. Ob dieses Anliegen begründet ist, muss der Petitionsausschuss prüfen. Eine Bescheidung von Petitionen, die sich gegen das Verhalten von Verwaltungsbehörden richten, ist nur nach sachlicher Prüfung der bisherigen Behandlung des „Vorganges“ durch die Behörde möglich. Deshalb räumt § 5 Abs. 1 und Abs. 2 SächsPetAG dem Petitionsausschuss das Recht ein, von den Behörden Akteneinsicht und Auskunft zu verlangen.
Der Petitionsausschuss übt also außerhalb der förmlichen Rechtsbehelfe und -mittel eine gesetzliche Aufsichts- und Kontrollbefugnis aus.

Deshalb wird auch die oberste Dienst- oder Aufsichtsbehörde in die Prüfung mit einbezogen.
Bestätigt wird das durch die Regelung des § 5 Abs. 3 sowie des § 6 Abs. 2 SächsPetAG.

10.2.7 Herausgabe einer Beistandschaftsakte durch das Jugendamt an das Sozialgericht

Ein Sozialgericht hat bei einem Jugendamt Akten angefordert, die bei einem dort beschäftigten Mitarbeiter entstanden waren, der - wie das gesetzlich vorgesehen ist - als Beistand eines Kindes zur Durchsetzung von Unterhaltsansprüchen gegen den Vater des Kindes eingesetzt war. Der Kindesvater führte nun einen Rechtsstreit gegen die Bundesanstalt für Arbeit, in dem das Sozialgericht aufzuklären hatte, ob der (unterhaltspflichtige) Kindesvater mit seiner ehemaligen Ehefrau unter Vermittlung des Jugendamtes eine Vereinbarung zur Absenkung der Unterhaltszahlungen geschlossen hatte. Das Sozialgericht verlangte hierzu vom Jugendamt Auskunft über die Vereinbarung sowie die Übersendung des „diesbezüglichen Schriftverkehrs“. Das Sozialgericht hatte der Anforderung eine Erklärung des Unterhaltsschuldners beigefügt, in der er sich damit einverstanden erklärte, dass die vom Sozialgericht zur Aufklärung des Sachverhalts im Rechtsstreit gegen die Bundesanstalt für Arbeit für erforderlich gehaltenen Unterlagen, insbesondere die Unterlagen des zuständigen Jugendamtes, beigezogen werden.

Die Herausgabe der Beistandschaftsakte des Jugendamtes an das Sozialgericht, um ein vom Unterhaltsschuldner betriebenes Verfahren in Angelegenheiten der Arbeitsförderung und sonstiger Aufgaben der Bundesanstalt für Arbeit zu führen, ist zur Aufgabenerfüllung des Beistandes nicht erforderlich und damit unzulässig.
Die Führung der Beistandschaft gemäß §§ 55, 56 SGB VIII ist eine sog. andere Aufgabe der Jugendhilfe gemäß § 2 Abs. 3 Nr. 11 SGB VIII, die aber in § 27 Abs. 1 SGB I nicht genannt wird. Deshalb handelt es sich hierbei nicht um eine Sozialleistung, die von einem Sozialleistungsträger (§ 12 SGB I) erbracht wird. Das Jugendamt als Sozialleistungsträger unterstützt lediglich den Mitarbeiter, dem es die Ausübung der

Aufgaben des Beistands übertragen hat, bei der Wahrnehmung dieser Funktion. Diese besteht in erster Linie darin, gesetzlicher Vertreter des Kindes oder des Jugendlichen in dem durch die Übertragung umschriebenen Rahmen zu sein (§ 55 Abs. 2 Satz 3 SGB VIII). Lediglich in zweiter Linie ist es eine Sozialleistung (vgl. Mörsberger in Miesner/Kaufmann/Mörsberger u. a., Kommentar zum SGB VIII, § 68 Rdnr. 1).
Da die Führung der Beistandschaft keine Sozialleistung des Sozialleistungsträgers ist, gilt für die Datenverarbeitung des Beistandes nicht das in § 35 Abs. 1 Satz 1 SGB I festgeschriebene Sozialgeheimnis. Das bedeutet, dass auch § 35 Abs. 2 SGB I nicht anwendbar ist, wonach eine Erhebung, Verarbeitung und Nutzung von Sozialdaten nur unter den Voraussetzungen des zweiten Kapitels des Zehnten Buches (§§ 67 ff. SGB X) zulässig ist.
Für den Schutz von Sozialdaten im Rahmen der Tätigkeit des Jugendamtes als Beistand gilt vielmehr nur § 68 SGB VIII (§ 61 Abs. 2 SGB VIII).

Nach § 68 Abs. 1 Satz 1 SGB VIII darf der Beamte oder Angestellte, dem die Ausübung der Beistandschaft übertragen ist, Sozialdaten nur erheben, verarbeiten oder nutzen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist.
Welche Aufgaben der Beistand zu erfüllen hat, regeln gemäß § 55 Abs. 1 SGB VIII die Vorschriften des Bürgerlichen Gesetzbuches, nämlich die §§ 1712 ff. BGB. Danach wird das Jugendamt Beistand des Kindes für die Feststellung der Vaterschaft, die Geltendmachung von Unterhaltsansprüchen sowie die Verfügung über diese Ansprüche.
Das Sozialgericht gibt an, die Beistandschaftsakte für die Sachverhaltsaufklärung in einem Rechtsstreit des Unterhaltsschuldners gegen die Bundesanstalt für Arbeit zu benötigen. Die Bundesanstalt für Arbeit ist Träger der Arbeitsförderung (§ 367 Satz 1 SGB III). Gegenstand des Rechtsstreites ist also eine Angelegenheit der Arbeitslosenversicherung oder der übrigen Aufgaben der Bundesanstalt für Arbeit. Mit der Führung der Beistandschaft, insbesondere der Geltendmachung von Unterhaltsansprüchen des Kindes, hat der Rechtsstreit des Unterhaltsschuldners gegen die Bundesanstalt für Arbeit nichts zu tun.
Folglich ist eine Datenübermittlung durch den Beistand an das Sozialgericht unzulässig.

Etwas anderes ergibt sich auch nicht aufgrund der Einwilligungserklärung des Unterhaltsschuldners.
Die Beistandschaftsakte enthält Informationen nicht nur über den Unterhaltsschuldner, sondern auch über das Kind, über die Sorgeberechtigte(n) sowie unter Umständen über weitere Personen. Neben dem Unterhaltsschuldner müssten also alle weiteren Betroffenen, also alle diejenigen, über die die Akte Informationen enthält, in die Übermittlung durch den Beistand an das Sozialgericht zu dem vom Gericht angegebenen Zweck einwilligen. Für das Kind müsste, falls dieses noch nicht die ausreichende Einsichtsfähigkeit besitzt, der gesetzliche Vertreter einwilligen.

Die Einwilligungserklärung allein des Unterhaltsschuldners reichte allerdings dann aus, wenn es sich um sog. Daten mit Doppelbezug handelte. Das sind solche Daten, die eine Aussage zwar über andere Personen als den Unterhaltsschuldner treffen, aber zugleich eben auch eine Aussage über den Unterhaltsschuldner selber. Ob ein solches Datum mit Doppelbezug vorliegt oder nicht, müsste der Beistand vor der Übermittlung des Datums für jedes Datum gesondert feststellen.

10.2.8 Im Rahmen der Berufung in den Landesseniorenbeirat vom SMS angeforderte Erklärung über MfS-Tätigkeit

Auf Grundlage einer Verwaltungsvorschrift wird in Sachsen ein sog. Landesseniorenbeirat gebildet, der die Staatsregierung zu Fragen berät, die die Lebensumstände der Senioren in Sachsen betreffen. Die Mitglieder dieses Beirates werden durch den Staatsminister für Soziales, Gesundheit, Jugend und Familie berufen. Sie üben ein Ehrenamt aus.
Das SMS forderte bisher von den zu berufenden Mitgliedern eine Erklärung über eine etwaige System-Nähe zu DDR-Zeiten an. Der Staatsminister hat mich um eine Stellungnahme hierzu gebeten.

Ich habe dem Staatsminister geraten, auf eine solche Befragung der designierten Seniorenbeirats-Mitglieder zu verzichten.

Für die Erhebung der abgefragten Daten gibt es keine Rechtsgrundlage. Die für den öffentlichen Dienst, einschließlich der Wahlbeamten, geltenden Vorschriften, insbesondere Art. 119 SächsVerf, sind auf den Landesseniorenbeirat nicht anwendbar. Nach der Verwaltungsvorschrift ist er ausschließlich Organ der Meinungsbildung und des Erfahrungsaustausches der Beteiligten zum Zweck der Beratung der Staatsregierung. Damit sind die Mitglieder des Beirates nicht als solche Teil der öffentlichen Verwaltung.
Hinzu kommt: Die verlangten Angaben zur Tätigkeit für den DDR-Staatssicherheitsdienst und ähnlicher Einrichtungen könnten vom SMS nicht überprüft werden, weil eine Auskunft des BStU gemäß § 20 Abs. 1 Nr. 6, § 21 Abs. 1 Nr. 6 StUG nicht zu erlangen wäre.
Für eine Überprüfung auf freiwilliger Grundlage gemäß § 20 Abs. 1 Nr. 7, § 21 Abs. 1 Nr. 7 StUG fehlt ebenfalls die Rechtsgrundlage, weil Mitglieder von Beiräten der genannten Art, insbesondere auch Anwärter auf eine Beiratsmitgliedschaft nicht unter den Katalog der genannten Vorschriften fallen.
Auch die angebliche Freiwilligkeit der Auskunftserteilung begründete keine Rechtmäßigkeit der Datenerhebung durch das SMS. Die Einwilligung der Betroffenen ersetzt die fehlende gesetzliche Aufgabenzuweisung nicht. Darüber hinaus ist die Freiwilligkeit der Einwilligung zweifelhaft, weil der Betroffene bei Verweigerung der Erklärung mit der Nicht-Berufung in den Beirat rechnen muss.

Dieses Ergebnis ist zwar juristisch sauber, aber eben doch unbefriedigend, wenn man bedenkt, dass der Sozialminister sich auf einen Ratgeber verlassen soll, der möglicherweise in früheren Zeiten gegen die Grundsätze der Menschlichkeit oder der Rechtsstaatlichkeit verstoßen hat. Ich habe dem Minister geraten, sich die Verbände, die die Mitglieder des Beirates vorschlagen, genau anzusehen und sie zu bitten, nur wirklich geeignete Persönlichkeiten zu benennen. Mehr kann er nicht tun.

Das SMS wird in Zukunft Erklärungen zur MfS-Vergangenheit der Beiräte nicht mehr anfordern.

10.2.9 Bekanntgabe von Sozialdaten durch Staatsanwaltschaften gegenüber der Presse

Ein Staatsanwalt hatte der Presse mitgeteilt, dass ein Augenarzt unter dem Verdacht stehe, gegenüber der Krankenkasse die Verschreibung von Kontaktlinsen unrechtmäßig abgerechnet zu haben.
Verstößt eine solche Pressemitteilung gegen das sog. verlängerte Sozialgeheimnis gemäß § 78 SGB X?

§ 78 Abs. 1 Satz 2 SGB X schreibt vor, dass auch der Empfänger von Sozialdaten, der keine Stelle im Sinne des § 35 SGB I und damit grundsätzlich nicht zur Wahrung des Sozialgeheimnisses verpflichtet ist, dieses Sozialgeheimnis zu wahren hat.

Verstießen ein Staatsanwalt oder ein Gericht, die gegen einen Leistungserbringer ermitteln, gegen das Sozialgeheimnis, wenn sie Informationen über das Strafverfahren an die Presse weitergeben, so bedeutete dies, dass solche Informationen niemals bekannt gegeben werden dürften, sofern der Personenbezug herstellbar ist. Das hätte wohl zur Folge, dass die Öffentlichkeit über Straftaten, die im Zusammenhang mit Sozialleistungen stehen, niemals unterrichtet werden dürfte. Auch die Öffentlichkeit der Hauptverhandlung in sämtlichen Strafverfahren dieser Art wäre somit infrage gestellt.

Zum gegenteiligen Ergebnis kommt man mit folgender Überlegung: § 78 Abs. 1 Satz 5 SGB X gestattet es Polizeibehörden, Staatsanwaltschaften und Gerichten sowie Behörden der Gefahrenabwehr, denen Sozialdaten übermittelt worden sind, diese Daten unabhängig vom Zweck der Übermittlung für Zwecke der Gefahrenabwehr, der Strafverfolgung und der Strafvollstreckung zu verarbeiten. Die Mitteilungen, die Staatsanwaltschaften und Gerichte nach allgemeinen Regeln zulässigerweise gegenüber der Presse machen, gehören meiner Auffassung nach - als Annex - zur Tätigkeit der betreffenden Stellen *zum Zwecke der Strafverfolgung*. Denn Strafverfolgung schließt neben den Strafzwecken der persönlichen Sühne, der Resozialisierung, der Prävention in Bezug auf den Täter (Spezialprävention)

auch die Abschreckung der Allgemeinheit (Generalprävention) ein. Andere Zwecke dürfen diese Stellen gar nicht verfolgen. Es ist ja begründungsbedürftig, dass - soweit dies zulässigerweise geschieht und dann auch auf Verlangen zu geschehen hat - Strafverfolgungsbehörden personenbezogene Daten der Presse mitteilen dürfen; dasselbe gilt für alle Mitteilungen, die Behörden, etwa im Bereich des Gesundheitswesens, der Umwelt und dergleichen, gegenüber der Presse machen. Man wird dies zwanglos datenschutzrechtlich nur so verstehen können, dass es sich um eine privilegierte Zweckänderung zugunsten eines Annexzweckes handelt, der für alle Behörden in gleicher Weise gilt, wie es auch für die in den Datenschutzgesetzen üblicherweise aufgeführten Annexzwecke wie Wahrnehmung von Aufsichts- und Kontrollbefugnissen, Rechnungsprüfung, Durchführung von Organisationsuntersuchung, Statistik für den Eigenbedarf (Statistiken im Verwaltungsvollzug), Ausbildungs- und Prüfungszwecke der Fall ist.

§ 477 Abs. 2 Satz 1 StPO steht dem nicht entgegen: Zum einen geht es gerade darum, § 78 Abs. 1 Satz 5 SGB X im Hinblick darauf *auszulegen,* inwieweit die Vorschrift als Verwendungsregelung einer Auskunft entgegenstehen könnte. Zum anderen sind die presserechtlichen Übermittlungsbefugnisse von Staatsanwaltschaften und Strafgerichten gerade nicht in der StPO und im EGGVG, sondern allgemein in § 4 SächsPresseG geregelt.

Die Unterrichtung der Presse - soweit legitimerweise auch personenbezogen - gehört im Vergleich zu anderen Behörden in einem gesteigerten Maße zu den Aufgaben der Strafverfolgungsbehörden (Staatsanwaltschaften, Strafgerichte): Zu der allgemeinen - und natürlich begrenzten - *Pressepflichtigkeit* der Träger öffentlicher Gewalt, die aus dem Demokratieprinzip folgt, kommt im Falle der Strafverfolgung der general-präventive Zweck der Strafe hinzu, dem unter heutigen gesellschaftlichen Bedingungen natürlich mit der Öffentlichkeit der Hauptverhandlung allein zu wenig gedient wäre.

11 Landwirtschaft, Ernährung und Forsten

11.1 Weitergabe von Anschriften und Telefonnummern von Jagdvorstehern durch die Landkreise und kreisfreien Städte als untere Jagdbehörden an Dritte

Ein Landkreis wollte wissen, ob es zulässig sei, dass er als untere Jagdbehörde (§ 51 Abs. 2 Nr. 3 SächsLJagdG) einem Dritten den Namen, die Anschrift und die Telefonnummer der Jagdvorstände der Jagdgenossenschaften im Kreisgebiet übermittelt.

Die Übermittlung dieser personenbezogenen Daten des Jagdvorstandes der jeweiligen Jagdgenossenschaft ist zulässig, und zwar aus folgendem Grund:

Eine Jagdgenossenschaft setzt sich gemäß § 9 Abs. 1 Satz 1 BJagdG aus den Eigentümern der Grundflächen zusammen, die zu einem gemeinschaftlichen Jagdbezirk gehören. Diese Jagdgenossenschaft ist gemäß § 11 Abs. 1 Satz 1 SächsLJagdG eine Körperschaft des öffentlichen Rechts. Der Jagdvorstand vertritt die Jagdgenossenschaft gerichtlich und außergerichtlich, § 9 Abs. 2 Satz 1 BJagdG. Als Vorstand einer Körperschaft des öffentlichen Rechts ist der Jagdvorstand ein Amtsträger. Die dienstliche Anschrift des Amtsträgers unterliegt nicht den Regelungen zum Schutz personenbezogener Daten, da mit dieser Angabe keine Aussage getroffen wird über die natürliche Person, sondern über deren öffentliches Amt.

Die untere Jagdbehörde darf also den Namen sowie die dienstliche Anschrift und Telefonnummer der Vorstände der Jagdgenossenschaften weitergeben. Das gilt auch dann, wenn die dienstliche Anschrift identisch ist mit der Privatanschrift des Jagdvorstandes: Hat die Jagdgenossenschaft keine Amtsräume und ist dienstlicher Kontakt deshalb nur über die Privatanschrift bzw. die private Telefonnummer des Vorstandes möglich, so begibt sich der jeweilige Vorstand mit der Angabe seiner Privatanschrift bzw. privaten Telefonnummer als dienstlicher Adresse bzw. Telefonnummer insoweit des Schutzes, unter dem diese Daten als personenbezogenes - privates - Datum stehen.

11.2 Datenübermittlung durch die Ämter für Landwirtschaft an die Sächsische landwirtschaftliche Berufsgenossenschaft auf der Grundlage vom § 197 Abs. 4 SGB VII

Durch das Gesetz zur Organisationsreform der landwirtschaftlichen Sozialversicherung (LSVOrgG) vom 17. Juli 2001 wurde auch § 197 SGB VII geändert: Der

neu eingefügte Absatz 4 Satz 1 i. V. m. Satz 4 normiert, dass die Ämter für Landwirtschaft dem Gesamtverband der landwirtschaftlichen Alterskassen (Kopfstelle) durch ein automatisiertes Abrufverfahren die bei ihnen maschinell vorhandenen Daten zur Weiterleitung an die zuständigen landwirtschaftlichen Berufsgenossenschaften übermitteln. Obwohl ein automatisiertes Abrufverfahren derzeit noch nicht eingerichtet ist, ersucht die Sächsische landwirtschaftliche Berufsgenossenschaft (SLBG) im Rahmen der Amtshilfe ein Amt für Landwirtschaft (AfL) um Mitteilung der Betriebsgröße eines landwirtschaftlichen Unternehmens (landwirtschaftliche Nutzfläche in Hektar). Die SLBG meint, das AfL sei ihr gemäß § 197 Abs. 4 SGB VII zur Auskunft verpflichtet. Das AfL verweigert die Auskunft mit der Begründung, die Datenübermittlung sei nicht zulässig. Der Vorgang wurde mir zur Prüfung vorgelegt, ich bin zu folgendem Ergebnis gelangt:

Ob die AfL *verpflichtet* sind, der SLBG die im Einzelfall verlangten Angaben über die Betriebsgröße zu übermitteln, habe ich nicht zu beurteilen. Datenschutzrechtlich stellt sich nämlich nur die Frage, ob die Übermittlung *zulässig* wäre. (Allerdings sind Übermittlungen, die geboten sind, selbstverständlich auch erlaubt.) Mit dieser datenschutzrechtlich bedingten Einengung ist die Frage der Zulässigkeit der Übermittlung wie folgt zu beantworten:

Insoweit Daten eines landwirtschaftlichen Betriebes gemäß § 197 Abs. 4 Satz 1 i. V. m. Satz 4 und i. V. m. Abs. 2 SGB VII von einem AfL an den Gesamtverband der landwirtschaftlichen Alterskassen durch automatisiertes Abrufverfahren zur Weiterleitung übermittelt werden dürfen, ist die betreffende Übermittlung *auch außerhalb* des automatischen Abrufverfahrens *unmittelbar an die SLBG* zulässig. Die Gründe sind folgende:

(1) Zur Abweichung im Übermittlungsverfahren:

§ 197 Abs. 4 Satz 1 i. V. m. Satz 4 SGB VII gebietet die Übermittlung im Wege eines automatisierten Abrufverfahrens. Daraus folgt, dass die Einrichtung eines solchen Verfahrens rechtmäßig ist und dass eine Nutzung erlaubt ist, sofern die konkreten Voraussetzungen der betreffenden Übermittlung erfüllt sind. Rechtsgrundlage für die einzelne Übermittlung ist ebenfalls § 197 Abs. 4 Satz 1 i. V. m. Satz 4 SGB VII, der abstrakt auch die Voraussetzungen der Nutzung des Verfahrens, also der Übermittlung, aufführt. Die Vorschrift enthält also - aus logischen Gründen - zugleich eine schlichte Übermittlungs-Erlaubnis-Regel. Denn sie setzt für die Einrichtung und Nutzung des automatisierten Abrufverfahrens die nicht in einer anderweitigen Vorschrift ausgesprochene Erlaubtheit der betroffenen Übermittlung voraus.

(2) Zur Abweichung beim Übermittlungsempfänger:

Nicht nur die (einfache) Übermittlung an den Gesamtverband der landwirtschaftlichen Alterskassen (Kopfstelle) ist zulässig, sondern gerade auch die Übermittlung unmittelbar an die landwirtschaftlichen Berufsgenossenschaften. Übermittelt werden sollen und dürfen die Daten gemäß § 197 Abs. 4 SGB VII nämlich *zur Weiterleitung an die zuständigen landwirtschaftlichen Berufsgenossenschaften*, d. h. die Übermittlung an die sog. Kopfstelle erfolgt ausschließlich zum Zweck der Weiterleitung, also Übermittlung, an die Berufsgenossenschaften. Denn diese (oder in anderen Fällen andere Träger der landwirtschaftlichen Sozialversicherung) sind es, die die in § 197 Abs. 2 SGB VII aufgeführten Daten zur Erfüllung ihrer gesetzlichen Aufgaben benötigen. Das dürfte selbstverständlich sein; es ergibt sich auch aus der amtlichen Überschrift des neuen § 197 SGB VII in der Fassung des Artikels 1 Nr. 8 Buchstabe a LSVOrgG: „Träger der landwirtschaftlichen Sozialversicherung“ sind nach wie vor (§ 123 SGB VII) unter anderem die landwirtschaftlichen Berufsgenossenschaften, und nicht etwa der Gesamtverband der landwirtschaftlichen Alterskassen, vgl. § 58 b ALG in der Fassung des Art. 2 des LSVOrgG. Vgl. ferner auch BT-DS 14/6177 S. 23 rechte Spalte unten.

Die Kopfstelle ist nur eine im Gesetz um der rationalen Aufgabenerfüllung willen zulasten des Datenschutzes hingenommene Zwischenstation, die selbst die Daten nicht für eigene Zwecke verarbeitet, sondern sie nur übermittelt.

Zusammenfassen kann man beide Überlegungen auf folgende Weise: Soweit das Gesetz die Datenübermittlung im gefährlichen automatischen Abrufverfahren und unter Einbeziehung eines Dritten bzw. eines Umweges erlaubt, erlaubt es erst recht die entsprechende Datenübermittlung ohne diese beiden dem Datenschutz abträglichen Umstände.

12 Umwelt

12.1 Übermittlung personenbezogener Daten durch ein Einwohnermeldeamt an einen Zweckverband

Ein Petent bat mich zu prüfen, ob sich ein Abwasserzweckverband vom Melderegister personenbezogene Daten besorgen darf. Der Petent meinte wohl, das Einwohnermeldeamt würde dem Abwasserzweckverband nicht nur Angaben über den Eigentümer als Gebührenschuldner, sondern auch Angaben über den Mieter machen, insbesondere also seinen Namen und seine Anschrift mitteilen.

Gemäß der Satzung des Abwasserzweckverbandes ist der Grundstückseigentümer Gebührenschuldner. Die Satzung regelt weiter, dass Bemessungsgrundlage für die Erhebung der Grundgebühr „die zum Beginn des Veranlagungszeitraumes auf dem Grundstück beim Einwohnermeldeamt gemeldeten Personen“ sind. Der Abwasserzweckverband hat auf meine Anfrage mitgeteilt, dass er bei den Einwohnermeldeämtern lediglich die aktuelle Anzahl der gemeldeten Einwohner abfragt.

Die Übermittlung dieses Datums durch das Einwohnermeldeamt an den Abwasserzweckverband ist zulässig, da eine Rechtsvorschrift - § 13 Abs. 1 SächsDSG - sie erlaubt. (Da die Anzahl der zu einem bestimmten Stichtag für ein bestimmtes Grundstück gemeldeten Personen kein Meldedatum im Sinne des § 29 SächsMG ist, richtet sich die Zulässigkeit der Datenübermittlung nicht nach dem Sächsischen Meldegesetz, sondern nach dem Sächsischen Datenschutzgesetz. Die Anzahl der für ein bestimmtes Grundstück gemeldeten Personen ist ein personenbezogenes Datum des Grundstückseigentümers.) Das Einwohnermeldeamt darf dem Abwasserzweckverband als öffentliche Stelle dieses Datum übermitteln, da es zur Erfüllung der Aufgaben des Abwasserzweckverbandes erforderlich ist und die Voraussetzungen des § 12 Abs. 2 i. V. m. § 11 Abs. 4 Nr. 8 SächsDSG vorliegen. Der Abwasserzweckverband hat gemäß § 63 Abs. 2 Satz 1 SächsWG i. V. m. §§ 1 und 2 SächsKomZG die Aufgabe, das in seinem Gebiet anfallende Abwasser zu beseitigen. Die vom Abwasserzweckverband betriebenen Beseitigungsanlagen sind öffentliche Einrichtungen, für deren Benutzung der Zweckverband gemäß § 9 Abs. 1 SächsWG Benutzungsgebühren erheben kann. Diese werden in einer Gebührensatzung entsprechend § 2 Abs. 1 SächsKAG erhoben. Zur Festsetzung der Grundgebühr ist das Datum „Anzahl der für ein bestimmtes Grundstück gemeldeten Personen“ erforderlich. Auch die Datenverarbeitung beim Einwohnermeldeamt als Drittem ist zulässig, da es einen unverhältnismäßigen Aufwand erforderte, die Daten beim betroffenen Grundstückseigentümer zu erheben.

12.2 Datenverarbeitung durch einen privaten Dritten, der von einem Landkreis beauftragt ist, in seinem Namen und für seine Rechnung einen Wertstoffhof zu betreiben

Ein Landkreis und eine GmbH haben einen „Vertrag über den Betrieb von Wertstoffhöfen“ geschlossen, der Landkreis hat zudem eine „Ordnung für die Nutzung der Wertstoffhöfe“ erlassen. Die Betreiber-Gesellschaft nimmt namens und im Auftrag des Landkreises gegen Gebühr Wertstoffe, wie Sperrmüll, Bauschutt und Gartenabfälle, aber auch Gewerbeabfälle, ab. Entsprechend der Regelung in der „Ordnung für die Nutzung der Wertstoffhöfe“ sind die Gebühren in der festgesetzten Höhe durch Barzahlung zu begleichen, wenn der Anlieferer eine natürliche Person ist. Anders, wenn eine juristische Person Wertstoffe anliefert: In diesem Fall erlässt der Landkreis einen schriftlichen Gebührenbescheid.

In der Quittung über die entrichteten Gebühren, die die Gesellschaft „namens und im Auftrag des Landkreises“ berechnet hat, hat der Anlieferer auch folgende Angaben zu machen: Name, Straße/Hausnummer, Ort, Kfz-Kennzeichen und Uhrzeit. Die Quittung wird im Wertstoffhof als Doppel aufbewahrt.

Diese Erhebung und Speicherung der genannten personenbezogenen Daten halte ich für unzulässig, wenn der Anlieferer eine natürliche Person ist; insoweit ist die Datenverarbeitung auf eine Erhebung zu beschränken, der sich keine Speicherung anschließt. Ist der Anlieferer eine juristische Person, ist neben der Erhebung auch die Speicherung der Daten zulässig.

Der Landkreis als öffentlich-rechtlicher Entsorgungsträger (§ 3 Abs. 1 SächsABG) hat die in seinem Gebiet angefallenen und überlassenen Abfälle zu verwerten oder zu beseitigen (§ 15 Abs. 1 KrW-/AbfG). Mit der Erfüllung dieser Pflichten kann der Landkreis auch Dritte beauftragen, wobei allerdings seine Verantwortlichkeit für die Erfüllung der gesetzlichen Pflichten unberührt bleibt (§ 16 Abs. 1 KrW-/AbfG). Die Betreiber-Gesellschaft übernimmt also nicht die Pflicht als solche, sondern lediglich deren Erfüllung, ist also „Erfüllungsgehilfe“ (vgl. Versteyl in Kunick, KrW-/AbfG, § 16, Rdnr. 12, Frenz, KrW-/AbfG, § 16, Rdnr. 1). Auch wenn also Mitarbeiter der privaten Betreiber-Gesellschaft die Wertstoffe entgegennehmen, erfüllt eigentlich der Landkreis die ihm durch das Gesetz übertragenen Aufgaben. Dabei ist das Benutzungsverhältnis zwischen ihm und dem Anlieferer durch die „Ordnung für die Nutzung der Wertstoffhöfe“ öffentlich-rechtlich ausgestaltet. Die Benutzungsordnung allerdings ist schon aus formellen Gründen nicht als Satzung zu qualifizieren, denn sie ist nicht vom Kreistag beschlossen (§ 3 Abs. 2 SächsLKrO). Vielmehr ist die vom Amtsleiter des Abfallwirtschaftsamtes des Landkreises erlassene Ordnung ein Verwaltungsakt in Gestalt einer Allgemeinverfügung (§ 35 Satz 2 VwVfG

i. V. m. § 1 SächsVwVfG; vgl. Kopp, VwVfG, § 35, Rdnr. 69, Maurer, Allgemeines Verwaltungsrecht, § 9, Rdnr. 34).

Zum Zwecke der Erfüllung der ihnen durch das Kreislaufwirtschafts- und Abfallgesetz zugewiesenen Aufgaben dürfen die zuständigen Behörden bei natürlichen und juristischen Personen die *erforderlichen* Daten erheben und erhobene Daten weiterverarbeiten (§ 12 b Abs. 1 Nr. 1 SächsABG). Zu den für die Aufgabenerfüllung erforderlichen Daten gehören auch die Angaben, aus denen sich ergibt, dass der öffentlich-rechtliche Entsorgungsträger eine Aufgabe erfüllen darf oder zu erfüllen hat. Die Pflicht zur Abfallbeseitigung bzw. -verwertung besteht - wie bereits zitiert - nur insoweit, als die Abfälle auf dem Gebiet der betreffenden Körperschaft *angefallen* sind (§ 15 Abs. 1 Satz 1 KrW-/AbfG). Das bedeutet, dass der Landkreis nicht solche Abfälle entsorgen muss, die im Gebiet eines anderen öffentlich-rechtlichen Entsorgungsträgers angefallen sind, aber in sein Gebiet verbracht und ihm überlassen wurden, etwa weil er niedrigere Entsorgungsgebühren verlangt. Ein privater Mülltourismus ist also ausgeschlossen (Frenz, KrW-/AbfG, § 15, Rdnr. 7).

Der Landkreis darf daher - wie es auch die Benutzungsordnung vorsieht - prüfen, ob die auf dem Wertstoffhof angelieferten Abfälle in seinem Gebiet *angefallen* sind. Angefallen im Rechtssinne ist Abfall genau dadurch, dass die betreffende Sache Abfall geworden ist, der Besitzer sich ihrer also entledigt, entledigen will oder entledigen muss (§ 3 Abs. 1 Satz 1 KrW-/AbfG). Angefallen ist der Abfall daher nicht erst mit und am Ort seiner Überlassung zur Verwertung bzw. Beseitigung (vgl. Kunick, KrW-/AbfG, § 15, Rdnr. 9). Einzig praktikables Kriterium zur Feststellung des Ortes des Anfalles ist im Normalfall der Wohnsitz bzw. Betriebssitz des Anliefernden. Das bedeutet, dass sich der Landkreis darauf beschränken darf, Abfälle von Einwohner des Kreises anzunehmen.

Erforderlich ist also die Erhebung der Daten, anhand deren die Eigenschaft „Einwohner des Landkreises“ bestimmt werden kann. Die *Speicherung* dieser Daten ist dagegen nicht erforderlich, und zwar aus folgendem Grund: Mit der Annahme der Abfälle und der Barbezahlung der Gebühren haben beide Beteiligten die sich aus dem Benutzungsverhältnis ergebenden Pflichten erfüllt, die Sache ist erledigt.

Die zur Bestimmung der Eigenschaft „Einwohner des Landkreises“ benötigten Daten müssen nicht durch das Verlangen nach Ausfüllen des Vordruckes - welches gleichzeitig den Beginn der Speicherung der Daten darstellt - erhoben werden. Die Erhebung kann vielmehr mittels Einsichtnahme in den Personalausweis (oder in einen anderen Ausweis) erfolgen. Die Beschäftigten der Betreiber-Gesellschaft können von den Anlieferern die Vorlage des Ausweises verlangen (§ 24 Abs. 1 VwVfG, § 12 Abs. 1 SächsABG); Ziffer 1 Abs. 2 Satz 3 der „Ordnung für die Nutzung der Wertstoffhöfe“ des Landkreises, dem zufolge in Zweifelsfällen der Anlieferer die

Herkunft der Abfälle zu belegen hat, ist in diesem Sinne zu verstehen und (als Verwaltungsakt, wie oben dargelegt) gesetzeskonform.

Anders ist die Rechtslage, wenn der Anlieferer eine juristische Person ist. Da in diesem Fall der Landkreis einen schriftlichen Gebührenbescheid erlässt, ist die Speicherung der betreffenden Daten erforderlich, um den Bescheid zuzustellen und den entsprechenden Zahlungsanspruch durchzusetzen.

Meine Rechtsauffassung habe ich sowohl dem Landkreis, als auch dem SMUL mitgeteilt - beide teilen diese: Der Landkreis hat zudem die Betreiber-Gesellschaft angewiesen, die betreffenden Daten nicht mehr zu speichern und andere Quittungsformulare zu benutzen bzw. die Felder der bisherigen unausgefüllt zu lassen.

13 Wissenschaft und Kunst

13.1 Befragung von Hochschulbediensteten zwischen Personaluntersuchung und Forschung

Durch eine Eingabe bin ich auf einen Vorgang hingewiesen worden, der sich an einer Fachhochschule abgespielt und gewisse Ähnlichkeit mit dem oben unter 5.7.2 erörterten Fall hat:

Das erweiterte Rektoratskollegium und das Kuratorium der Fachhochschule hatten eine sog. „Marketingkonzeption“ verabschiedet, zu deren Bestandteilen auch eine „wissenschaftliche Untersuchung zur Arbeitszufriedenheit“ der Hochschulbediensteten gehören sollte, welche die Hochschule mit eigenen personellen Mitteln durchführte, und zwar als Diplomarbeit „Analyse der Arbeitszufriedenheit am Beispiel der Mitarbeiter der FH X“.

Die betreuende Professorin, die zugleich das Amt des „Prorektors für Hochschulmarketing“ bekleidete, hatte zusammen mit der Diplomandin den Fragebogen ausgearbeitet. Dieser war aber dann noch - ein eindeutig wissenschaftsfremder Vorgang! - auf Verlangen des Personalrates der Hochschule geändert worden, woraufhin der Personalrat dann, wie mir die Hochschule durch die Prorektorin mitteilte, dem Fragebogen zugestimmt hatte und auch bei der Vernichtung der Fragebögen am Ende der Durchführung der Untersuchung mitwirken sollte.

Gefragt wurde nach der Zufriedenheit mit den verschiedensten genauer bestimmten sächlichen Arbeitsbedingungen, den Öffnungszeiten der Bibliothek, der Mensa, aber auch nach Stressempfinden, den Quellen, die der Befragte zur Aktualisierung seines Lehrstoffes nutze sowie nach den Führungsfähigkeiten des unmittelbaren Vorgesetzten und der Beurteilung des Betriebsklimas. Am Schluss, auf dem letzten Blatt, wie im Fall von 5.7.2 auch hier wieder, trotz Zusicherung von „Anonymität“, Fragen nach Geschlecht, Alter, Professoren- oder „Mitarbeiter“-Eigenschaft, Fachbereich und Dauer des Dienstverhältnisses an der Hochschule.

Die wissenschaftliche Untersuchung eines Gegenstandes und die Gestaltung einer Diplomarbeit sind bekanntlich nicht Gegenstand von Mitbestimmungsrechten eines Personalrates. Einen Personalrat gehen auch die personenbezogenen Daten, die ein Diplomand bei vom Personalrat Vertretenen erhebt, nichts an.

Vielmehr ist klar: Bestimmend für das Erhebungsprogramm und die ganze Aktion war in erster Linie der von der Spitze der Hochschulverwaltung beschlossene Zweck,

sich ein Bild von der Arbeitszufriedenheit unter den Bediensteten der Hochschule, untergliedert nach Einflussfaktoren, zu verschaffen. Es war, mit anderen Worten, eine von der Dienststellen-Leitung veranstaltete Bedienstetenbefragung zum Dienstbetrieb, die in das Gewand einer wissenschaftlichen Untersuchung (Diplomarbeit) gehüllt war.

Ähnlich wie in dem unter Punkt 5.7.2 erörterten Fall habe ich von einer Beanstandung abgesehen und mich darauf beschränkt, zu verlangen, dass die Daten (Fragebögen) nunmehr in folgender Weise verarbeitet wurden:

- Entgegen der ursprünglichen Absicht durfte die Erstbetreuerin, weil sie als Prorektorin zugleich zur organisatorischen Spitze der Universitätsverwaltung gehörte, nicht mehr die einzelnen Bögen einsehen. Nur der Zweitgutachter sollte die Fragebögen zur Kenntnis nehmen dürfen (zur Beurteilung der Diplomarbeit) und dann unter Verschluss nehmen, bis die Arbeit bestandskräftig benotet sein würde, und danach für die einwandfreie Vernichtung sorgen.

- Die Angaben in den Freitextfeldern - die unter dem Gesichtspunkt des Personenbezuges besonders problematisch sind (Handschrift; Konkretheit des Inhaltes) - durften nur zu ganz abstrakten Auswertungen benutzt werden; dies galt noch mehr für die Vorgesetzten-Bewertungen.

- Die Angaben auf der letzten Seite des Fragebogens durften nicht zur Kenntnis genommen und mussten sofort vernichtet werden.

Um Statistik im Rechtssinne hat es sich hier nicht gehandelt: Insoweit es sich um Verwaltungstätigkeit statt um Wissenschaft handelte, war es eine Befragung von Bediensteten durch den Dienstherrn - wenn auch zu sehr auf subjektive Einschätzungen gerichtet, um eine Organisationsuntersuchung (vgl. § 12 Abs. 3 Satz 1 SächsDSG, vgl. aber auch § 31 Abs. 1 Satz 1 SächsDSG) zu sein. Auch wenn es sich vom untersuchten Gegenstand her um „Massenerscheinungen“ und dementsprechend der Methode nach um Statistik handelt, fallen solche Personalbefragungen durch den Dienstherrn nicht unter das Statistikrecht. Dieses betrifft das informationsrechtliche Außenverhältnis des jeweiligen Trägers öffentlicher Gewalt. Diese Unterscheidung zeigt sich auch an dem gerade erwähnten, etwas anders gelagerten Fall der Organisationsuntersuchungen: Soweit zu deren Durchführung auch Daten Privater verarbeitet werden müssen, die bei den zu untersuchenden Verwaltungsabläufen anfallen, sind sie in § 12 Abs. 3 Satz 1 SächsDSG, gewissermaßen als Annex-Zweck, mit erfasst: Die Datenverarbeitung gilt nicht als Zweckänderung. Wenn zu ihrer Durchführung zusätzlich auch Beschäftigtendaten verarbeitet werden müssen, wie es bei der schlichten Personalbefragung dagegen ausschließlich der Fall ist, ist die maßgebliche Vorschrift, welche die Verarbeitung der personenbezogenen Daten erlaubt, § 31 Abs. 1 SächsDSG.

13.2 Anfragen des Deutschen Krebsforschungszentrums (DKFZ) an die Gesundheitsämter zu Verstorbenen im Rahmen der Deutschen Thorotraststudie

Das DKFZ (Stiftung des öffentlichen Rechts mit Sitz in Heidelberg) führt die sog. Deutsche Thorotrast-Studie durch. Ziel des Forschungsvorhabens ist die Erfassung der Spätfolgen und die Berechnung des Strahlenrisikos durch die Anwendung des Röntgenkontrastmittels „Thorotrast“ in den Jahren 1930 bis 1950. Dazu werden seit 1968 Probanden in regelmäßigen Abständen von mehreren Jahren untersucht. Bei in der Zwischenzeit verstorbenen Probanden ist, wie es heißt, die genaue Kenntnis der Todesursache mitsamt der hierfür ursächlichen Grundleiden sowie der Kenntnis aller wesentlichen Krankheitszustände notwendig.

Diese Daten sollen bei den zuständigen Gesundheitsämtern erhoben werden. Das DKFZ schreibt diese an und bittet darum, einen beigefügten Erhebungsbogen auszufüllen. Es weist schließlich noch darauf hin, dass statt dessen auch eine Kopie der Rückseite des Leichenschauscheines geschickt werden könne.

Zur Zulässigkeit dieser Datenübermittlung habe ich dem DKFZ mitgeteilt, dass die Gesundheitsämter dem DKFZ gemäß § 14 Abs. 5 Satz 3 Nr. 2 und Abs. 6 SächsBestG die Angaben über den Zeitpunkt und den Ort des Todes (§ 14 Abs. 2 Nr. 3 SächsBestG) sowie Angaben über die Todesursache und weitere wesentliche Krankheiten oder Veränderungen zur Zeit des Todes (§ 14 Abs. 2 Nr. 8 SächsBestG) durch Ausfüllen des übersandten Fragebogens übermitteln dürfen.

Aus datenschutzrechtlichen Gründen ist es jedoch nicht zulässig, dass die Gesundheitsämter dem DKFZ statt des ausgefüllten Erhebungsbogens eine Kopie der Rückseite des Leichenschauscheins senden. Denn die Rückseite des Leichenschauscheins - gemeint ist der vertrauliche Teil der Todesbescheinigung - enthält auch Angaben, die das DKFZ für das Forschungsvorhaben nicht benötigt.

Da das DKFZ trotz des entsprechenden Hinweises das Anschreiben nicht geändert hat, habe ich - um für Sachsen eine rechtmäßige Verfahrensweise sicher zu stellen - das SMS darum gebeten, als oberste Landesgesundheitsbehörde die Gesundheitsämter der Landkreise und kreisfreien Städte anzuweisen, nur den ihnen übermittelten Fragebogen auszufüllen, nicht jedoch dem DKFZ eine Kopie des vertraulichen Teils der Todesbescheinigung zur Verfügung zu stellen.

Nach Klärung der Frage, ob eine solche Anweisung zulässig ist (vgl. Beitrag 10.1.3), hat das SMS die Gesundheitsämter im oben genannten Sinne angewiesen.

14 Technischer und organisatorischer Datenschutz

14.1 Datenschutzgerechte Gestaltung von IT-Produkten

Verwaltungshandeln ist mittlerweile ohne IT-Unterstützung nicht mehr denkbar. Da jedoch jede öffentliche Stelle nur nach Recht und Gesetz handeln darf, müsste sie gerade bei der Verarbeitung personenbezogener Daten von vornherein datenschutzrechtliche Überlegungen berücksichtigen. Leider werden bei der Anschaffung neuere IT-Produkte solche Überlegungen in der Regel viel zu spät angestellt. In der Folge müssen dann teure Modifikationen vorgenommen werden, die aber – da sie nicht richtig integriert sind – auch nur unvollkommen funktionieren.

Der hier vorgestellte Katalog* stellt in vier Komplexen beispielhaft Datenschutz- und Datensicherheitsanforderungen sowie in ihrem Zusammenhang zu berücksichtigende Fragestellungen nach wichtigen Rechtsnormen dar und bietet damit eine erste Prüfmöglichkeit für die notwendigen datenschutzrechtlichen und –technischen Forderungen an neu anzuschaffende IT-Produkte.

Im Einzelnen sollte für jede Fragestellung untersucht werden,
- ob sie jeweils relevant für das IT-Produkt ist,
- ob das IT-Produkt zur Erfüllung der Datenschutzanforderung beiträgt, diese erschwert oder den Punkt unberührt lässt,
- ob eine Realisierung gemäß dem Stand der Technik erfolgt,
- die Erfüllung der Anforderungen keinen erheblichen Aufwand erfordert,
- welche Standardeinstellung ausgeliefert wird,
- welche Konfigurationsmöglichkeiten oder andere Freiheitsgrade bestehen und
- wie all dies dokumentiert und nutzeradäquat umgesetzt ist.

Komplex 1 stellt zunächst Anforderungen an die Technikgestaltung. Dies betrifft insbesondere Anforderungen der Datenvermeidung und der Transparenz.
Komplex 2 befasst sich mit den einschlägigen Datenschutzbestimmungen, um die Zulässigkeit der angestrebten Datenverarbeitung überprüfen zu können.

In *Komplex 3* wird untersucht, welche technisch-organisatorischen Maßnahmen zum Schutz der Betroffen unterstützt werden.

Komplex 4 stellt Kriterien vor, um die Umsetzungen der Rechte der Betroffenen (z. B. Benachrichtigung, Auskunft, Transparenzgebote) beurteilen zu können.

* Der Katalog basiert auf einer Ausarbeitung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holsteinischen zu Anforderungen an IT-Produkte beim Datenschutzaudit.

Da das Sächsische Datenschutzgesetz bisher nicht novelliert ist, habe ich die Fundstellen noch nach dem derzeitigen Stand vermerkt. Bei den nicht gekennzeichneten Stellen ist eine gesetzliche Normierung in der Diskussion. Generell ergeben sich allerdings größtenteils diese Anforderungen an IT-Produkte ohnehin aus § 9 SächsDSG.

Komplex 1: Grundsätzliche technische Ausgestaltung

1.1 Datensparsamkeit

Untersuchungsgegenstand:
Wurden die Anforderungen der Datensparsamkeit umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Bestehen Möglichkeiten, dass Betroffene anonym oder pseudonym agieren oder sie wenigstens nachträglich zu anonymisieren oder pseudonymisieren?
- Ist ein vollständiger Verzicht auf personenbezogene Daten möglich? Wenn nein, warum nicht?
- Welche (Kombinationen von) personenbezogenen Daten sind wirklich erforderlich? Wovon hängt dies ab?
- Wird auf das Anlegen von temporären Datenbeständen (z. B. unnötige Protokollierung, Parallel- und Zwischenspeicherung) verzichtet bzw. sind diese Datenbestände wirksam gegen unbefugten Zugriff gesichert?

1.2 Frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren, wenn Daten noch erforderlich, aber Personenbezug verzichtbar

Untersuchungsgegenstand:
Gibt es Methoden für frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren personenbezogener Daten?

In diesem Zusammenhang wichtige Fragestellungen:
- Wie werden Löschen, Anonymisierung und Pseudonymisierung umgesetzt (automatisch / in welchen Abhängigkeiten)?
- Wird die Pseudonymisierung/Anonymisierung zum frühestmöglichen Zeitpunkt vorgenommen?
- Wovon hängt der Zeitpunkt der Anonymisierung oder Pseudonymisierung ab?
- Sind geeignete Maßnahmen ergriffen worden, um die Zuordnungsfunktion bei einer Pseudonymisierung zu sichern? Ist die Zuordnungsfunktion geeignet, oder besteht die Gefahr, mit nur wenig Zusatzwissen einzelne Daten depseudonymisieren zu können (etwa bei einer Pseudonymisierung durch Vertauschen von Namensbuchstaben etc.)?
- Zu technischen Fragen des Löschens siehe auch Abschnitt 4.3.2.

1.3 Transparenz und Verfahrensbeschreibung

Untersuchungsgegenstand:
Liegt eine aussagekräftige und aktuelle Verfahrensbeschreibung vor?

In diesem Zusammenhang wichtige Fragestellungen:
- Ist die Transparenz der Datenverarbeitung (Datenflüsse, Speicherungsorte, Übermittlungswege, Zugriffsmöglichkeiten) gegenüber Anwendern (Systemadministration und Nutzer) sowie Betroffenen gewährleistet?
- Sind die Vorkenntnisse, die zum Verstehen der Produktbeschreibung erforderlich sind (Sprache, Know-how), angemessen?
- Inwieweit ist ein leichter Zugriff auf die Produktbeschreibung und eine geeignete Auswertbarkeit gewährleistet (Inhaltsverzeichnis, Index, Volltextsuche)?
- Wird die Aktualität sichergestellt?
- Wird das zu Grunde liegende Konzept ausreichend erläutert?
- Besteht eine Einsichtsmöglichkeit in den Quelltext/das Gerät? Für wen (auch für Außenstehende, oder nur für den Auftraggeber)?

1.4 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

Komplex 2: Zulässigkeit der Datenverarbeitung

Die Frage der Zulässigkeit einer Datenverarbeitung beurteilt sich danach, welches Recht auf die Stellen anzuwenden ist, für die das Produkt vorgesehen ist. Bei öffentlichen Stellen im Freistaat Sachsen gilt als Auffanggesetz das Sächsische Datenschutzgesetz, für die Verarbeitung von Sozialdaten das Sozialgesetzbuch. Daneben sind spezielle bereichsspezifische Regelungen zu beachten. Beispielhaft (aber nicht abschließend) seien hier genannt:

- Bundesdatenschutzgesetz für öffentliche Wettbewerbsunternehmen
- Bundesstatistikgesetz,
- Personenstandsgesetz,
- Pass- und Personalausweisgesetz,
- Strafprozessordnung,
- §§ 185 ff. Strafvollzugsgesetz,
- Straßenverkehrsgesetz,
- Teledienstedatenschutzgesetz,
- Telekommunikationsgesetz (nebst TDSV),

• Sächsisches Krankenhausgesetz,
• Sächsisches Meldegesetz,
• Sächsisches Statistikgesetz,
• Sächsisches Polizeigesetz.

2.1 Allgemeine Voraussetzung der Zulässigkeit (z. B. §§ 11 f. SächsDSG, §§ 4, 13 ff. BDSG, §§ 67 a ff. SGB X)

2.1.1 Vorliegen der gesetzlichen Voraussetzungen

Untersuchungsgegenstand:
Sind die Zulässigkeitsvoraussetzungen für die Datenverarbeitung erfüllt?

In diesem Zusammenhang wichtige Fragestellungen:
- Gibt es einen abgeschlossenen Katalog von Daten, die verarbeitet werden sollen? Wenn ja: Wird die Erhebung und Speicherung auf diese Daten beschränkt (keine Freitextfelder!)? Wenn nein: Beschränken sich die Daten auf das Erforderliche?
- Erfolgt eine Verarbeitung besonders sensibler Daten (§ 67 Abs. 12 SGB X, § 3 Abs. 9 BDSG), die die Zulässigkeit einschränken könnte (§§ 67 a Abs. 1 Satz 2, 67 b Abs. 1 Satz 2 SGB X, §§ 13 Abs. 2, 14 Abs. 5 BDSG)? Wie wird eine solche Einschränkung umgesetzt?
- Unterliegen die Daten zusätzlichen besonderen materiellen Anforderungen (z. B. berufliche Schweigepflicht, vgl. § 203 StGB) und wie werden diese bei der weiteren Verarbeitung berücksichtigt?
- Inwieweit sind Pseudonymisierungs- bzw. Anonymisierungsgebote (z. B. § 30 Abs. 3 SächsDSG, § 40 Abs. 2 BDSG) zu beachten?

2.1.2 Erfolgt eine Datenverarbeitung im Auftrag oder eine Systembetreuung durch Externe (§ 7 SächsDSG, § 80 SGB X, vgl. § 11 BDSG)?

Untersuchungsgegenstand:
Sind die normativen und formalen Voraussetzungen für eine Datenverarbeitung im Auftrag gegeben?

In diesem Zusammenhang wichtige Fragestellungen:
- Wie wird die Kontrolle des Auftragnehmers durch den Auftraggeber unterstützt?
- Wie wird das Recht des Auftraggebers, dem Auftragnehmer Weisungen zu erteilen, unterstützt?
- Wie sind die technischen und organisatorischen Maßnahmen umgesetzt, die die Bindung des Auftragnehmers an die Weisungen der Daten verarbeitenden Stelle sicherstellen?

2.1.3 Einwilligung (§ 4 SächsDSG, § 4 a BDSG, § 67 b Abs. 2, 3 SGB X)

Untersuchungsgegenstand:
Wird die Wirksamkeit einer Einwilligung unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:
- Enthält eine Einwilligungsformulierung hinreichend bestimmte Angaben zu verarbeitenden Stellen/Empfängern, Art der Verarbeitung, verarbeitete Daten und Zweckbestimmung, insbesondere bei besonderen Arten personenbezogener Daten (§ 4 a BDSG)?
- Sind die Formerfordernisse nach § 4 Abs. 3 SächsDSG, § 4 a Abs. 1 Sätze 3 und 4 BDSG bzw. § 67 b Abs. 2 SGB X gewahrt?
- Ist die ausreichende Informierung des Einwilligenden gewährleistet (§ 4 Abs. 2 SächsDSG)?
- Gibt es eine Unterstützung durch das IT-System (dabei ist zu berücksichtigen, dass i. d. R. die Einwilligung vor der ersten Speicherung vorliegen muss)?

2.2 Zulässigkeit in den einzelnen Phasen der Datenverarbeitung

2.2.1 Erhebung grundsätzlich nur beim Betroffenen, nur ausnahmsweise bei Dritten oder verdeckt (§ 11 SächsDSG, § 13 BDSG, § 67 a Abs. 1 SGB X)

Untersuchungsgegenstand:
Werden gesetzliche Regelungen bei der Erhebung von Daten umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Erfolgt eine Unterrichtung bzw. Aufklärung des Betroffenen (Artikel 10 EG-Richtlinie, § 19 a BDSG, § 67 a Abs. 3, 5 SGB X) bzw. des Dritten (§ 67 a Abs. 4 SGB X)? In welcher Form unterstützt das Verfahren dies?
- Erfolgt eine verdeckte Erhebung von Daten ohne Kenntnis der Betroffene (z. B. bei biometrischen Verfahren)?

2.2.2 Speicherung bzw. weitere Verarbeitung (§§ 12 bis 16 SächsDSG, §§ 14 bis 17 BDSG, § 67 b SGB X)

2.2.2.1 Sicherstellung der Zweckbindung

Untersuchungsgegenstand:
Wie wird sichergestellt, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung verarbeitet werden bzw. dass eine Zweckänderung nur innerhalb des gesetzlichen Rahmens erfolgt?

In diesem Zusammenhang wichtige Fragestellungen:
- Wie wird der Zweck dokumentiert, für den die personenbezogenen Daten erhoben wurden?
- Siehe auch Abschnitt 2.2.3 und 2.2.4.

2.2.2.2 Erleichterung der Umsetzung der Trennung nach § 12 Abs. 5 SächsDSG bzw. § 15 Abs. 5 BDSG

Untersuchungsgegenstand:
Wird die Möglichkeit der Trennung unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:
- Wie wird die Trennung technisch umgesetzt?
- Gibt es Verfahren zur automatisierten Pseudo-/Anonymisierung (siehe auch Abschnitt 1.2)?
- Werden schutzwürdige Belange, die einer Weitergabe von untrennbar verbundenen Daten entgegenstehen, geprüft?

2.2.3 Übermittlung (§§ 13 bis 16 SächsDSG, §§ 4 b, 15 f. BDSG, §§ 67 d bis 78 SGB X)

Untersuchungsgegenstand:
Werden die Vorschriften zur Übermittlung umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Erfolgt eine Protokollierung? Sind die datenschutzrechtlichen Vorschriften für die Protokolldaten erfüllt?
- Erfolgt ein Hinweis bzw. eine Verpflichtung auf die Zweckbindung der erhaltenen Daten (vgl. § 13 Abs. 3 und § 15 Abs. 4 SächsDSG, § 4 b Abs. 6 BDSG, § 78 Abs. 2 SGB X)?
- Kann eine Zweckbindung technisch überwacht werden und können Daten, die nicht übermittelt werden dürfen, von der Übermittlung ausgeschlossen werden?
- Wird die Richtigkeit der Empfängeradresse verifiziert? Gibt es Filter für mögliche Adressaten bzw. Adressatenkreise, an die keinesfalls eine Übermittlung erfolgen darf (z. B. durch Sperrung von Empfängeradressen außerhalb des Hauses in einem E-Mail- System)?
- Filter für ausgehende Informationen: Gibt es Mechanismen, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch rückstandslose Beseitigung von personenbezogenen (Zusatz-)Daten bei möglicher Herausgabe (z. B. detaillierte Informationen über den Autor in Word-Dokumenten, automatisierte Weitergabe von Zusatzinformationen bei HTTP-Kommunikation durch Voreinstellungen im Webbrowser)?
- Gibt es Maßnahmen zur Steigerung der Sensibilität der Verarbeiter, um diese vor

unbedachten/unerlaubten Übermittlungen zu schützen?
- Sind bei der Übermittlung an Dritte Maßnahmen vorgesehen, um Daten zu anonymisieren oder pseudonymisieren (siehe auch Abschnitt 1.2)?
- Wird der Betroffene bei der Übermittlung besonderer Arten von personenbezogenen Daten unterrichtet (Art. 11 EG-Richtlinie, § 16 Abs. 3 BDSG)?

2.2.4 Zweckbindung (§ 12 Abs. 1 SächsDSG, § 14 Abs. 1 BDSG, § 67 c Abs. 1 SGB X) und Zweckänderung (§ 12 Abs. 2 SächsDSG, § 14 Abs. 2 BDSG, § 67 c Abs. 2 SGB X)

Untersuchungsgegenstand:
Wird die Beachtung einer Zweckbindung unterstützt bzw. werden evtl. vorgesehene und zugelassene Zweckänderungen auf das erforderliche Maß begrenzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Gibt es eine revisionssichere Protokollierung der Verarbeitung, um Zweckänderungen nachweisen zu können?
- Wird die Zweckbindung dadurch garantiert, dass personenbezogene Daten vermieden werden oder ihre Verkettbarkeit und damit eine zweckändernde Nutzung erschwert oder verhindert wird?
- Gibt es eine Kennzeichnung von Datensätzen mit entsprechenden Zwecken sowie Zugriffsrechte, die andere Auswertungsmethoden oder eine Übermittlung einschränken?

2.2.5 Löschung nach Wegfall der Erfordernisse (§ 19 SächsDSG, § 20 Abs. 2 BDSG)

Untersuchungsgegenstand:
Wird sichergestellt, dass Daten nach Wegfall der Erfordernis gelöscht werden oder ein Personenbezug abgetrennt wird?

In diesem Zusammenhang wichtige Fragestellungen:
- Sind Fristen (Löschungsfristen, Wiedervorlagefristen) zu beachten? Wie wird deren Beachtung sichergestellt?
- Siehe auch Abschnitt 4.3.2 zu Löschung.
- Siehe auch Abschnitt 4.3.2 zur Anonymisierung/Pseudonymisierung.

2.3 Werden zusätzlich die speziellen materiell-rechtlichen Anforderungen beim Einsatz besonderer technischer Verfahren beachtet?

Untersuchungsgegenstand:
Wie wird die Beachtung zusätzlicher spezieller materiell-rechtlicher Anforderungen beim Einsatz besonderer technischer Verfahren sichergestellt?

In diesem Zusammenhang wichtige Fragestellungen:
Sind besondere Anforderungen einschlägig, z. B.
- gemeinsame und Abrufverfahren (§ 8 SächsDSG, §§ 6 Abs. 2, 10 BDSG);
- Zulässigkeit von mobilen personenbezogenen Datenverarbeitungssystemen (§ 6 c BDSG);
- automatisierte Einzelentscheidungen (Art. 15 EG-Richtlinie, § 6 a BDSG, § 67 b Abs. 4 SGB X);
- Videoüberwachung und -aufzeichnung (z. B. § 6 b BDSG).

Siehe auch Abschnitte 3.2.4.1 (mobile Datenverarbeitungssysteme), 3.2.4.2 (Videoüberwachung), 3.2.4.3 (automatisierte Einzelentscheidungen).

2.4 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen

3.1 Allgemeine Pflichten

3.1.1 § 9 SächsDSG bzw. § 9 BDSG oder § 78 a SGB X jeweils mit Anhang

3.1.1.1 Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren (§ 9 Abs. 2 Nr. 1 SächsDSG, Anlage zu § 9 Satz 1 Nr. 1 BDSG)

Untersuchungsgegenstand:
Wird durch geeignete Maßnahmen Unbefugten der Zutritt zu Datenverarbeitungsanlagen verwehrt?

In diesem Zusammenhang wichtige Fragestellungen:
- Unterliegen die Zugangskontrollmechanismen ihrerseits datenschutzrechtlichen Regelungen (insbesondere bei Chipkarten, Token, biometrische Verfahren durch die Verarbeitung von Sekundärdaten)?

3.1.1.2 Maßnahmen, um die Nutzung von Datenverarbeitungssystemen durch Unbefugte zu verhindern (§ 9 Abs. 2 Nr. 2 und 3, Anlage zu § 9 Satz 1 Nr. 2 BDSG)

Untersuchungsgegenstand:
Wird durch geeignete Maßnahmen Unbefugten die Nutzung von Datenverarbeitungssystemen verwehrt?

In diesem Zusammenhang wichtige Fragestellungen:
- Ist die Vergabe von Zugangsrechten adäquat und revisionssicher?
- Ist ein Passwortschutz sicher umgesetzt (z. B. durch Einmalpasswörter (z. B. Challenge-Response), zeitabhängige Passwörter, Schutz gegen Ausspähung oder Erraten, Länge, Vergabe/Wechsel durch Nutzer selbst, automatisierte Beschränkung des Gültigkeitszeitraumes, Einschränkung der Wiederverwendbarkeit, Sperrmöglichkeit bei Fehlversuchen)?
- Unterliegen die Zugangskontrollmechanismen ihrerseits datenschutzrechtlichen Regelungen (insbesondere bei Chipkarten, Token, biometrischen Verfahren durch die Verarbeitung von Sekundärdaten)?
- Werden Firewalls oder Intrusion Detection & Response Systems wirkungsvoll gegen unbefugte Zugriffe eingesetzt?
- Sind Maßnahmen zum Löschen/Sperren/Zerstören der Daten oder Geräte bei unbefugtem Öffnen/Eingriffen (z. B. bei Chipkarten) vorgesehen?
- Werden Mechanismen eingesetzt, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch die Reduktion des Einsichtwinkels bei Monitoren oder Vermeidung von Abstrahlung bei Monitoren, (Funk-)Tastatur, Maus usw. (Tempest)?
- Wurden Maßnahmen ergriffen, um die Sensibilität der Verarbeiter zu steigern (z. B. automatisierte Warnhinweise etc.)?

3.1.1.3 Maßnahmen, um den unbefugten Zugriff auf Daten zu verhindern (§ 9 Abs. 2 Nr. 4 und 5 SächsDSG, Anlage zu § 9 Satz 1 Nr. 3 BDSG)

Untersuchungsgegenstand:
Wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können?

In diesem Zusammenhang wichtige Fragestellungen:
- Werden Systemadministrationsebene und Anwendungsebene ausreichend getrennt?
- Können und werden ausreichend detaillierte Zugriffsrechte vergeben? Sind ggf. Rollenkonzepte (etwa besondere Berechtigungen von Systemadministration und Kontrollrollen wie Leitung, Datenschutzbeauftragtem oder Revision) berücksichtigt?

- Sind neben nutzerbezogenen Rollenkonzepten auch objektbezogene Rechtevergaben möglich?
- Wie wird dokumentiert, welchen Personen welche Nutzungsrechte an welchen informationstechnischen Geräten, Programmen und automatisierten Dateien für welche Zeiträume gewährt wurden (z. B. durch die Bereitstellung von Werkzeugen zur Dokumentation der Nutzungsrechtevergabe und Administration)?
- Wie wird dokumentiert, welche Personen für welche Zeiträume befugt sind, Änderungen an der Funktionsweise von informationstechnischen Geräten, an den Programmen, an der Speicherorganisation der automatisierten Dateien und den Nutzungsrechten vorzunehmen?
- Wird die rückstandslose Beseitigung von personenbezogenen Daten von Datenträgern/ Geräte(teile)n (z. B. Festplatten, Schreibbänder, Faxbauteile), die an Dritte weitergegeben werden können, gewährleistet oder unterstützt?
- Wurden Maßnahmen ergriffen, um die Sensibilität der Verarbeiter zu steigern (z. B. automatisierte Warnhinweise etc.)?
- Zu technischen Fragen des Löschens siehe auch Abschnitt 4.3.2.

3.1.1.4 Maßnahmen, um eine sichere Übermittlung von Daten zu gewährleisten (§ 9 Abs. 2 Nr. 9 SächsDSG, Anlage zu § 9 Satz 1 Nr. 4 BDSG)

Untersuchungsgegenstand:
Wird durch geeignete Maßnahmen gewährleistet, dass Daten sicher übermittelt werden, und kann festgestellt werden, an wen die Daten übermittelt werden sollen?

In diesem Zusammenhang wichtige Fragestellungen:
- Werden anerkannte und offen gelegte Verschlüsselungsverfahren eingesetzt?
- Sind Schlüsselgenerierung und Schlüsselmanagement adäquat realisiert?
- Wurden ausreichende Schlüssellängen eingesetzt?
- Wurden Maßnahmen vorgesehen, falls sich die verwendeten Verfahren oder Schlüssellängen als unzulänglich herausstellen (z. B. Wechsel des Verfahrens oder seiner Komponenten, umschlüsseln etc.)
- Sind Maßnahmen zum Löschen/Sperren/Zerstören der Daten oder Geräte bei unbefugtem Öffnen/Eingriffen (z. B. bei Chipkarten) vorgesehen?
- Werden geeignete Mechanismen eingesetzt, um eine absichtliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. Kennzeichnung der Daten für Sensibilisierung oder Nachverfolgbarkeit (z. B. steganographische Markierung)?
- Filter für ausgehende Informationen: Gibt es Mechanismen, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z. B. durch rückstandslose Beseitigung von personenbezogenen (Zusatz-)Daten bei möglicher Herausgabe (z. B. detaillierte Informationen über den Autor in Word-Dokumenten, automatisierte Weitergabe von Zusatzinformationen

bei HTTP-Kommunikation durch Voreinstellungen im Webbrowser)? (siehe auch Abschnitt 2.2.3)
- Zu technischen Fragen des Löschens siehe auch Abschnitt 4.3.2.
- Zu technischen Fragen der Sicherung der Übermittlung siehe auch Abschnitt 2.2.3.

3.1.1.5 Maßnahmen, um eine nachträgliche Kontrolle der Datenerhebung, -verarbeitung und -nutzung zu gewährleisten (§ 9 Abs. 2 Nr. 6 und 7 SächsDSG, Anlage zu § 9 Satz 1 Nr. 5 BDSG)

Untersuchungsgegenstand:
Werden Daten und Datenverarbeitungsvorgänge (u. a. Eingabe, Veränderung, Weitergabe, Löschung etc.) protokolliert, wenn dies rechtlich erforderlich ist?

In diesem Zusammenhang wichtige Fragestellungen:
- Wie lassen sich die Protokolldaten auswerten? Gibt es automatisierte Auswertungsroutinen? Nach welchen Kriterien?
- Wurden die datenschutzrechtlichen Anforderungen für die Verarbeitung der Protokolldaten geprüft? Sind ggf. spezielle Regelungen zu beachten (z. B. bei Aufzeichnung von Telefonaten, Videoüberwachung)?
- Wann werden die Protokolldaten gelöscht (zeitgesteuert statt speicherplatzgesteuert)?
- Welche Maßnahmen wurden zum Schutz überlaufender Protokolldateien unternommen?
- Zu technischen Fragen des Löschens siehe auch Abschnitt 4.3.2.

3.1.1.6 Maßnahmen zur Sicherung der Einhaltung von Weisungen des Auftraggebers (§ 9 Abs. 2 Nr. 8 SächsDSG, Anlage zu § 9 Satz 1 Nr. 6 BDSG)

Untersuchungsgegenstand:
Wie werden datenschutzrechtliche Forderungen bei der Auftragsdatenverarbeitung realisiert?

In diesem Zusammenhang wichtige Fragestellungen:
- siehe Abschnitt 2.1.2

3.1.1.7 Maßnahmen zur Gewährleistung der Verfügbarkeit von Daten (Art. 17 Abs. 1 EG-Richtlinie, Anlage zu § 9 Satz 1 Nr. 7 BDSG)

Untersuchungsgegenstand:
Sind die Daten gegen zufällige Zerstörung oder Verlust geschützt?

In diesem Zusammenhang wichtige Fragestellungen:
- Werden ausreichende Maßnahmen zur Sicherstellung der Verfügbarkeit (z. B.

Sicherheitskopien in erforderlichem Umfang mit geeigneter Lagerung, ggf. unterbrechungsfreie Stromversorgung, Zugangs, Zutritts- und Zugriffsrechte auch für Stellvertreter) ergriffen?

3.1.1.8 Maßnahmen zur Sicherung der Trennungsmöglichkeit (Anlage zu § 9 Satz 1 Nr. 8 BDSG)

Untersuchungsgegenstand:
Existieren Möglichkeiten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?

In diesem Zusammenhang wichtige Fragestellungen:

- siehe Abschnitt 2.2.2.2

3.1.1.9 Weitere technische und organisatorische Maßnahmen

Untersuchungsgegenstand:
Sind durch die bisher untersuchten oder weitere Mechanismen die Sicherheitsziele wie Vertraulichkeit und Integrität im notwendigen Umfang gewährleistet?

In diesem Zusammenhang wichtige Fragestellungen:
- Kommen Maßnahmen zur Sicherstellung der Integrität von Daten und Programmen (z. B. Virenschutz, Prüfsummen, digitale Signatur, Kapselung von Programm(teil)en, Deaktivieren von möglicherweise schädigenden Funktionen (z. B. ActiveX)) zur Anwendung und sind sie adäquat umgesetzt?
- Wird die Vertraulichkeit von Datenbeständen bei Speicherung und Übermittlung ausreichend sichergestellt?
- Zu technischen Fragen der Verschlüsselung siehe auch Abschnitt 3.1.1.4.

3.1.2 Erleichterung bei der Erstellung des Verfahrensverzeichnisses (§ 10 SächsDSG, Meldepflicht §§ 4 d, 4 e BDSG)

Untersuchungsgegenstand:
Ist die automatisierte Erstellung der Meldung möglich?

In diesem Zusammenhang wichtige Fragestellungen:
- Werden Werkzeuge (Formulare, interaktive Tools) zur Erstellung von individuell zugeschnittenen Dokumentationen und Konzepten bereitgestellt?
- Werden prototypische Dokumentationen und Konzepte bereitgestellt?

3.1.3 Sonstige Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten (§§ 4 e, 4 f BDSG, vgl. § 81 Abs. 4 SGB X)

Untersuchungsgegenstand:
Wird der behördliche Datenschutzbeauftragter bei der Wahrnehmung seiner Pflichten unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:
- Werden Test und Freigabe unterstützt (z. B. durch die Mitlieferung von relevanten Testdaten, Hinweise zu Prüfungen, Bereitstellung von Formularen etc.)?
- Wird die datenschutzrechtliche Kontrolle des Verfahrens durch geeignete Maßnahmen (z. B. Bereitstellung adäquater Dokumentation, Hilfsmittel bei der Auswertung von Protokolldaten, etc.) unterstützt?

3.2 Spezifische Pflichten

3.2.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens (§ 3 a Satz 2 BDSG, § 67 Abs. 8 a SGB X)

Untersuchungsgegenstand:
Findet eine gebotene oder geforderte Pseudonymisierung statt?

In diesem Zusammenhang wichtige Fragestellungen:
- Ist eine Pseudonymisierung von Daten für Zwecke der Forschung (§ 30 Abs. 3 SächsDSG, § 40 Abs. 2 BDSG) geboten?
- Siehe auch Abschnitt 1.2.

3.2.2 Technische Umsetzung von Transparenz- und Beteiligungsgeboten für die Betroffenen bei besonderem Technikeinsatz

3.2.2.1 bei Chipkarten (§ 6 c BDSG)

Untersuchungsgegenstand:
Werden die besonderen Vorschriften zur Information der Betroffenen bei der Verwendung personenbezogener Speicher- und Verarbeitungsmedien umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Sind die Verarbeitungsgeräte so gestaltet, dass Verarbeitungsvorgänge sowie Art und Umfang personenbezogener Daten jederzeit erkennbar sind?

3.2.2.2 bei Videoüberwachung (§ 6 b Abs. 2, 4 BDSG)

Untersuchungsgegenstand:
Werden die gesetzlichen Vorgaben umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Wird die Tatsache einer Aufzeichnung den Betroffenen erkennbar gemacht?
- Wird die Einhaltung der gesetzlichen Löschungsfristen für Aufzeichnungen sichergestellt?
- Werden geeignete Sicherungsmaßnahmen zum Schutz der Aufzeichnungen ergriffen? (siehe auch Abschnitt 3.1.1.2 bis 4)

3.2.2.3 bei automatisierten Einzelentscheidungen (§ 6 a Abs. 2 Nr. 2, Abs. 3 BDSG)

Untersuchungsgegenstand:
Werden die gesetzlichen Vorgaben umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Gibt es Rechtsgrundlagen für automatisierte Einzelentscheidungen, die sich ausschließlich auf die Ergebnisse automatisierter Verfahren stützen?
- Auf welche Weise können Betroffene ihre besonderen persönlichen Interessen geltend machen?

3.3 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

Komplex 4: Rechte der Betroffenen (§§ 17 bis 21 SächsDSG, §§ 6, 19 bis 21 BDSG)

4.1 Aufklärung und Benachrichtigung (Art. 10, 11 EG-Richtlinie, § 19 a BDSG)

Untersuchungsgegenstand:
Inwieweit werden Aufklärung und Benachrichtigung von Betroffenen geleistet oder unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:
- Gibt es besondere Maßnahmen, um die Transparenz der Datenverarbeitung für den Betroffenen sicherzustellen?
- Können einzelne Datenverarbeitungsschritte (z. B. Übermittlungen in Form eines "Einzelnutzungsnachweises") dem Betroffenen verdeutlicht werden?

4.2 Auskunft (§ 17 SächsDSG, § 19 BDSG, §§ 25, 83 SGB X)

Untersuchungsgegenstand:
Wird eine Auskunft vom Verfahren angemessen unterstützt?

In diesem Zusammenhang wichtige Fragestellungen:
- Gibt es eine automatisierte Auskunftsbearbeitung durch das Verfahren, so dass Hemmschwellen beim Betroffenen und zeitliche Verzögerungen gering sind?
- Sind alle Daten für die Auskunft leicht auffindbar; gibt es Hilfsmittel dazu?
- Werden untrennbare Verknüpfung mit personenbezogenen Daten anderer Betroffener vermieden?
- Gibt es eine Protokollierung bei der Übermittlung personenbezogener Daten?
- In welcher Weise erfolgt eine Authentisierung des Auskunftsberechtigten?
- Erfasst die Auskunftsmöglichkeit den gesamten Auskunftsanspruch [gespeicherte Daten, Zweck und Rechtsgrundlage, Herkunft und Empfängerkreis (Auftragnehmer, Datenveränderung), Funktionsweise (logischer Aufbau)] von automatisierten Verfahren?

4.3 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung (§§ 18 bis 20 SächsDSG, § 20 BDSG, § 84 SGB X)

4.3.1 Berichtigung

Untersuchungsgegenstand:
In welcher Form leistet oder unterstützt das Verfahren die Berichtigung von Daten?

In diesem Zusammenhang wichtige Fragestellungen:
- Gibt es eine automatisierte Berichtigungsbearbeitung?
- Wie wird eine korrekte und unverzügliche Umsetzung der Berichtigung gesichert?
- Wie wird eine automatisierte Berichtigung qualitätsgesichert?
- Wie werden Berichtigungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

4.3.2 Vollständige Löschung

Untersuchungsgegenstand:
Wie ist die Löschung realisiert?

In diesem Zusammenhang wichtige Fragestellungen:
- Wird vollständig und irreversibel gelöscht?
- Geschieht dies durch physikalisches Löschen auf allen Medien (ohne zusätzliche Kopien, etwa innerhalb einer Funktion zum Rückgängigmachen von Löschungen)?

- Ist eine Selektivität des Löschens möglich (z.B. problematisch bei CD-ROM)?
- Wird durch Überschreiben gelöscht? Ist die Umsetzung (z. B. Anzahl der Überschreibvorgänge) adäquat?
- Wie ist die Umsetzung der Löschung auf Backup-Medien realisiert?
- Wie werden Löschungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?
- Wie werden Lösch- und Prüffristen (Wiedervorlage) realisiert oder unterstützt?

4.3.3 Sperrung

Untersuchungsgegenstand:
Wie wird eine Sperrung von Daten umgesetzt?

In diesem Zusammenhang wichtige Fragestellungen:
- Gibt es eine Möglichkeit, die Datensätze so zu kennzeichnen, dass sie für die normale Verarbeitung nicht zur Verfügung stehen, aber gleichwohl gespeichert bleiben?
- Wie wird dies gewährleistet?
- Wie wird die Sperrung und ggf. Aufhebung der Sperre protokolliert (Zeitpunkt, Auftraggeber, etc.)? (siehe auch Abschnitt 3.1.1.5)

4.3.4 Einwand bzw. Widerspruch gegen die Verarbeitung (Art. 14 EG-Richtlinie, § 20 Abs. 5 BDSG, § 84 Abs. 1 a SGB X)

Untersuchungsgegenstand:
Gibt es eine technische Unterstützung des Widerspruchsrechtes?

In diesem Zusammenhang wichtige Fragestellungen:
- Wie werden Widersprüche an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

4.4 Sonstige Anforderungen

Welche sonstigen Anforderungen sind in diesem Komplex zu beachten, die sich aus den (ggf. spezielleren) Rechtsvorschriften zu Datenschutz und Datensicherheit ergeben?

14.2 Elektronische Signaturen (digitale Signaturen)

Der wichtigste Anwendungsbereich kryptographischer Verfahren ist neben der Verschlüsselung die elektronische oder digitale Signatur (vgl. 8/14.3). Eine digitale

Signatur kann die handschriftliche Unterschrift unter einer E-Mail, unter einem Antrag bei der Behörde oder unter einem Vertragsentwurf ersetzen. Sie wird zum Signieren von Dokumenten genutzt und kann Warenbestellungen oder Bezahlvorgänge mit elektronischem Geld absichern.

Mit dem Signaturgesetz* (SigG), dem Gesetz zur Anpassung der Formvorschriften des Privatrechts und der Signaturverordnung sind in Deutschland inzwischen die ersten rechtlichen Voraussetzungen und technischen Anforderungen geschaffen und an die europäische Rechtsentwicklung angepasst worden, unter denen eine Gleichstellung der Schriftform mit der elektronischen Form geregelt ist.

Die bisher im Rechts- und Geschäftsverkehr bekannten digitalen Signaturen sind im technologieoffenen Begriff der „elektronischen Signatur" integriert. Nach dem Signaturgesetz wird zwischen elektronischen Signaturen, fortgeschrittenen und qualifizierten elektronischen Signaturen unterschieden.
Einfache elektronische Signaturen sind elektronische Daten, die elektronischen Dokumenten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung des Unterzeichners dienen. Als elektronische Signatur gilt bereits das Anfügen eines Namens oder einer eingescannten Unterschrift unter ein elektronisches Dokument. Allerdings ist damit keine Sicherheit gegeben, weil diese „Unterschrift" beliebig oft kopiert und unter andere Dokumente gesetzt werden kann. Eine fortgeschrittene elektronische Signatur (z. B. bei der Nutzung von PGP) kann zusätzlich die Identität des Unterzeichners bestätigen und prüfen, ob die Daten nachträglich verändert wurden.
Die gesetzlichen Anforderungen an eine Signatur erfüllt jedoch nur die qualifizierte elektronische Signatur. Sie beruht gegenüber der fortgeschrittenen elektronischen Signatur zusätzlich auf einem gültigen qualifizierten Zertifikat und muss gesetzlich festgelegten Sicherheitsanforderungen genügen. Sie ist der handschriftlichen Unterschrift gleichgestellt und als Beweismittel zulässig. Die Rahmenbedingungen für ihren Einsatz und die Pflichten der Zertifizierungsdiensteanbieter regelt das Signaturgesetz. Beim Einsatz qualifizierter elektronischer Signaturen für öffentlich-rechtliche Verwaltungstätigkeit können Rechtsvorschriften zusätzliche Anforderungen anordnen.

Im Allgemeinen ist freigestellt, welche Art der elektronischen Signatur verwendet wird, soweit nicht durch Rechtsvorschriften konkrete Forderungen vorgeschrieben sind.

* Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001, BGBl. I, S. 876.

Kryptographisch basieren fortgeschrittene und qualifizierte elektronische Signaturen auf asymmetrischen Verschlüsselungsverfahren (vgl. TB 6/14.2) und Hash-Funktionen*. Beim Signieren wird ein Hashwert wie ein „digitaler Fingerabdruck“ für die elektronischen Daten (z. B. Dokument) berechnet. Dieser wird mit dem Signaturschlüssel (privater Schlüssel des Unterzeichners) verschlüsselt und den elektronischen Daten hinzugefügt. Eine Hash-Funktion berechnet für ein Dokument immer den gleichen Hashwert (Prüfsumme), solange der Inhalt des Dokuments nicht verändert wird. Beim Prüfen wird die Signatur (verschlüsselter Hashwert) mit dem Signaturprüfschlüssel (öffentlicher Schlüssel des Unterzeichners) entschlüsselt. Zugleich wird ein aktueller Hashwert für die elektronischen Daten berechnet, der mit dem entschlüsselten Hashwert verglichen wird. Bei Gleichheit wird bestätigt, dass die elektronischen Daten nachträglich nicht verändert wurden und dass die signierten Daten vom Unterzeicher stammen. Bei Ungleichheit wird die Signatur als ungültig abgelehnt.
Zur Sicherheit des Signatur- bzw. Prüfverfahrens ist der Signaturprüfschlüssel durch eine vertrauenswürdige Stelle (Zertifizierungsdiensteanbieter) mit einem elektronischen Zertifikat einer Person zuzuordnen. Außerdem ist der Signaturschlüssel, der z. B. auf einer Chipkarte gespeichert ist, geheim zu halten und vor unbefugter Nutzung zu schützen. Die Anwendungskomponenten (z. B. Spezialsoftware), die zur Erzeugung bzw. Prüfung elektronischer Signaturen eingesetzt werden, dürfen nur auf vertrauenswürdigen IT-Systemen betrieben werden. Geeignete Kryptoalgorithmen werden im Bundesanzeiger mindestens für die kommenden sechs Jahre veröffentlicht, gegebenenfalls aktualisiert und ergänzt.

14.3 Sicherheitsprobleme bei der E-Mail-Verschlüsselung in lokalen Netzen

Im Februar 2002 informierte ”heise online” (www.heise.de) über Sicherheitsprobleme bei Verschlüsselungs-Plugins wie PGP oder Sphinx, in einer Outlook/Exchange-Umgebung.

Verschlüsselungs-Plugins werden auch bei der E-Mail-Kommunikation in öffentlichen Stellen zum Schutz personenbezogener Daten eingesetzt. Bisher konnte man darauf vertrauen, dass eine verschlüsselte E-Mail die Vertraulichkeit der Nachricht auch in lokalen Netzen vor unbefugter Kenntnisnahme schützen würde.
Seit der Veröffentlichung der Sicherheitslücke ist dies nicht mehr der Fall. In diesem Beitrag werden die Ursachen des Problems aufgezeigt und Sicherheitsempfehlungen für eine vertrauliche E-Mail-Kommunikation gegeben.

* Eine Hashfunktion ist ein Algorithmus, der eine Nachricht (Bitfolge) beliebiger Länge auf eine Nachricht (Bitfolge) fester, kurzer Länge - den sogenannten Hashwert - abbildet.

”heise online” berichtete, dass trotz Aktivierung der Verschlüsselung im Plugin, die E-Mail einschließlich eines eventuell vorhandenen Dateianhangs vorab unverschlüsselt zwischen dem E-Mail-Client und dem Exchange-Server über das RCP-Protokoll (Remote Procedure Call) übertragen und im Entwurfs-Ordner des Exchange-Servers gespeichert wird. Dies erfolge nach Aussagen von Microsoft bei der Standard-Installation von Outlook aus Performance-Gründen im Hintergrund. Mit einem Netzwerk-Sniffer könne dieses aufgedeckt werden. Beim Senden wird die E-Mail dann wunschgemäß verschlüsselt übermittelt, aber zuvor wurde sie bereits unverschlüsselt an den Server übertragen.
Auf dem Übertragungsweg vom Exchange-Server zum Empfänger wird die E-Mail-Nachricht immer verschlüsselt gesendet, sofern die Verschlüsselung im Plugin aktiviert wurde. Die Vertraulichkeit der Nachricht ist auf diesem Übertragungsweg gesichert.

Wenn Outlook in Verbindung mit POP3- oder IMAP-Mail-Server eingesetzt wird, wird die E-Mail-Nachricht immer verschlüsselt übermittelt, falls die Verschlüsselung aktiviert ist.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte ebenfalls vor dem Sicherheitsproblem nach einer internen Überprüfung. Das BSI will nun auf Microsoft und die Spinx-Plugin-Hersteller einwirken, damit sie kurzfristig ein Patch oder ein Update zur Behebung des Sicherheitsproblems erstellen. Bis dahin wird vom BSI folgende Verfahrensweise empfohlen:

1. Falls die E-Mail-Daten intern offen und nur extern vertraulich behandelt werden müssen, besteht kein dringender Handlungsbedarf, sofern die IT-Grundschutzmaßnahmen umgesetzt sind.
2. Ansonsten sind ergänzende Sicherheitsmaßnahmen erforderlich:
   - keine Speicherung von E-Mail-Entwürfe in Outlook (Extras – Optionen – Einstellungen: ”Nicht gesendete Nachrichten automatisch speichern” deaktivieren),
   - SMTP/POP3/IMAP als Austauschprotokoll verwenden,
   - Dateianhänge bereits vor dem ”Einfügen” in die E-Mail verschlüsseln.

14.4 Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, erstellt vom Arbeitskreis Medien unter Beteiligung des Arbeitskreises Personalwesen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang

mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

a) Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenig personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber (zur Vereinfachung bezeichnet „Arbeitgeber“ sowohl den Arbeitgeber als auch den öffentlich-rechtlichen Dienstherrn) so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenig personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung nachträglichen Kontrollen vorzuziehen.

b) Die Bediensteten sind mit den technischen Möglichkeiten vertraut zu machen, wie die eingesetzten Verfahren datenschutzgerecht angewendet werden können. Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten umfassend darüber zu informieren (Grundsatz der Transparenz).

c) Es sind geeignete Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Insbesondere sollte jeder internetfähige PC mit leicht bedienbarer, auch bei den Kommunikationspartnern vorhandener Verschlüsselungssoftware ausgestattet sein, um zu verhindern, dass aus Bequemlichkeit personenbezogene oder andere sensible Daten unverschlüsselt übertragen werden.

d) Automatisierte zentrale und wegen einer Verschlüsselung auch lokale Virenchecks sind notwendig. Um aktive Inhalte zu überprüfen, empfiehlt sich der Einsatz von lokaler Sandbox-Software.

II. Dienstliche Nutzung

a) Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations-

bzw. Teledienstesrechts (vgl. § 1 Abs. 1 Nr. 1 Teledienstedatenschutzgesetz - TDDSG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den einschlägigen Vorschriften des Beamtenrechts bzw. des BDSG (für Tarifbedienstete des Bundes) oder den Landesdatenschutzgesetzen (für Tarifbedienstete der Länder).

b) Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen, über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

c) Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen (z. B. Psychologen, Ärzte, Sozialarbeiter und - pädagogen), muss entsprechend der Rechtsprechung des Bundesarbeitgerichtes zu Verbindungsdaten über dienstliche Telefonate eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verbindungsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

d) Der Arbeitgeber darf die Nutzungs- und Verbindungsdaten der Personalvertretung nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Soweit allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen - was überwiegend der Fall sein wird -, ist eine Auswertung dieser Daten unzulässig.

e) Soweit die grundlegenden Datenschutzprinzipien eingehalten werden, kann die Dienstvereinbarung Regelungen enthalten, die im Einzelfall hinter den unter a) genannten Vorschriften zurückbleiben. Weder das BDSG noch die Landesdatenschutzgesetze bzw. die beamtenrechtlichen Vorschriften schließen dies von vornherein aus. Nur wenn eine gesetzliche Regelung unabdingbar ist, kommt eine Abweichung zuungunsten der Beschäftigten nicht in Betracht.

f) Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung

der Protokolldaten über die unter a) genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internetnutzung auszuräumen.

g) Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG, den Landesdatenschutzgesetzen und dem Beamtenrecht des Bundes und der Länder auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.

h) Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist.

i) Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, die gefährlichen oder verdächtigen ausführbaren Code enthalten (also insbesondere html-Seiten als Mail-body, Dateien mit den Erweiterungen *.exe, *.bat, *.com oder gepackte Dateien wie *.zip, *.arj, *.lha).

III. Private Nutzung

1. Allgemeines

a) Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, ist er ihnen gegenüber TK- bzw. Teledienste-Anbieter.

b) Vom Arbeitgeber beauftragte Zugangsanbieter (Access Provider) sind zwar diesem gegenüber TK- bzw. Teledienste-Anbieter, gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers.

c) Der Arbeitgeber ist den Beschäftigten gegenüber zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren.

d) Es gelten die Regelungen der Telekommunikations-Datenschutzverordnung, des Teledienstedatenschutzgesetzes bzw. des Mediendienste-Staatsvertrages.

e) Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich

möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Voraussetzungen nicht erfüllen wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

f) Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen - am sinnvollsten durch Dienstvereinbarung oder -anweisung - unter Beteiligung des Personalrats eindeutig geregelt werden.

g) Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

2. Besonderheiten bei E-Mail

a) Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

b) Der Arbeitgeber sollte vor dem Hintergrund des von ihm zu wahrenden Telekommunikationsgeheimnisses entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder - falls privates Surfen erlaubt ist - sie auf die Nutzung eines (kostenlosen) Web-Mail-Dienstes verweisen.

c) Wie bei der dienstlichen Nutzung (vgl. Nr. II. i) dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das ausführbaren Code enthalten kann. Die Verfahrensweise ist den Beschäftigten zuvor bekannt zu geben. Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mail ganz oder teilweise unterdrückt werden oder virenverseucht sind. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung der betreffenden Beschäftigten zulässig.

d) Eine darüber hinaus gehende inhaltliche Kontrolle ist nicht zulässig.

14.5 Wahrung des Fernmeldegeheimnisses bei Abwesenheit

Mit der zunehmenden Integration des Kommunikationsmediums E-Mail in die Vorgangsverwaltung haben immer mehr öffentliche Stellen Probleme, wie sie im Falle der Abwesenheit mit eingehender E-Mail-Post umgehen. Es ist schwierig (ähnlich wie bei Telefongesprächen), genau zwischen dienstlicher und privater E-Mail zu differenzieren. Auch wenn nur die dienstliche Nutzung von E-Mail gestattet ist, kann nicht ausgeschlossen werden, dass eingehende E-Mail privater Natur ist. In der Regel wird z. B. über die Visitenkarte die E-Mail-Adresse breit gestreut. Dabei kann nicht vorausgesetzt werden kann, dass die Absender die Nutzungsregelungen beim Empfänger kennen. Da für private Mails aber das Fernmeldegeheimnis gilt, darf bei einer Abwesenheit der dienstliche Vertreter solche Mails nicht einfach zur Kenntnis nehmen.

Ich habe in meinem 9. Tätigkeitsbericht (S. 163) vorgeschlagen, für die private Nutzung einen eigenen E-Mail-Account vorzusehen. Damit träten solche Schwierigkeiten nicht auf, da für das dienstliche Postfach eine einfache Vertretungsregelung in Kraft treten könnte und das private Postfach nicht kontrolliert würde. Dies ist jedoch mit erheblichem organisatorischen und Kostenaufwand verbunden, so dass viele öffentlichen Stellen nicht von einer solchen Möglichkeit Gebrauch machen, sondern bei einem Zugang bleiben.

Damit verbleiben mehrere Varianten:

1. Der Mitarbeiter leitet pauschal alle E-Mails an einen Vertreter weiter. Der Vertreter öffnet die E-Mails; sobald er jedoch erkennt, dass die E-Mail privaten Charakter hat, schließt er sie und löscht sie aus seinem Postfach. Diese Variante hat den Vorteil, dass die Arbeitserledigung (z. B. bei wichtigen Terminsachen) nicht gefährdet wird. Allerdings wird auf diese Weise das Fernmeldegeheimnis verletzt. Nach § 85 TKG Abs. 1 unterliegen dem Fernmeldegeheimnis „der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war". Das ist schon bei der flüchtigen Kenntnisnahme durch den Vertreter der Fall. Damit ist, selbst wenn man von einer Einwilligung des abwesenden Mitarbeiters ausgeht, das Fernmeldegeheimnis in Bezug auf den Absender der E-Mail verletzt. Damit ist diese Variante nicht zulässig.

2. Der Mitarbeiter aktiviert bei Abwesenheit den Abwesenheitsassistenten und verweist im Text auf die E-Mail-Adresse seines Vertreters. Diese durchaus datenschutzkonforme Lösung hat allerdings zur Folge, dass möglicherweise wichtige Unterlagen nicht termingerecht ankommen, da nicht gewährleistet werden kann, dass der Absender in jedem Fall die Abwesenheitsnotiz erhält.

3. Ich empfehle eine Mischvariante, die sich mit derzeitig im Einsatz befindlichen E-Mail-Clients realisieren lässt. Der Mitarbeiter aktiviert gemäß Variante 2 den Abwesenheitsassistenten mit einem Hinweistext. Darüber hinaus formuliert er innerhalb des Abwesenheitsassistenten für bestimmte Absender mit eindeutig dienstlichen Hintergrund Weiterleitungsregeln, die auch zur Anwendung kommen, wenn er off-line ist. Diese Absender sollte er ggf. vor seinem Urlaubsantritt über die Weiterleitung informieren. Da diese Positivliste sich auf denjenigen Absenderkreis beschränken kann, von dem zu vermuten ist, dass während der Abwesenheit Nachrichten kommen, und da die Weiterleitungsregeln bis hin zum Betreff sehr differenziert gestaltet werden können, kann sowohl der organisatorische Aufwand in Grenzen gehalten und ein Eingriff in das Fernmeldegeheimnis vermieden werden.

14.6 Orientierungshilfe Tele- und Mediendienste*

A. Vorbemerkung

Diese Orientierungshilfe soll in erster Linie den Anbietern von Tele- und Mediendiensten bei der datenschutzgerechten Gestaltung von Angeboten helfen. Doch auch Internet-Nutzer können die Orientierungshilfe verwenden, um sich von der Einhaltung datenschutzrechtlicher Anforderungen durch Tele- und Mediendienste ein Bild zu machen.

Der Erfolg eines Tele- oder Mediendienstes hängt wesentlich vom Vertrauen ab, das ihm seine Nutzer entgegenbringen. Insofern sollte ein Anbieter die Orientierungshilfe als Gelegenheit verstehen, die positive Entwicklung seines Unternehmens zu fördern. Kunden, die unsicher sind, für welche Zwecke ihre Daten verwendet oder und an wen sie übermittelt werden, neigen eher dazu, Dienste nicht in Anspruch zu nehmen oder den Anbieter zu wechseln.

Die Orientierungshilfe beschränkt sich also auf die für Online-Dienste und das Internet typische logische Interaktion zwischen Nutzer und Anbieter von Tele- und Mediendiensten. Nicht betrachtet werden

- die reine Transportebene; hierfür sind die Bestimmungen des Telekommunikationsrechts, insbesondere das Telekommunikationsgesetz (TKG) einschlägig. Zu den Telekommunikationsdiensten gehören z. B. E-Mail-Transport und Internet-Telefonie,
- die Datenverarbeitung auf der Inhalts- bzw. Anwendungsebene (etwa bei Bank- und Versicherungsgeschäften). Hier sind das Bundesdatenschutzgesetz (BDSG), die Landesdatenschutzgesetze und ggf. datenschutzrechtliche Spezialvorschriften (z. B. das Sozialgesetzbuch) zu beachten.

* Orientierungshilfe des Hamburger Datenschutzbeauftragten, erstellt v. Peter Schaar unter Mitwirkung von Frank Möller (Stand 1. Juli 2002).

B. Was sind Tele- und Mediendienste?
Seit 1997 gibt es für Internet- Angebote gesetzliche Regelungen. Während Teledienste der Regelungskompetenz des Bundes zugeordnet sind, unterliegen Mediendienste der Zuständigkeit der Länder. Die Unterscheidung ist in der Praxis insofern unproblematisch, weil die Regelungswerke für Tele- und Mediendienste einen im Wesentlichen identischen Wortlaut haben.

Teledienste sind elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung bestimmt sind. Hier steht also der einzelne Nutzer mit seinen individuellen Geschäften im Vordergrund, wenn er z. B. seine Bankgeschäfte tätigt oder Informationsangebote (z. B. aus Datenbanken) nutzt, die keiner redaktionellen Bearbeitung unterliegen. Beispiele für Teledienste: Access Provider, electronic Banking, Datenbankabruf (mit Inhalten ohne journalistisch-redaktionelle Gestaltung), Warenbestellungen, Tarifrechner (z. B. von Versicherungen oder Telefongesellschaften), automatische Fahrplanauskünfte etc.

Mediendienste sind dagegen elektronische Verteildienste und solche, bei denen die redaktionelle Gestaltung zur Meinungsbildung im Vordergrund steht. Sie richten sich an die Allgemeinheit. Beispiele: Angebote von Tageszeitungen oder Zeitschriften, elektronische Fanzines, redaktionell bearbeitete Newsletter, Unternehmenspräsentationen etc.
Zahlreiche Online-Dienste, Portale oder Verzeichnisdienste weisen somit Merkmale auf, die innerhalb ihres Angebots unterschiedliche Zuordnungen erfordern.

Rechtsgrundlagen
§ 2 Mediendienste-Staatsvertrag (MDStV)
§ 2 Teledienstegesetz (TDG)
§§ 1, 2 Teledienstedatenschutzgesetz (TDDSG)

C. Rechtliche Anforderungen
1) Nennung der verantwortlichen Stelle/Anbieterkennzeichnung
Für den Nutzer muss erkennbar sein wer für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bei der Erbringung eines Tele- oder Mediendienstes verantwortlich ist. Zudem enthalten das TDDSG und der MDStV in erster Linie aus Gründen des Verbraucherschutzes die Verpflichtung zur Veröffentlichung verschiedener Angaben über den Diensteanbieter. Die Anbieterkennzeichnung ist in unterschiedlichen Zusammenhängen von Bedeutung, nämlich immer dann, wenn ein Nutzer durch den Teledienst einen Schaden erleidet bzw. in seinen Rechten beeinträchtigt wird und deshalb wissen muss, wem gegegnüber er seine Rechte geltend machen kann.
Nutzer von Tele- und Mediendiensten können ihre Auskunftsrechte bezüglich der über

sie gespeicherten Daten (vgl. § 4 Abs. 7 TDDSG, § 20 Abs. 1 MDStV, siehe hier im Abschnitt 6) und sonstige datenschutzrechtliche Ansprüche (Widerspruch, Sperrung, Löschung, Korrektur, Richtigstellung oder Hinzufügung einer eigenen Darstellung) nur dann in Anspruch nehmen bzw. durchsetzen, wenn sie den entsprechenden Diensteanbieter identifizieren können. Folglich muss die datenschutzgerechte Gestaltung eines Tele- oder Mediendienstes auch an der Vollständigkeit und Zugänglichkeit seiner Anbieterkennzeichnung gemessen werden.

Rechtsgrundlagen
§ 4 Abs. 3 BDSG
„Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über
1. die Identität der verantwortlichen Stelle, (...) zu unterrichten."

§ 6 TDG (entspr. § 10 Abs. 2 MDStV):
„Diensteanbieter haben für geschäftsmäßige Teledienste mindestens folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich den Vertretungsberechtigten,
2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post,
3. soweit der Teledienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, Angaben zur zuständigen Aufsichtsbehörde,
4. das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,
5. soweit der Teledienst in Ausübung eines Berufs im Sinne von Artikel 1 Buchstabe d der Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens 3-jährige Berufsausbildung abschließen (ABl. EG Nr. L 19 S. 16), oder im Sinne von Artikel 1 Buchstabe f der Richtlinie 92/51/EWG des Rates vom 18. Juni 1992 über eine zweite allgemeine Regelung zur Anerkennung beruflicher Befähigungsnachweise in Ergänzung zur Richtlinie 89/48/EWG (ABl. EG Nr. L 209 S. 25), die zuletzt durch die Richtlinie 97/38/EG der Kommission vom 20. Juni 1997 (ABl. EG Nr. 184 S. 31) geändert worden ist, angeboten oder erbracht wird, Angaben über
   a) die Kammer, welcher die Diensteanbieter angehören,
   b) die gesetzliche Berufsbezeichnung und den Staat, in dem die Berufsbezeichnung verliehen worden ist,

c) die Bezeichnung der berufsrechtlichen Regelungen und dazu, wie diese zugänglich sind,
6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27 a des Umsatzsteuergesetzes besitzen, die Angabe dieser Nummer.

Weitergehende Informationspflichten, insbesondere nach dem Fernabsatzgesetz, dem Fernunterrichtsschutzgesetz, dem Teilzeit-Wohnrechtegesetz oder dem Preisangaben- und Preisklauselgesetz und der Preisangabenverordnung, dem Versicherungsaufsichtsgesetz sowie nach handelsrechtlichen Bestimmungen bleiben unberührt."

§ 7 TDG (entspr. § 10 Abs. 4 MDStV):
„Diensteanbieter haben bei kommerziellen Kommunikationen, die Bestandteil eines Teledienstes sind oder die einen solchen Dienst darstellen, mindestens die folgenden Voraussetzungen zu beachten.
1. Kommerzielle Kommunikationen müssen klar als solche zu erkennen sein.
2. Die natürliche oder juristische Person, in deren Auftrag kommerzielle Kommunikationen erfolgen, muss klar identifizierbar sein.
3. Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke müssen klar als solche erkennbar sein, und die Bedingungen für ihre Inanspruchnahme müssen leicht zugänglich sein sowie klar und unzweideutig angegeben werden."

§ 10 Abs. 1 MDStV:
„Diensteanbieter haben für Mediendienste folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:
1. Namen und Anschrift sowie
2. bei juristischen Personen auch Namen und Anschrift des Vertretungsberechtigten."

§ 10 Abs. 3 MDStV:
"Diensteanbieter von journalistisch-redaktionell gestalteten Angeboten, in denen vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben oder in periodischer Folge Texte verbreitet werden, müssen zusätzlich zu den Angaben nach Absatz 1 und unbeschadet des Absatzes 2 einen Verantwortlichen mit Angabe des Namens und der Anschrift benennen. Werden mehrere Verantwortliche benannt, so ist kenntlich zu machen, für welchen Teil des Mediendienstes der jeweils Benannte verantwortlich ist. Als Verantwortlicher kann nur benannt werden, wer
1. seinen ständigen Aufenthalt im Inland hat,
2. nicht infolge Richterspruchs die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat,
3. voll geschäftsfähig ist und
4. unbeschränkt strafrechtlich verfolgt werden kann."

Den genannten Rechtsgrundlagen ist gemeinsam, dass sie dem Nutzer ein hinreichendes Maß an Transparenz sichern sollen. Der Nutzer muss erkennen können, mit welchen Personen oder Firmen er es zu tun hat, wenn er Angebote in Anspruch nimmt.
Nach § 6 TDG (§ 10 Abs. 2 MDStV) besteht Kennzeichnungspflicht für alle "geschäftsmäßigen Angebote". Unter diesen Begriff fallen also alle Teledienste, deren Angebote auf einen längeren Zeitraum angelegt sind. Dabei kommt es auf eine Gewinnerzielungsabsicht übrigens nicht an. Eine Geschäftsmäßigkeit liegt nicht vor, wenn Inhalte nur einmalig oder kurzfristig angeboten werden, wie z. B. bei privaten Gelegenheitsgeschäften in *Newsgroups* oder vergleichbaren virtuellen Schwarzen Brettern. Der Begriff der Geschäftsmäßigkeit sichert also ein Stück Verhältnismäßigkeit: Während man vom Verfasser einer Kleinanzeige nicht die Angabe einer kompletten Anbieterkennzeichnung verlangen wird, unterliegt der Anbieter des Verteildienstes zahlreicher Kleinanzeigen selbstverständlich der Kennzeichnungspflicht.
Anders ist dies bei der Impressumspflicht gem. § 10 Abs. 1 MDStV. Hier wird kein Unterschied nach geschäftsmäßigen oder nicht geschäftsmäßigen Angeboten vorgenommen. Es sind also auch alle nicht geschäftsmäßigen Medienangebote mit einem Impressum zu versehen.
Die Verpflichtung zur Angabe der Identität gemäß § 4 Abs. 3 BDSG bezieht sich ausschließlich auf die für die Datenverarbeitung verantwortliche Stelle. Bei Einschaltung von Stellen, die personenbezogene Daten gemäß § 11 BDSG im Auftrag verarbeiten (etwa Rechenzentren), muss lediglich die auftraggebende Stelle genannt werden. Dagegen müssen auch solche Diensteanbieter die Informationspflichten gemäß §§ 6,7 TDG, § 10 MDStV beachten, die Informationen nur durchleiten (§ 9 TDG), Proxy-Server betreiben (§ 10 TDG) oder Informationen für Nutzer speichern (§ 11 TDG).

Bedingt durch die vielfältigen technischen Konstellationen im Internet ist ggf. eine differenziertere Unterrichtung erforderlich. Ein Beispiel ist das sog. Web-Hosting. Hierbei überträgt der Anbieter von Inhalten die technische Abwicklung seines Dienstes einem Dritten. Dieser als Host bezeichnete Dienstleister kann auf unterschiedliche Weise in die Abläufe einbezogen sein. Bei der Verarbeitung personenbezogener Daten im Rahmen des Angebots (etwa bei elektronischen Bestellungen) handelt es sich im Regelfall um Auftragsdatenverarbeitung und der Auftraggeber trägt die Verantwortung für personenbezogene Daten des Nutzers (§ 11 BDSG). Der Auftraggeber ist Adressat sämtlicher Daten-schutzrechte, die Betroffene geltend machen können, z. B. Auskunftsrechte. Der Auftraggeber ist gemäß § 4 Abs. 3 BDSG verpflichtet, seine Identität als verantwortliche Stelle anzugeben. Soweit der Betreiber des Hostding-Service in eigener Verantwortung personenbezogene Daten erhebt, verarbeitet oder nutzt (beispielsweise in Logdateien), unterliegt auch er der Informationspflicht gem. § 4 Abs. 3 BDSG. Damit der Nutzer überhaupt die Möglichkeit bekommt, diese

Information zur Kenntnis zu nehmen, muss der Diensteanbieter den Nutzer in diesem Fall auf die Identität des Hosting Service hinweisen.

Realisierungsmöglichkeiten
- Impressum auf der Homepage,
- Impressum auf jeder Web-Seite,
- Verweis (Link) auf Impressum auf jeder Web-Seite oder auf der Homepage,
- Hinweis zu Beginn des Dialogs bei sonstigen interaktiven Angeboten.

Unzureichend ist
- Nennung eines Verantwortlichen ohne Anschrift,
- Nennung eines Firmennamens ohne Benennung eines Vertretungsberechtigten einschließlich seiner Anschrift,
- die Angabe lediglich einer Postfachanschrift,
- Nennung eines Verantwortlichen in den AGB,
- keine Nennung des Hosting Service, soweit dieser bei der Abwicklung eines Angebots in eigener Verantwortung personenbezogene Daten verarbeitet.

2) Unterrichtung des Nutzers
Der Nutzer ist zu Beginn des Nutzungsvorgangs umfassend über die Verarbeitung seiner Bestands- und Nutzungsdaten zu unterrichten. Dazu gehören auch Hinweise auf Widerspruchsrechte z. B. aus § 6 Abs. 3 TDDSG oder auf das Recht zum Widerruf erteilter Einwilligungen (§ 4 Abs. 3 TDDSG).

Rechtsgrundlagen
§ 4 Abs. 1 TDDSG (entspr. § 18 Abs. 1 MDStV)
„Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG Nr. L 281 S. 31) zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.“

§ 6 Abs. 3 TDDSG
„Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter

hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 4 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden."

a) Unterrichtung zu Beginn des Nutzungsvorgangs

Zukunftsweisend sind Ansätze, die den Datenschutz als Grundlage der Geschäftspolitik sehen, die ihn also in ihre „Policy" integrieren. Wenn am Anfang einer Nutzungsbeziehung eine klare Information darüber stattfindet, welche Daten erhoben und zu welchen Zwecken verwendet werden können, stärkt dies das gegenseitige Vertrauen und nützt der Geschäftsbeziehung.

Zur Gestaltung einer Unterrichtung von Nutzern bzw. einer Privacy Policy lässt sich der OECD Privacy Statement Generator (http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm) heranziehen. Die Verwendung des Generators entbindet den Diensteanbieter jedoch nicht von der Verpflichtung zur die Einhaltung der nach deutschem Recht vorgesehenen Unterrichtungspflichten. Ein weiteres Werkzeug zur Stärkung der Transparenz ist die Platform for Privacy Preferences (P3P - http://www.w3.org/P3P).

Hierbei verständigen sich die Rechner von Anbieter und Nutzer über den Austausch personenbezogener Daten. Auch die Verwendung von P3P entbindet den Diensteanbieter nicht davon, die Inhalte der Datenschutzerklärung entsprechend der Vorgaben des deutschen Rechts zu gestalten.

Die Erhebung personenbezogener Daten im Rahmen von Tele- und Mediendiensten beginnt grundsätzlich dann, wenn der Nutzer ein Web-Angebot aufruft, denn dabei werden die IP-Adresse des vom Nutzer verwendeten Rechners und weitere technische Angaben automatisch an den Anbieter weitergeleitet. Spätestens zu dem Zeitpunkt, wenn der Nutzer zur Angabe persönlicher Daten aufgefordert wird oder wenn Dateien mit direktem oder indirektem Personenbezug von seinem Rechner abgerufen werden, die dort schon gespeichert vorliegen (etwa in Cookies - vgl. 2c), muss der Diensteanbieter den Nutzer unterrichten. Sofern Daten des Nutzers in Staaten außerhalb des Europäischen Wirtschaftsraums (derzeit: EU-Staaten, Norwegen, Island und Liechtenstein) verarbeitet werden, ist darauf gesondert hinzuweisen. Neben der Aufklärung über die zur Anwendung kommende Verfahrensweise muss ein Hinweis auf Namen und Sitz des betreffenden Verarbeiters gegeben werden (vgl. 1).

Die Unterrichtung muss vollständig und verständlich sein. Die Unterrichtung bzw. der Hinweis auf die Unterrichtung ist so anzubringen, dass der Nutzer sie üblicherweise zur Kenntnis nimmt, wenn er das entsprechende Angebot aufruft. Das bedeutet, dass die Information

- in ausreichender Schriftgröße erfolgt,
- im oberen, üblicherweise im sichtbaren Bereich ohne Blättern/Rollen des Bildschirminhalts („Scrollen") untergebracht und
- hinreichend auffällig (etwa farblich hervorgehoben, Fettdruck) gestaltet ist.

Realisierungsmöglichkeiten
- ausführliche und verständliche Unterrichtung auf der Homepage des Anbieters,
- ausdrücklicher Verweis (Link) auf die Unterrichtung auf einer anderen Seite. Soweit auf Datenschutz-Informationen durch einen Verweis (Link) hingewiesen wird, die an anderer Stelle gespeichert sind, gelten diese Anforderungen auch für den Verweis. Der Link muss in verständlicher Weise als Hinweis auf den Datenschutz erkennbar sein; der Gegenstand der Unterrichtung muss für den Nutzer zweifelsfrei aus der Bezeichnung des Links hervorgehen, z.B. „Information über die Erhebung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten für Zwecke der ...“,
- Unterrichtung in einem elektronischen Erhebungsformular,
- ausdrücklicher Verweis (Link) auf die Unterrichtung in dem elektronischen Erhebungsformular,
- Unterrichtung vor dem Absenden des Formulars in einem Pop Up Fenster mit ausdrücklicher Abbruchmöglichkeit *(nur als Ergänzung einer anderen Form der Unterrichtung, weil diese Funktion das vorherige Herunterladen von aktiven Inhalten - etwa Java Skript, Active-X, VB Script - voraussetzt, auf deren Aktivierung datenschutzbewusste Nutzern aus Sicherheitsgründen verzichtet haben könnten),*
- schriftliche Information des Nutzers vor der ersten Erhebung personenbezogener Daten.

Unzureichend ist:
- allgemeiner Hinweis auf Nutzungsbedingungen oder Allgemeine Geschäftsbedingungen (AGB),
- pauschaler Hinweis, dass dem Datenschutz Rechnung getragen wird,
- Hinweis, dass personenbezogene Daten verarbeitet werden,
- Information erst nach erfolgter Datenerhebung bzw. während der Datenübertragung,
- Nennung einer Firma oder Firmengruppe ohne Angabe des Staates, in dem die Datenverarbeitung stattfindet,
- Hinweis darauf, dass die Daten nur innerhalb eines Unternehmens oder einer Firmengruppe verwendet werden.

b) Abrufmöglichkeit der Unterrichtung
Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein. Es ist darauf zu achten, dass die Unterrichtung durch den Nutzer ohne besondere Vorkenntnisse im Angebot gefunden werden kann. Dies kann z. B. durch Verweis (Link) auf die Unterrichtung an anderer Stelle (z. B. Homepage) geschehen.

Realisierungsmöglichkeiten
- Speicherung der Tatsache und des Inhalts der Unterrichtung in einer Protokolldatei des Anbieters mit individueller Abrufmöglichkeit des Nutzers,

- Speicherung der Tatsache und des Inhalts der Unterrichtung in einer Datei auf dem Rechner des Nutzers,
- Speicherung der Unterrichtung auf dem Rechner des Anbieters (ohne personenbezogene Protokollierung der individuellen Unterrichtung). In diesem Fall müssen bei Änderungen der Unterrichtung auch die älteren Versionen gespeichert und zum Abruf durch den Nutzer bereitgehalten werden, damit der tatsächliche Gegenstand der Unterrichtung nachvollzogen werden kann.

Unzureichend ist:
- individuelle Protokollierung der Unterrichtung beim Diensteanbieter ohne Abrufmöglichkeit des Inhalts der Unterrichtung für den Nutzer,
- Abrufmöglichkeit nur für die neueste Version der Unterrichtung, wenn auch auf Grundlage einer früheren Version Daten erhoben wurden.

c) Unterrichtung über Verwendung von Cookies

Cookies können entweder zur Verbindungssteuerung während einer Sitzung oder zum Wiedererkennen mehrfacher Nutzung eines Angebots durch denselben Nutzer eingesetzt werden. Während im ersten Fall die Cookies nach Beendigung der Sitzung wieder gelöscht werden können, bleiben sie im anderen Fall längere Zeit auf dem Computer des Nutzers gespeichert. Es handelt sich um Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen. Nutzungsprofile, die vom Anbieter unter Verwendung der Inhalte von Cookies gespeichert werden, sind nicht anonym, sondern weisen einen indirekten Personenbezug auf (vgl. 5).

Die Unterrichtungspflicht betrifft Cookies, die längerfristig - also über die jeweilige Sitzung hinaus - auf dem Rechner abgelegt werden. Der Nutzer ist beim Setzen eines derartigen Cookies zu unterrichten. Die Verwendung von Cookies für Nutzungsprofile kann unter bestimmten Umständen auch unzulässig sein (vgl. 3). Soweit Cookies dafür verwendet werden, die Registrierung des Nutzers in Nutzungsprofilen zu unterbinden, weil der Nutzer der Verwendung seiner Daten für diesen Zweck widersprochen hat, ist er auch über den Inhalt derartiger („opt out“) Cookies zu informieren.

Die Unterrichtung muss Informationen über den Zweck, den Inhalt und das Verfallsdatum des Cookies enthalten. Die Unterrichtung kann unterbleiben, soweit Cookies ausschließlich für die Dauer der jeweiligen Sitzung zwischengespeichert und danach automatisiert gelöscht werden und ein Personenbezug nicht hergestellt wird.

Realisierungsmöglichkeiten
- Unterrichtung auf Homepage,
- ausdrücklicher Verweis (Link) auf die Unterrichtung in der Homepage,
- Unterrichtung auf der Seite, die Links auf Seiten mit Cookies enthält, bzw. ausdrücklicher Verweis (Link) auf eine entsprechende Unterrichtung.

Unzureichend ist:
- Hinweis auf Konfigurationsmöglichkeiten im Browser,
- pauschaler Hinweis, dass Cookies verwendet werden,
- Unterrichtung der Nutzer erst, nachdem das Cookie gesetzt wurde.

3) Nutzungsprofile unter Pseudonym
Zwar darf ein Diensteanbieter nach § 6 Abs. 3 TDDSG (§ 19 Abs. 4 MDStV) für Zwecke der Werbung, der Marktforschung oder der bedarfsgerechten Gestaltung des Dienstes Nutzerprofile unter Verwendung von Pseudonymen erstellen. Er darf dies jedoch nur dann tun, wenn der Nutzer dieser Verwendung seiner Daten nicht widersprochen hat. Auf dieses Widerspruchsrecht ist der Nutzer „zu Beginn des Nutzungsvorgangs“ (§ 4 Abs. 1 TDDSG) hinzuweisen. Mit der Unterrichtung ist ihm die Möglichkeit einzuräumen, dieses Widerspruchsrecht praktisch wahrzunehmen. Weiterhin muss er jederzeit die Möglichkeit haben, seinen diesbezüglichen Willen zu ändern (vgl. 4).

Rechtsgrundlagen
§ 6 Abs. 3 TDDSG (entspr. § 19 Abs. 4 MDStV)
„Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder der bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 4 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.“

a) Führung von Nutzungsprofilen

Zulässig ist:
- die ausschließliche Verwendung von Nutzungsdaten, die ohnehin bei der Inanspruchnahme von Telediensten entstehen und deren Erhebung für Zwecke der Angebotsvermittlung oder der Abrechnung eines Dienstes zulässig ist. Nutzungsprofile dürfen nur unter Pseudonym gebildet werden,
- die Führung des Nutzungsprofils unter Pseudonym (Datum, das an Stelle des Namens zur Zuordnung bestimmter Informationen über einen Nutzer verwendet wird). Die Identifikatoren, die üblicherweise von Ad Services zur Erstellung von Online-Profilen verwendet werden, sind als Pseudonyme anzusehen. Der Diensteanbieter muss durch technisch-organisatorische Maßnahmen sicherstellen, dass eine Aufdeckung des Pseudonyms (insb. durch Zusammenführung mit Identifikationsdaten des Nutzers) unterbleibt,
- die ausschließlich interne Verwendung von unter Pseudonym geführten Nutzungsdaten durch den Diensteanbieter,
- eine Übermittlung von Nutzungsdaten an andere Diensteanbieter zum Zwecke von

deren Marktforschung in anonymisierter Form, d. h. ohne jeden Personenbezug und ohne Pseudonym (§ 6 Abs. 5 Satz 4 TDDSG),
- die Verwendung der Nutzungsprofile ausschließlich für die im Gesetz genannten Zwecke, d. h. für die Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der Dienste.

Jede über die gesetzliche Erlaubnis hinausgehende Erstellung oder Verwendung von Nutzungsprofilen bedarf der ausdrücklichen Einwilligung durch den Nutzer.

Unzulässig ist:
- die Führung von Nutzungsprofilen, bei denen die Daten dem Betroffenen direkt zugeordnet werden. Die Zuordnung kann dabei sowohl unter dem Namen als auch unter anderen den Betroffenen direkt identifizierenden Merkmalen geschehen (z. B. Konto- oder Kundennummer, Kfz-Kennzeichen, Telefonnummer, E-Mail-Adresse, Anschrift),
- die nachträgliche Herstellung des Personenbezugs bei Nutzungsprofilen, die unter Pseudonym geführt werden, z. B. durch Auswertung von elektronischen Formularen, die der Nutzer bei einer Bestellung verwendet hat,
- die Verknüpfung von Nutzungsdaten mit sonstigen Angaben über den Betroffenen, z. B. aus Kundendatenbanken,
- die Übermittlung von Nutzungsdaten an Dritte, insbesondere an andere Diensteanbieter unter Pseudonym oder mit direktem Personenbezug,
- die Verwendung der Nutzungsprofile für andere als die gesetzlich vorgeschriebenen Zwecke, z. B. zur Bonitätsprüfung.

b) Widerspruchsmöglichkeit

Das Widerspruchsrecht hat z. B. Konsequenzen für die Verwendung von Cookies. Von der Nutzung auszuschließen sind die Cookies derjenigen, die der Nutzung ihrer Daten unter Pseudonym widersprochen haben. Soweit zur Realisierung des Widerspruchsrechts ebenfalls die Cookie-Technologie verwendet wird, ist auch für die „opt out"-Cookies die Unterrichtungspflicht zu beachten (vgl. 2 c).

Realisierungsmöglichkeiten
- umfassende Unterrichtung des Betroffenen über Widerspruchsrechte einschließlich eines Hinweises auf (möglicherweise negative) Folgen eines Widerspruchs,
- Hinweis auf Widerspruchsrechte auf der Webseite, auf der die Daten des Nutzers erhoben werden,
- ausdrücklicher Hinweis auf Widerspruchsrecht im Webangebot, soweit Nutzungsdaten unter Pseudonym für Nutzungsprofile verwendet werden sollen,
- Hinweis auf die Widerspruchsmöglichkeit auf den Seiten, durch die Cookies gesetzt werden, die für die Bildung von Nutzungsprofilen verwendet werden sollen,
- Hinweis auf die Widerspruchsmöglichkeit auf den Seiten, die mit Seiten verlinkt sind, die Cookies setzen,

- Widerspruchsoption als Formularfeld im Zusammenhang mit der Erhebung der Bestandsdaten zu Beginn des Vertragsverhältnisses (z. B. als Streichungs- oder Ankreuzlösung),
- als von der Startseite jederzeit zugängliches Formularfeld „Änderung der Bestandsdaten“,
- Widerspruchsmöglichkeit per E-Mail (in diesem Fall muss technisch und organisatorisch gewährleistet werden, dass die E-Mails mit Widersprüchen unverzüglich bearbeitet und die Widersprüche umgesetzt werden),
- Opt-Out-Feld im Erhebungsformular bei elektronischen Anträgen,
- Verwendung von „opt out“-Cookies, die das Setzen von „Profil-Cookies“ verhindern.

Unzureichend wäre:
- keine Informationen über Widerspruchsmöglichkeiten,
- allgemeine Information über Widerspruchsrechte in allgemeinen Geschäfts- bzw. Nutzungsbedingungen,
- Einräumung eines Widerspruchsrechts („opt-out“) in Fällen, in denen eine Einwilligung erforderlich ist,
- Beschränkung der Widerspruchsmöglichkeit auf die Schriftform,
- personalisierte Opt-out-Cookies bei Nutzung von Cookies zur Nutzeridentifizierung.

4) Einwilligung

Es gilt der Grundsatz, dass personenbezogene Daten von Diensteanbietern nur zur Durchführung von Telediensten beziehungsweise Mediendiensten erhoben, verarbeitet und genutzt werden dürfen, soweit dies eine Rechtsvorschrift erlaubt oder der Nutzer eingewilligt hat.

Rechtsgrundlage
§ 3 Abs. 1 TDDSG (entspr. § 17 Abs. 1 MDStV)

„Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.“

a) Grenzen der Einwilligung

Soweit der Anbieter personenbezogene Daten aufgrund einer Einwilligung erheben, verarbeiten oder nutzen will, darf die Einwilligung grundsätzlich nicht zur Voraussetzung der Nutzungsmöglichkeit des Dienstes gemacht werden. Bei Telediensten kann eine derartige Einwilligung verlangt werden, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten in zumutbarer Weise möglich ist. Die Einwilligung hat in jedem Falle auf der freien Entscheidung des Nutzers zu beruhen.

Rechtsgrundlage
§ 3 Abs. 4 TDDSG (entspr. § 17 Abs. 4 MDStV)
„Der Diensteanbieter darf die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist."

§ 4 a Abs. 1 BDSG:
„Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben."

Mit Einwilligung des Nutzers ist zulässig:
- Erhebung, Verarbeitung und Nutzung personenbezogener *Bestandsdaten* für Zwecke der Beratung, der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste (§ 5 TDDSG; § 19 Abs. 1 MDStV),
- Aufnahme in ein Teilnehmerverzeichnis,
- Erhebung der E-Mail-Adresse für die Zusendung eines Newsletters,
- Erhebung von besonderen Interessen, um den Dienst auf die Vorlieben des Nutzers zuzuschneiden,
- Abfrage von Zugangsdaten, die für die Nutzung eines geschlossenen Dienstes erforderlich sind.

Unzulässig ist:
- obligatorische Erhebung von Daten, die für die Erbringung des jeweiligen Dienstes nicht erforderlich sind (etwa des Namens und der Anschrift bei einem Newsletter, der per E-Mail zugestellt werden soll),
- obligatorische Personalisierung des Zugangs als Voraussetzung für einen allgemein zugänglichen Tele- oder Mediendienst, soweit die Personalisierung nicht für Vermittlungs- und Abrechnungszwecke erforderlich ist,
- pauschale Einwilligung in die Nutzung der erhobenen Daten für andere Zwecke in allgemeinen Geschäftsbedingungen oder Nutzungsbedingungen.

b) Form der Einwilligung
Die Einwilligung kann bei Tele- und Mediendiensten elektronisch oder in Schriftform erfolgen. Dabei beziehen sich die Regeln zur elektronischen Einwilligung im TDDSG bzw. MDStV lediglich auf die Verarbeitung personenbezogener Daten, die sich auf das Verhältnis zwischen dem Diensteanbieter und dem Nutzer beziehen, und zwar im

unmittelbaren Zusammenhang mit dem jeweiligen Tele- bzw. Mediendienst. Alle über diese spezielle Beziehung hinausreichenden Datenverarbeitungen bedürfen nach dem BDSG im Regelfall der Schriftform bzw. einer qualifizierten elektronischen Signatur nach den Vorgaben des § 126a BGB.

Rechtsgrundlagen
§ 4 Abs. 2 TDDSG (entspr. § 18 Abs. 2 MDStV)
„Bietet der Diensteanbieter dem Nutzer die elektronische Einwilligung an, so hat er sicherzustellen, dass
1. sie nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann,
2. die Einwilligung protokolliert wird und
3. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann."

Hinzuweisen ist auch auf § 4 a Abs. 1 Satz 4 BDSG:
„Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben."

Realisierungsmöglichkeiten
- Der Diensteanbieter verwendet ein Verfahren, das die ausdrückliche Einwilligung des Nutzers gewährleistet, z. B.
- indem er den Text der Einwilligung per E-Mail an den Nutzer sendet und den Nutzer zu einer Bestätigung der Einwilligung auffordert ("double opt in"),
- indem die Einwilligungserklärung dem Nutzer in einem Bildschirmfenster angezeigt wird; der Nutzer bestätigt durch Anklicken eines eindeutig beschrifteten Auswahlfeldes, dass er einverstanden ist; der Text der Einwilligung wird dem Nutzer mit Hinweis auf sein recht zum jederzeitigen Widerruf per E-Mail zugesandt ("confirmed opt in").
- Grundsätzlich zulässig ist auch die Einwilligung per Mausklick; dem Nutzer werden in einem Formular verschiedene Wahlmöglichkeiten angeboten; durch "Absenden" des Formulars, also dessen Bestätigung per Mausklick, erklärt der Nutzer sein Einverständnis. Im Hinblick auf die mangelnde Sicherheit des Internet sollte hiervon nur dann Gebrauch gemacht werden, wenn bereits ein Anbieter-Nutzer-Verhältnis besteht und die Identität des Nutzers dem Diensteanbieter bekannt ist.
- Möglichkeit des Nutzers zum elektronischen Abruf der Einwilligung aus dem Angebot (als Bestandteil des Dienstes).
- Ablage der Einwilligung auf dem Rechner des Nutzers nach entsprechendem Hinweis mit interaktivem Zugriff, der durch das Clientprogramm gesteuert wird.

Unzureichend ist:
- eine bloße Information statt ausdrücklicher Einwilligung (z. B. Hinweis auf allgemeine Geschäftsbedingungen bzw. Nutzungsbedingungen),
- die Einräumung eines Widerspruchsrechts (opt out) statt einer Einwilligung (opt in)

mit dem Hinweis darauf, dass die Einwilligung als erteilt gilt, sofern der Betroffene nicht widerspricht,
- das Einblenden einer Einwilligungserklärung, die der Betroffene nicht ausdrücklich bestätigen muss,
- das Fehlen eines Hinweises darauf, dass bestimmte Angaben freiwillig sind,
- die Unterbrechung der Anmeldeprozedur zu einem Dienst, wenn der Nutzer nicht seine Einwilligung zur Datenverarbeitung für andere Zwecke erteilt oder personenbezogene Daten preisgibt, die für die Erbringung des konkreten Dienstes nicht erforderlich sind,
- die Auskunft über elektronisch erteilte Einwilligungen nur auf schriftliche Anfrage des Nutzers.

c) Protokollierung bzw. Abrufmöglichkeit der Einwilligung
Damit auch nachträglich festgestellt werden kann, ob und ggf. welche Einwilligungen erteilt wurden, sehen die gesetzlichen Vorschriften vor, dass die Erklärungen zu protokollieren sind und vom Nutzer jederzeit abgerufen werden können (vgl. 2b). Die Beweislast für das Vorliegen einer Einwilligung liegt bei derjenigen Stelle, die personenbezogene Daten verarbeitet, also beim Diensteanbieter.

Rechtsgrundlagen
§ 4 Abs. 2 TDDSG (entspr. § 18 Abs. 2 MDStV)
„Bietet der Diensteanbieter dem Nutzer die elektronische Einwilligung an, so hat er sicherzustellen, dass
1. sie nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann,
2. die Einwilligung protokolliert wird und
3. der Inhalt der Einwilligung jederzeit vom Nutzer abgerufen werden kann."

Realisierungsmöglichkeiten
- Der Nutzer kann den Einwilligungstext aus dem Angebot (als Bestandteil des Dienstes) abrufen; es werden auch ältere Fassungen von Einwilligungserklärungen bereitgehalten, soweit auf ihrer Basis noch personenbezogene Daten verarbeitet werden.
- Der Einwilligungstext wird dem Nutzer auf Anfrage ohne zeitliche Verzögerung zugesandt (automatisch generierte E-Mail)
- Ablage der Einwilligung auf dem Rechner des Nutzers nach entsprechendem Hinweis mit interaktivem Zugriff, der durch das Clientprogramm gesteuert wird.

Unzureichend ist:
- Auskunft über elektronisch erteilte Einwilligungen nur auf schriftliche Anfrage des Nutzers.
- Abrufmöglichkeit nur für aktuelle Einwilligungstexte, obwohl auch personenbezogene Daten auf Basis früherer Fassungen der Erklärung verarbeitet werden

d) Widerruf einer erteilten Einwilligung
Der Nutzer hat das jederzeitige Recht, eine erteilte Einwilligung mit Wirkung auf die Zukunft zu widerrufen. Sofern die Möglichkeit zur elektronischen Erteilung einer Einwilligung besteht, muss diese auch elektronisch abrufbar und auf diesem Wege jederzeit widerrufbar sein.

Rechtsgrundlagen
§ 4 Abs. 3 TDDSG (entspr. § 18 Abs. 3 MDStV)
„Der Diensteanbieter hat den Nutzer vor Erklärung seiner Einwilligung auf sein Recht auf jederzeitigen Widerruf mit Wirkung für die Zukunft hinzuweisen."

Realisierungsmöglichkeiten
- Der Nutzer hat während der Nutzung des Dienstes die Möglichkeit, ein Bildschirmfenster aufzurufen, das ein eindeutig beschriftetes Auswahlfeld enthält, durch dessen Bestätigung er den Widerruf ausdrückt und veranlasst.
- Der Nutzer hat aus dem Dienst heraus die Möglichkeit, ein Feld zu klicken, was dazu führt, dass er vom Dienst eine E-Mail erhält, deren Rücksendung seitens des Betreibers als Bestätigung des Widerrufs anzusehen ist.
- Nennung einer Stelle (E-Mail-Adresse, Telefonnummer oder postalische Adresse), an die der Widerruf gesendet werden kann

Unzureichend ist:
- Ein Hinweis auf ein lediglich schriftliches Widerrufsrecht einer erteilten Einwilligung.
- Hinweis auf Widerrufsrecht ohne Nennung der Stelle, an die der Widerruf gerichtet werden kann.
- Kostenpflichtigkeit von Widerrufserklärungen (z. B. durch Nennung einer "0190"-Telefonnummer).

5) Anonyme und pseudonyme Nutzungsmöglichkeiten
Anonyme und pseudonyme Nutzungsmöglichkeiten sind keineswegs ein Luxus, der nur auf besonderen Wunsch oder als außergewöhnliche Leistung für eine Minderheit zur Verfügung gestellt wird. Vielmehr ergibt sich die Notwendigkeit dieser Nutzungsformen unmittelbar aus dem Grundsatz des Datenschutzrechts, wonach im Hinblick auf personenbezogene Daten der Grundsatz der Datenvermeidung und Datensparsamkeit gilt (vgl. § 3 a BDSG).
Daten, die unter Pseudonym gespeichert werden, sind zwar noch personenbezogen, können aber nur mit Zusatzkenntnissen (insb. über Zuordnungsregeln) den Betroffenen zugeordnet werden. Zu unterscheiden sind selbst generierte Pseudonyme, Referenz- und Einwegpseudonyme. Soweit Cookies für die Bildung von Nutzungsprofilen unter Pseudonym gesetzt werden sollen, sind die Nutzer beim Setzen zu informieren (vgl. 2c).

Rechtsgrundlagen
§ 3 Abs. 6 BDSG
„Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können."

§ 3 Abs. 6 a BDSG
„Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren."

§ 3 a BDSG
„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhält-nis zu dem angestrebten Schutzzweck steht."

§ 4 Abs. 6 TDDSG (entspr. § 18 Abs. 6 MDStV)
„Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren."

Realisierungsmöglichkeiten
- Angebot eines Informationsdienstes ohne Individualisierung und Personalisierung,
- freie Vergabe der Kennung durch den Nutzer (als Pseudonym) ohne Abfrage von Identifikationsdaten,
- Verwendung von Cookies mit Identifikator/ID (als Pseudonym) zur Steuerung des Dienstes. In diesem Fall muss der Nutzer vor dem Setzen des Cookies informiert werden (siehe unter 2c),
- Verwendung von Cookies mit Identifikator/ID (als Pseudonym) zur Bildung von Benutzerprofilen durch den Anbieter. In diesem Fall muss der Nutzer vor dem Setzen des Cookies informiert werden (siehe unter 2c),
- echte Wahlmöglichkeit für den Nutzer, den Dienst entweder personalisiert, unter Pseudonym oder anonym zu nutzen (mit Information über die jeweiligen Konsequenzen).

Unzulässig ist:
- obligatorische Personalisierung, soweit dies nicht für die Erbringung des jeweiligen

Dienstes erforderlich ist und der Dienst auch anonym oder unter Pseudonym erbracht werden kann,
- Verwendung von Pseudonymen, die vom Anbieter oder durch Dritte ohne weiteres den Trägern der Pseudonyme zugeordnet werden können,
- Verwendung der von den Nutzern verwendeten IP-Nummern als Pseudonyme (da eine Teilmenge der IP-Nummern - insbesondere bei statischer Vergabe - einzelnen Benutzern direkt zugeordnet werden kann),
- unzureichende Information über die Möglichkeit der anonymen Nutzung oder der Nutzung unter Pseudonym,
- nachträgliche Zuordnung eines Pseudonyms zu Daten über den Träger desselben ohne dessen ausdrückliche informierte Einwilligung.

6) Auskunftsrechte
Der Nutzer hat ein umfassendes Recht auf Auskunft über die Daten, die der Anbieter über ihn gespeichert hat. Dieses Recht bezieht sich nicht nur auf die zu seiner Person gespeicherten Daten, sondern darüber hinaus auch auf den logischen Aufbau einer automatisierten Datensammlung. Auskunftsrechte lassen sich durch Verträge mit dem Nutzer nicht ausschließen oder beschränken.

Rechtsgrundlagen
§ 4 Abs. 7 TDDSG (entspr. § 20 Abs. 1 MDStV)
„Der Diensteanbieter hat dem Nutzer auf Verlangen unentgeltlich und unverzüglich Auskunft über die zu seiner Person oder seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden."

§ 20 Abs. 3 MDStV
„Werden über Angebote personenbezogene Daten von einem Diensteanbieter ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet und wird der Nutzer dadurch in seinen schutzwürdigen Interessen beeinträchtigt, kann er Auskunft über die zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit durch die Mitteilung die journalistische Aufgabe des Anbieters durch Ausforschung des Informationsbestandes beeinträchtigt würde oder aus den Daten

1. auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung mitgewirkt haben, oder

2. auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Der Nutzer kann die Berichtigung unrichtiger Daten oder die Hinzufügung einer eigenen

Darstellung von angemessenem Umfang verlangen. Für die Aufbewahrung und Übermittlung gilt Absatz 2 entsprechend."

§ 6 Abs. 1 BDSG
„Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden."

§ 6a Abs. 3 BDSG
„Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten."

Realisierungsmöglichkeiten
- Online-Auskunft nach Authentifizierung des Nutzers durch Eingabe von Kennung und Passwort,
- Auskunftserteilung unter Pseudonym über die Daten, die unter diesem Pseudonym gespeichert sind, soweit eine Authentifizierung unter diesem Pseudonym möglich ist (z. B. über die Eingabe von Pseudonym und Passwort),
- Auskunft per E-Mail an die E-Mail-Adresse des Nutzers,
- Bei Auskunftserteilung über das Internet sollte eine verschlüsselte Datenübertragung möglich sein (ansonsten: Hinweis auf Risiken),
- Sofern der Nutzer dies wünscht, muss die Auskunft in schriftlicher Form erfolgen.

Unzureichend bzw. unzulässig ist:
- ein allgemeiner Hinweis auf Arten von Daten, die gespeichert wurden, anstatt Auskunft über die konkret gespeicherten Merkmalsausprägungen,
- ein unvollständiger Zugriff des Nutzers auf seine Daten (z. B. der Online-Zugriff nur auf eigene Abrechnungsdaten, ansonsten Verweis auf die Schriftform),
- die Verweigerung der Auskunft über Daten, die unter Pseudonym gespeichert sind.

7) Hinweis auf Weiterleitung an Dritte („externe Links")
Über Links können zahlreiche Informationen und Angebote auf einfache Weise miteinander verknüpft werden. Für den Nutzer kann von Nachteil sein, dass er vielfach nicht in der Lage ist zu erkennen, wann er einen bestimmten Server bzw. den Verantwortungsbereich eines Diensteanbieters verlässt und mit einem anderen in Kontakt tritt. Weiterhin besteht bei Internetangeboten vielfach eine enge Verzahnung von Informationsangeboten und Werbung. Technisch möglich ist auch eine verborgene automatische Weiterleitung.

Um den Nutzer vor Täuschungen zu schützen, sind Anbieter von Tele- und Mediendiensten verpflichtet, dem Nutzer die Weitervermittlung an Dritte

anzuzeigen. Dies gilt auch für Werbeeinblendungen, die im Internet regelmäßig mit einer Weitervermittlung versehen sind. Werbeeinblendungen (wie auch alle anderen „kommerziellen Kommunikationen“) müssen als solche zu erkennen sein. Sie müssen daher von anderen Inhalten bzw. Informationen abgehoben sein. Werbeeinblendungen müssen ihren Auftraggeber erkennen lassen, d. h. es muss der Name des Verantwortlichen spätestens mit Aufruf eines Hyperlinks identifizierbar sein.

Rechtsgrundlagen
§ 4 Abs. 5 TDDSG
„Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.“

§ 18 Abs. 5 MDStV
„Die Weitervermittlung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.“

§ 10 Abs. 4 MDStV
Wortgleich mit § 7 TDG (s. o.)

Realisierungsmöglichkeiten
- Die Weitervermittlung wird innerhalb eines kleinen Erläuterungstextes gezeigt, der den Anbieter des vermittelten Angebots nennt bzw. den Hinweis, dass es sich hier um einen externen Link, also eine Weitervermittlung handelt.
- Sofern der Mauszeiger auf eine Weitervermittlung zeigt, öffnet sich auf dem Bildschirm ein erläuterndes Hinweisfähnchen. Idealerweise nennt es z. B. den Namen des Anbieters oder Servers, zu dem hier weitervermittelt wird.
- Bannerwerbung lässt sich analog der üblichen Darstellungsweise in Zeitschriften mit dem Hinweis „Anzeige“ kennzeichnen.
- Aus der Auflistung von Ergebnissen anbietereigener Suchmaschinen muss ebenfalls ersichtlich sein, welche der angegebenen Verweise zu externen Stellen führen.
- In jedem Falle muss Werbung (bzw. „kommerzielle Kommunikation“) als solche für den Nutzer erkennbar sein, z. B. durch Darstellung von Firmen- oder Produktlogos der Anbieter, auf die verwiesen wird.

Unzureichend bzw. unzulässig:
- lediglich optische Hervorhebung von Links ohne eine Trennung nach „internen“ und „externen“ Verweisen,
- Verzicht auf die Nennung des Anbieters/Servers, an den weitervermittelt wird, bzw. die Nichterkennbarkeit eines Verweises, der zu einem Dritten führt,
- Nutzer glauben zu machen, er werde zu einem Informationsangebot weitergeleitet,

obwohl die Absicht in der Werbung für bestimmte Dienstleistungen oder Produkte besteht,
- optisch an andere Anbieter angelehnte Gestaltung des Angebots (z. B. im Rahmen von strategischen Allianzen), was dazu führt, dass der Nutzer anhand der Aufmachung nicht erkennen kann, dass er sich nunmehr innerhalb des Angebots eines Dritten bewegt,
- pauschaler Hinweis, dass das Angebot Weitervermittlungen enthält,
- Verzicht auf eine Kennzeichnung, sofern es sich um unterschiedliche Firmen innerhalb eines Unternehmensverbundes o. ä. handelt,
- Hinweis auf Weiterleitungen in den AGB.

8) Ordnungswidrigkeiten und Bußgelder
Um die Ernsthaftigkeit der Bestimmungen über die Tele- und Mediendienste zu unterstreichen, wurden in die Gesetze entsprechende Bußgeldvorschriften aufgenommen. Besonders kleine und mittlere Unternehmen können sich durch ihr fahrlässiges Verhalten eine ernsthafte wirtschaftliche Belastung einfangen. Größere Unternehmen hingegen müssen sich besonders über die Folgen des öffentlichen Bekanntwerdens von gegen sie eingeleiteten Bußgeldverfahren im klaren sein. Während vorsätzliche oder fahrlässige Verstöße gegen einzelne Vorschriften des Teledienstedatenschutzgesetzes mit Beträgen bis zu 50.000,-- Euro geahndet werden können, sieht der (gegenüber dem TDDSG jüngere) Mediendienstestaatsvertrag für eine stattliche Reihe von 16 Tatbeständen Geldbußen von 50.000,-- bzw. in überwiegender Zahl der Tatbestände sogar bis zu 250.000,-- Euro vor (vgl. § 9 TDDSG; § 24 MDStV).

14.7 Positionspapier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen*

1 Ausgangslage

Mit dem Terrorismusbekämpfungsgesetz wurden in § 4 Passgesetz und § 1 Personalausweisgesetz nahezu gleich lautende Regelungen folgenden Inhalts aufgenommen:

* Verabschiedet auf der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07.03. - 08.03.2002.

- Pässe und Personalausweise dürfen neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von
- Fingern,
- Händen oder
- Gesicht des Inhabers enthalten.
- Alle biometrischen Merkmale und die Angaben über die Person dürfen auf den Ausweispapieren verschlüsselt gespeichert werden. Durch ein Bundesgesetz ist Folgendes zu regeln:
- Arten der biometrischen Merkmale,
- Einzelheiten der Einbringung von Merkmalen und Angaben in verschlüsselter Form,
- Art der Speicherung und
- Art ihrer sonstigen Verarbeitung und Nutzung.
- Die biometrischen Merkmale dürfen nur verwendet werden, um die Echtheit des Dokumentes und die Identität des Inhabers zu prüfen.
- Eine bundesweite Datei darf nicht eingerichtet werden.

Um beurteilen zu können, ob diese Maßnahmen geeignet und angemessen sind, müssen die verschiedenen biometrischen Verfahren aus Datenschutzsicht bewertet werden. Im Folgenden werden verschiedene Verfahren beschrieben und die Risiken aufgezeigt, die im Zusammenhang mit einem flächendeckenden Einsatz biometrischer Merkmale in Ausweisdokumenten zu erkennen sind.

2 Technische Möglichkeiten

2.1 Nutzung vorhandener biometrischer Merkmale

Bevor neue Merkmale in Ausweisen gespeichert werden, sollte geklärt werden, ob die vorhandenen nicht bereits ausreichen, um die Identität des Ausweisinhabers zu prüfen. Auf die Erhebung neuer personenbezogener Daten muss dann verzichtet werden. Könnten Verfahren eingesetzt werden, die bereits vorhandene biometrische Merkmale nutzen, wäre eine geringere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung als bei der Verwendung eines völlig neuen Merkmals ausreichend.

Lichtbild

Mit dem Foto des Inhabers enthalten deutsche Ausweisdokumente bereits biometrische Daten. Mit heute vorhandener Technik ist es grundsätzlich möglich, das Foto auf dem Personalausweis automatisch mit dem Gesicht der Person zu vergleichen, die den Ausweis vorlegt.

Möglicherweise können die zurzeit verwendeten Passbilder die Qualitätsanforderungen an eine automatisierte Verarbeitung nicht in vollem Umfang erfüllen. Bisher gibt es allerdings keine verlässlichen Aussagen über die Bildqualität, die für biometrische Verfahren erforderlich ist. Ebenso wenig ist bisher geklärt, wie sich biometrische Merkmale im Laufe der Zeit ändern. Möglicherweise müsste die Gültigkeitsdauer von Personalausweisen wesentlich verkürzt werden, damit die Verifikation anhand des Passbildes im Ausweis über die gesamte Gültigkeitsdauer sichergestellt werden kann.

Unterschrift

Die Unterschrift des Inhabers ist ein weiteres biometrisches Merkmal, das schon jetzt auf jedem deutschen Ausweisdokument vorhanden ist. Ein automatischer Vergleich der vorhandenen mit einer bei der Kontrolle geleisteten Unterschrift wäre jedoch wenig sinnvoll, weil die zur Erkennung erforderlichen dynamischen Daten der Unterschrift (Druckverlauf, Schreibpausen) im Ausweis nicht gespeichert sind.

2.2 Biometrische Vermessung des Gesichtes

Sollen biometrische Daten des Gesichtes neu erhoben und in den Ausweispapieren maschinenlesbar beispielsweise als Barcode oder elektronischer Datensatz gespeichert werden, sind hohe Qualitätsanforderungen an die Erfassungs- und Kontrollsysteme zu stellen, um eine ausreichende Wiedererkennungsrate sicherzustellen. Für gute Ergebnisse sind gleichmäßig ausgeleuchtete Frontalaufnahmen von Gesichtern erforderlich. In der Praxis werden diese Anforderungen nur mit hohem Aufwand realisierbar sein.

2.3 Papillarmuster der Finger

Werden nur die Merkmale eines bestimmten Fingers genutzt, entstehen Probleme, wenn dieser bei der Erfassung oder bei Vergleichen verletzt oder anderweitig stark beansprucht ist (z. B. bei Bauarbeitern). Die Erfassung von Daten mehrerer Finger und alternative Vergleiche bei Kontrollen sind sehr aufwändig. Außerdem zeigen Tests, dass ein signifikanter (statistisch aber noch nicht abschließend verifizierter) Prozentsatz von Papillarmustern aus physiologischen Gründen nicht nutzbar ist (siehe Punkt 3.2).

2.4 Handgeometrie und Handlinien

Bei der Vermessung der Handgeometrie handelt es sich um ein System, das in den USA bereits im Einsatz ist. Über die Erkennungsqualität gibt es keine verlässlichen Angaben. Über die Möglichkeiten der Nutzung der Handlinien gibt es ebenfalls

keine gesicherten Erkenntnisse. Die Problematik der Verletzungen oder sonstigen Einschränkungen der Nutzung einer Hand und der sich daraus ergebenden Notwendigkeit der Alternativdaten ist vergleichbar mit der bei der Papillarmusterverwendung. Unklar ist zurzeit auch die Wiedererkennungsqualität bei Handveränderungen durch Arbeits- und Alterungsprozesse.

2.5 Iris- und Retinastruktur

Die gesetzliche Formulierung „Gesicht" lässt eine Erfassung detaillierter Merkmale der Augen nicht zu. Ungeachtet dessen ist festzustellen, dass diese Verfahren bisher noch nicht im größeren Stil eingesetzt worden sind. Sie sind sowohl technisch als auch organisatorisch sehr aufwändig. Bisher ist eine genaue Kopfpositionierung erforderlich, so dass fraglich ist, ob sie durch „Ungeübte" in den Erfassungsstellen und an den Kontrollstellen praktiziert werden können. Sofern das Gesicht, die Iris oder die Retina durch ein Infrarot- oder Lasersystem abgetastet wird, ist damit zu rechnen, dass derartige Systeme auf eine signifikante Ablehnung durch die Betroffenen stoßen.

2.6 Weitere biometrische Merkmale

Aus technischer Sicht ist nicht auszuschließen, dass zur Prüfung der Identität Betroffener auch andere biometrische Merkmale verwendet werden könnten (z. B. Stimme, Bewegungsmuster). Diese Merkmale werden hier jedoch nicht weiter betrachtet, weil laut Pass- und Personalausweisgesetz neben dem Lichtbild und der Unterschrift nur biometrische Merkmale von Fingern, Händen oder dem Gesicht des Inhabers verwendet werden dürfen (siehe 1).

3 Allgemeine technische Randbedingungen

3.1 Vorgaben aus der bestehenden Rechtslage

Aus dem rechtlichen Rahmen ergeben sich für die zu schaffenden Regelungen aus technischer Sicht, unabhängig von der Art der genutzten biometrischen Merkmale, folgende Vorgaben:

- Die Kontrollsysteme bestehen aus vier Komponenten, die untrennbar und unbeeinflussbar miteinander verknüpft sein müssen:
- Leseeinheit für die aktuellen biometrischen Merkmale,
- Leseeinheit für die Ausweispapiere,
- Entschlüsselungs- und Vergleichseinheit und
- Einheit zur Freigabe bzw. Sperrung der Passage.
- Um Manipulationen ausschließen zu können, müssen die biometrischen Systeme bei der Kontrolle stand-alone arbeiten.

- Die enthaltenen Softwarekomponenten sollten zertifiziert (z. B. nach Common Criteria oder ITSEC) und signiert sein. Das gilt auch für Hardwarekomponenten, soweit mit ihnen Entschlüsselungen vorgenommen werden.
- Eine Speicherung von personenbezogenen Daten auf den Datenträgern der Kontrollsysteme über den Abschluss des Kontrollvorgangs hinaus ist nicht zulässig.
- Die Zahl der Personen, die Kontrollen trotz falscher Identität passieren können, muss möglichst gering sein (vgl. FAR unter 3.2).
- Eine regelmäßige Falsch-Rückweisung durch Unzulänglichkeiten bei den gespeicherten Daten muss vor der Ausgabe der Ausweise und Pässe schon durch die örtlichen Ausweisbehörden ausgeschlossen werden. Bevor die ausgebende Stelle den Ausweis aushändigt, muss sie ihn daher mit einem entsprechenden Referenz-Kontrollsystem prüfen.
- Die Verschlüsselung kann wahlweise bei der örtlichen Behörde oder in der Bundesdruckerei erfolgen.
- Der Verschlüsselungsalgorithmus muss wissenschaftlich anerkannt sein und dem Stand der Technik entsprechend als sicher gelten (mindestens für den Zeitraum der Gültigkeit der Ausweise).
- Der Schlüssel darf Unbefugten nicht bekannt werden.
- Wird auf eine Verschlüsselung der Daten verzichtet, müssen die gespeicherten Werte auf andere Weise gegen Missbrauch gesichert werden.

3.2 Stand der wissenschaftlichen Erkenntnisse zu biometrischen Verfahren

- Bisher gibt es keine wissenschaftlich gesicherten Erkenntnisse zu biometrischen Verfahren bei großen Anwendergruppen. Es können lediglich Erfahrungen mit kleineren Systemen (z. B. die automatisierte Kontrolle der Einwanderungsbehörde auf amerikanischen Flughäfen [Handgeometrie] oder auf den Flughäfen Schiphol und Frankfurt [Irisscan]) herangezogen werden.

- Die Leistungsfähigkeit biometrischer Systeme wird durch ihre Zurückweisungsrate berechtigter Personen (FRR False Rejection Rate) und ihre Überwindungssicherheit gegenüber unberechtigten Personen (FAR False Acception Rate) beschrieben. Beide Raten stehen in einem engen Zusammenhang. Je größer die Überwindungssicherheit ist, um so mehr berechtigte Personen werden abgewiesen. Die Ermittlung der FAR und der FRR und der Beziehung zueinander ist sehr aufwändig. Für große Anwendergruppen gibt es deshalb bisher keine herstellerneutralen Untersuchungen.

- Biometrische Systeme sind bislang hinsichtlich der FRR und der FAR nicht ausreichend überprüft, um flächendeckend eingesetzt zu werden. Das betrifft auch Fragen der Manipulationssicherheit des Gesamtsystems. Von besonderer Bedeutung

ist die Verbindung zwischen Rechner und Sensor, da bei unzureichender Sicherung biometrische Merkmale durch Einspielen (Replay) entsprechender Datensätze vorgetäuscht werden können.

- Auch die Lebenderkennung ist bisher wenig ausgereift. Es ist deshalb nicht auszuschließen, dass biometrische Systeme durch die Präsentation nachgebildeter Merkmale (Silikonabdruck eines Fingerabdrucks, Foto eines Gesichtes usw.) überwunden werden können.

- Zur FER (False Enrollment Rate), die den Anteil der Personen nennt, bei denen das jeweilige biometrische Merkmal nicht geeignet ist oder nicht zur Verfügung steht, gibt es bisher keine gesicherten wissenschaftlichen Erkenntnisse. Eine FER von 1% bedeutet beispielsweise bei bundesweiten Ausweisdokumenten, dass mehr als 500.000 Personen bei Kontrollen immer mit Fehlermeldungen rechnen müssen, da sie durch das System nicht erkannt werden. In jedem Fall muss ein Rückfallsystem für die Nutzer vorhanden sein, die eine sehr schlechte Merkmalsausprägung besitzen oder überhaupt nicht erfasst werden können.

4 Einheitliches Personenkennzeichen

Mit neu erfassten biometrischen Merkmalen bzw. mit den daraus generierten Datensätzen lässt sich eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen. Deshalb muss ausgeschlossen werden, dass die zusätzlichen biometrischen Merkmale der Ausweise sowohl für weitere staatliche Zwecke (z. B. Strafverfolgung) als auch im privatrechtlichen Bereich (z. B. für Vertragsabschlüsse) verwendet werden. Ein derartiges Merkmal käme sehr schnell einem einheitlichen Personenkennzeichen gleich, das gemäß dem Volkszählungsurteil des Bundesverfass ungsgerichts unzulässig ist (BVerfGE 65, 1 [53]).
In Bereichen, in denen Biometrie für andere als die in § 4 Passgesetz und § 1 Personalausweisgesetz genannten Zwecke zum Einsatz kommt (z. B. Zugangskontrolle), wäre eine Verknüpfung der verschiedenen Daten technisch möglich. Dies könnte zum einen durch Verwendung der im Ausweis gespeicherten Daten als Referenzmaterial für solche Zwecke erfolgen. Zum anderen könnten gespeicherte biometrische Daten mit denen abgeglichen werden, die zum Zwecke der Ausweiserstellung verwendet werden. Dies wäre, auch wenn es keine durchgängig verwendeten Standards für die Codierung biometrischer Daten gibt, verfahrensübergreifend prinzipiell durchführbar.

5 Speicherung biometrischer Daten

Zur Vermeidung der unbefugten Nutzung von Ausweisdokumenten ist nur eine biometrische Verifikation erforderlich, d. h. der Abgleich der biometrischen Merkmale

einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Eine Speicherung außerhalb des Ausweises ist dafür nicht erforderlich. Das Ziel der Erkennung von „Doppelidentitäten“ durch Abgleich biometrischer Daten einer unbekannten Person mit denjenigen anderer Personen (Identifikation) setzt die Speicherung personenbezogener Daten in zentralen Referenzdateien voraus. Aus Sicht des Datenschutzes ist eine solche Datensammlung insbesondere im Hinblick auf die Bildung eines einheitlichen Personenkennzeichens und die unvermeidlichen Missbrauchsmöglichkeiten jedoch abzulehnen.

Für die Ausweise selbst besteht die Möglichkeit, die Referenzdaten als Rohdaten oder als biometrischen Datensatz zu speichern. Während Rohdaten ggf. auch grafisch gespeichert werden können (z. B. das Bild eines Fingerabdrucks), muss für elektronische Biometriedaten („Template“, „Vektor“) der Ausweis mit einem maschinenlesbaren Datenträger (Barcode, Speicherchip etc.) versehen werden. Um einen Missbrauch dieser Daten zu verhindern, kommt insbesondere eine verschlüsselte Speicherung in Betracht. Während dies gegen einen alltäglichen Zugriff schützen mag, kann bei der Vielzahl von Geräten, in denen der Entschlüsselungsschlüssel vorhanden sein muss (bei Polizei und Grenzkontrollbehörden), jedoch kaum davon ausgegangen werden, dass die verschlüsselt gespeicherten Daten auf Dauer vor interessierten Dritten verborgen bleiben (siehe 3.1).

6 Überschießende Daten

Einige biometrische Merkmale lassen neben der Nutzung zur Identifizierung auch völlig andere Auswertungen zu. So kann möglicherweise auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von Bildern des Gesichts, der Hand und des Augenhintergrunds, von verhaltensbasierten biometrischen Merkmalen (Sprache, Unterschrift) sowie in besonderer Weise von genetischen Daten.

In der Regel sind nur aus den biometrischen Rohdaten solche Zusatzinformationen ableitbar, nicht aber aus den daraus gewonnenen Templates. Aus diesem Grund dürfen insbesondere die Rohdaten selbst nicht zentral gespeichert werden. Außerdem sind im Verarbeitungsprozess einer biometrischen Kontrolle die Rohdaten möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

7 Eignung für die Überwachung

Die Speicherung biometrischer Merkmale außerhalb des Ausweises birgt neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung. Gelingt es,

biometrische Daten im Alltag zu erfassen und diese mit einer zentralen Datenbank abzugleichen, können weitgehende Bewegungsprofile der Betroffenen erstellt werden. Im Gegensatz zu einer Erfassung eines biometrischen Merkmals unter Mitwirkung des Betroffenen handelt es sich hierbei um nicht-kooperative Vorgänge, die dem Betroffenen womöglich nicht einmal bewusst sind. Dafür sind Merkmale geeignet, die kontaktlos und über eine gewisse Distanz erfasst werden können. Dies trifft zurzeit vor allem auf die Gesichtserkennung zu, die bei geeignetem Blickwinkel mittels gewöhnlicher Kameras erfolgen kann. Da es datenschutzrechtlich geboten ist, sensitive Daten nur in Kenntnis der Betroffenen zu erheben, sind nicht-kooperative passive Systeme abzulehnen.

Demgegenüber ist die flächendeckende Erfassung des Fingerabdrucks oder der Handgeometrie ohne Wissen und Mitwirkung des Betroffenen nicht oder nur unter sehr großem Aufwand möglich. Zwar können Fingerabdrücke auch heimlich von berührten Gegenständen abgenommen werden. Dies eignet sich jedoch - wegen des hierfür erforderlichen Aufwands - nur zur Behandlung von Einzelfällen und ist daher mit einer Überwachung nicht vergleichbar.

8 Ergebnis

Im Ergebnis zeigt sich, dass keines der weiteren biometrischen Merkmale unproblematisch ist. Vor der Entscheidung, ob ein bestimmtes biometrisches Merkmal in Ausweise aufgenommen werden soll, müssen die verschiedenen Risiken daher sorgfältig gegeneinander abgewogen werden.

Vor der gesetzlichen Einführung neuer biometrischer Merkmale ist eine Evaluation durch einen Großversuch geboten. Dabei wären Ausweise mit zusätzlichen Sicherheitsmerkmalen (z. B. Hologramm) ohne biometrische Merkmale zu erproben und zu bewerten und mit Ausweisen zu vergleichen, die ebenso ausgestaltet sind, jedoch biometrische Merkmale enthalten. Zu prüfen wäre auch, wie hoch das Risiko für Bürgerinnen und Bürger wäre, wegen Gerätedefekten bei hard- oder softwaregestützter Erkennung der Merkmale bzw. wegen statistisch zu erwartenden Falscherkennungen bei der Ausweiskontrolle trotz eines echten eigenen Ausweises aufgehalten und intensiver überprüft zu werden, als sonst notwendig.

14.8 Verschwundene Diskette mit Einwohnermeldedaten bei der Rasterfahndung

Ein Journalist teilte mir mit, dass im Zusammenhang der Rasterfahndung eine von einer Kommunalverwaltung gefertigte Diskette mit Einwohnermeldedaten offenbar auf dem

Postweg zum Landeskriminalamt verschwunden sei. Nachforschungen bestätigten den Sachverhalt. Das LKA hatte wegen der Eilbedürftigkeit der Rasterfahndung keine zusätzlichen Sicherheitsanforderungen zum Datenträgerversand festgelegt. Daraufhin hat die Kommune eine verschlüsselte Diskette auf dem Postweg an das LKA gesandt, die nicht angekommen ist. Die Kopie des Datenträgerbegleitscheines lag vor.

Zur Gewährleistung des Datenschutzes haben die Meldebehörden und die Datenempfänger die erforderlichen personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes bei der Datenübermittlung zu treffen. Insbesondere sind die Maßnahmen zur Transportkontrolle (§ 9 Abs. 2 Nr. 9 SächsDSG) zu beachten, d. h. dass die Daten beim Transport nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden dürfen.
Die Versandart der Datenträger ist daher abhängig vom Gefährdungspotential auszuwählen und muss eine rechtzeitige Zustellung garantieren. Je mehr Personen mit der Beförderung befasst und je länger die Zeiten sind, in denen der Datenträger unbeaufsichtigt bleibt, desto weniger kann im allgemeinen die Vertraulichkeit und Integrität garantiert werden. Dementsprechend sind angemessene Versandarten (z. B. Deutsche Post AG, Kurierdienste, persönlicher Kurier, persönliche Übergabe) auszuwählen. Der Versand eines Datenträgers per Einschreiben mit Rückschein oder als Wertbrief könnte zwar den Transportweg nachvollziehbar machen, aber nicht verhindern, dass die Daten unbefugt zur Kenntnis genommen, kopiert, verändert und/oder missbräuchlich genutzt werden. Kryptographische Verfahren sind dabei besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern.

Die Kommune hatte löblicherweise dementsprechend gehandelt. Sie hat die Daten zur Rasterfahndung mit der PGP-Funktion „selbstentschlüsselndes Archiv“ (PGP Version 6.5) verschlüsselt, auf dem Datenträger gespeichert und per Post mit einem Datenträgerbegleitschein versandt. Zur Verschlüsselung der Meldedaten wurde vom Absender ein Kennwort vergeben. Nach der Empfangsbestätigung durch das LKA wäre dann das Kennwort übermittelt worden. Nach der Eingabe des richtigen Kennwortes hätte die Datei entschlüsselt und weiterverarbeitet werden können. Dieses Verfahren verhindert auch bei Verlust des Datenträgers eine unberechtigte Kenntnisnahme der Einwohnermeldedaten zur Rasterfahndung. Durch die Verschlüsselung der Meldedaten ist der erforderliche Datenschutz gewährleistet.

Das Landeskriminalamt Sachsen hätte als anfordernde Stelle wegen des besonderen Verwendungszusammenhangs der Daten - (trotz der hohen Eilbedürftigkeit) - auch ausreichende Datenschutzmaßnahmen für den Transportweg fordern und vor allem selbst realisieren müssen. Dies ist ein Verstoß gegen § 9 SächsDSG. Da dies jedoch ein Einzelfall war, bei dem auf Grund der von der Kommune getroffenen Maßnahmen kein Schaden eingetreten ist, und das LKA seit dem Vorfall nur Kuriere

für die Abholung einsetzt sowie an einer Anweisung zur sicheren Übermittlung von Meldedaten arbeitet, habe ich nach § 26 Abs. 2 SächsDSG von einer Beanstandung abgesehen.

14.9 Löschen personenbezogener Daten auf Datenträgern

Falls eine Gemeindeverwaltung ein neues EDV-System einführt und die bisher eingesetzten und noch funktionsfähigen PCs wirtschaftlich verwerten möchte, so muss sie die gespeicherten Daten löschen. Dabei ist bloßes Löschen der Festplatte mit Löschbefehlen der meisten Betriebssysteme nicht ausreichend, weil nur der Verzeichniseintrag des Dateinamens gelöscht wird, d. h., der Speicherplatz, auf dem die Datenblöcke mit vertraulichen Daten weiterhin gespeichert bleiben, wird als wieder verwendbar gekennzeichnet.
Die „gelöschten" Daten könnten mit geeigneten Tools (z. B. Diskmonitor, DOS-Befehl: UNDELETE) wiederhergestellt werden, solange der Plattenbereich nicht mit anderen Daten überschrieben wurde. Die wiederhergestellten Dateien könnten dann von den neuen Nutzern unbefugt zur Kenntnis genommen und missbräuchlich genutzt werden.

Um dieses zu verhindern, sollten die Daten auf der Festplatte und auf anderen magnetischen Datenträgern durch mehrfaches Überschreiben mit einer zufälligen Zeichenfolge oder durch Neuformatieren (z. B. für Disketten unter DOS mit FORMAT A: /U) gelöscht werden. Die Datenträger können auch durch physisches Zerstören (z. B. Zerkleinern, Einschmelzen) vernichtet und damit auch gelöscht werden. Letzteres ist auch für nur einmal beschreibbare Datenträger (z. B. CD-Rs) anwendbar.

Welche Methode gewählt werden sollte, ist vom Schutzbedarf der Daten abhängig und von der Entscheidung, ob eine Weiterverwendung der Datenträger oder PCs möglich ist.

Zum unwiderruflichen Löschen können auch die Löschfunktionen von Dienstprogrammen wie z. B. BCWipe, Cryptext, Eraser und PC Inspector™ dienen. Ein Teil dieser Löschprogramme kann als Freeware (kostenlose Software) aus dem Internet geladen werden. Diese Löschprogramme unterstützen Betriebssysteme wie Windows 95/ 98/ NT/ 2000 und Windows ME. Außerdem kann mit dem DOS-Befehl: COPY NUL *dateiname.erw* die Datei überschrieben werden. Mit UNDELETE lässt sich diese Datei zwar wiederherstellen, aber sie ist nun leer.
Dienstprogramme wie Norton Utilities (WipeInfo) oder PC Tools (Wipe) können ebenfalls Dateien unwiderruflich löschen.
Zu beachten ist jedoch, dass ein sicherer Löschvorgang erst nach mehrfachem Überschreiben der Daten erreicht wird. In der Fachliteratur wird mindestens ein

zweimaliges, besser aber ein drei- bis siebenmaliges Überschreiben mit einem Bit-Muster empfohlen.

Weitere Hinweise zum sicheren Löschen können dem IT-Grundschutzhandbuch 2001 des Bundesamtes für Sicherheit in der Informationstechnik und den folgenden Informationen entnommen werden:

- Auf der Homepage des unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (www.datenschutzzentrum.de) wird unter der Rubrik „Datenschutz und Technik“ über eine Begutachtung der Löschprogramme BCWipe und Cryptext, sowie über rückstandsloses Löschen von Dateien mit dem Programm PGP informiert.
- Nach einem Testurteil der Zeitschrift PC WELT vom September 2000 sei das Programm Eraser (Freeware) einfach zu bedienen und lösche nachhaltig Dateien und Verzeichnisse durch mehrfaches Überschreiben.
- Unsere Datenschutzbehörde nutzt PGP Version 6.5.1 u.a. auch zum sicheren Löschen von Dateien und von Altdaten auf freien Speicherplätzen der Laufwerke. Der Löschbefehl ist einfach zu bedienen. Die zu löschende Datei wird im Explorer mit der rechten Maustaste ausgewählt. Aus den PGP-Menüpunkten wird der Löschbefehl gewählt und nochmals bestätigt, dass die angezeigte Datei unwiederherstellbar gelöscht werden soll. Mit PGPtools (Bestandteil von PGP) kann auch der freie Speicherplatz auf Laufwerken gelöscht werden. Die Anzahl der auszuführenden Durchläufe (max. 26) kann vom Benutzer festgelegt werden. Je mehr Durchläufe ausgeführt werden, desto sicherer werden die alten ungültigen Daten von der Festplatte gesäubert. Für den Dienstgebrauch dürften 3 bis 10 Durchläufe ausreichend sicher sein.

14.10 Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten, erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1. Einleitung

In den letzten Jahren hat sich die Informationstechnologie sehr schnell weiterentwickelt. Dies gilt insbesondere im Bereich der Vernetzung und der offenen Kommunikationssysteme. Die verstärkte Nutzung neuer Kommunikationsformen, wie z. B. E-Mail, erfordert eine neue Art der Verbreitung der Kommunikationsadressen. Hierzu werden zunehmend elektronische Verzeichnisse eingesetzt. Da auf die Informationen in diesen Verzeichnissen von verschiedenen Stellen aus direkt zugegriffen werden kann und insbesondere beliebige Informationen gespeichert werden können, geht die Funktionalität weit über die bisherigen Möglichkeiten eines

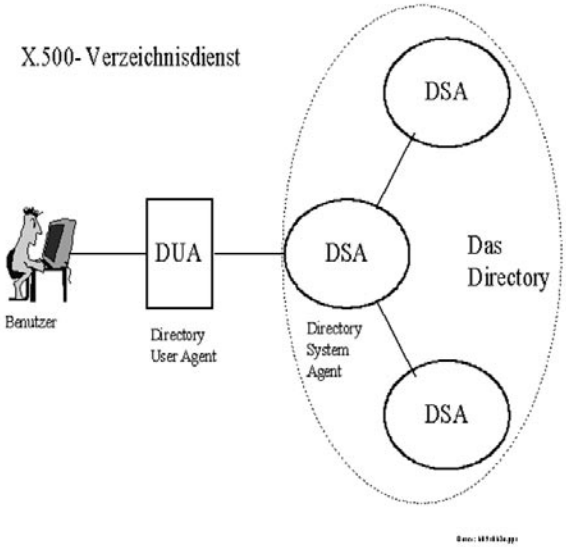
in Papierform vorliegenden Adress- und Telefonverzeichnisses hinaus. Hieraus ergibt sich die Notwendigkeit, daß von der datenverarbeitenden Stelle festgelegt werden muss, welche Daten im Verzeichnis gespeichert werden.
Zum Einsatz kommen sowohl ISO-konforme (X.500) Systeme als auch Industriestandards (z. B. Network Directory System, NDS). Da in einem Verzeichnisdienst auch personenbezogene Daten gespeichert werden können, ist die Betrachtung datenschutzrechtlicher Aspekte notwendig. Im Verzeichnisdienst existieren verschiedene datenschutzrechtliche Probleme. Diese betreffen zum einen technische Aspekte, wie z. B. die sichere Übertragung personenbezogener Daten, zum anderen rechtliche Aspekte, wie Inhalt, Form und Zugriff auf Einträge. Im Vordergrund steht dabei, daß schutzwürdige Belange der verzeichneten Personen nicht beeinträchtigt werden.
Diese Empfehlung befasst sich mit den Möglichkeiten des datenschutzgerechten Einsatzes von Verzeichnisdiensten.
Sie basiert auf dem Betrieb eines Verzeichnisdienstes in einer definierten *Netzwerkumgebung (Intranet) innerhalb der öffentlichen Verwaltung***.** Die intranetübergreifende Verbindung mehrerer Verzeichnisse, z. B. über das Internet, wird nicht betrachtet.
Des Weiteren wird die generelle Problematik der Systemverwaltung der beteiligten Rechnersysteme auch nicht mit einbezogen, da diese unabhängig von Verzeichnisdiensten sind.

2. Verzeichnisdienste

2.1 Verzeichnisdienst: X.500

X.500 (ISO-9594) ist ein von der Comité Consultatif International Télégraphique et Téléphonique (CCITT) und der International Standardization Organization (ISO) erarbeiteter Standard, der einen global verteilten Verzeichnisdienst - *den Verzeichnisdienst* - beschreibt. Er kann als ein in vielen Aspekten erweitertes elektronisches Telefonbuch, dass neben Telefonnummern auch andere Kommunikationsadressen, wie z. B. E-Mail-Adressen, enthält, betrachtet werden. Darüber hinaus können relativ beliebige Informationen über Organisationen, deren Mitarbeiter, Rechner, Peripheriegeräte und verfügbare Dienste, also das gesamte Spektrum aller im Kontext von vernetzten Computer- und Kommunikationssystemen vorkommenden Elementen, enthalten sein.
Die Benutzer des Directory-Systems können sowohl menschliche Benutzer als auch Anwendungsprogramme sein. Bei der Interaktion mit dem Directory greift der Benutzer über einen *Directory User Agent* (DUA) auf die Directory-Informationen zu. Dabei sieht die Verzeichnisnorm das *Directory Access Protocol* (DAP) als Zugangsprotokoll vor. Aufgrund der Komplexität hat sich dieses allerdings am Markt nicht durchgesetzt, sondern wurde teilweise (insbesondere in den Endgeräten)

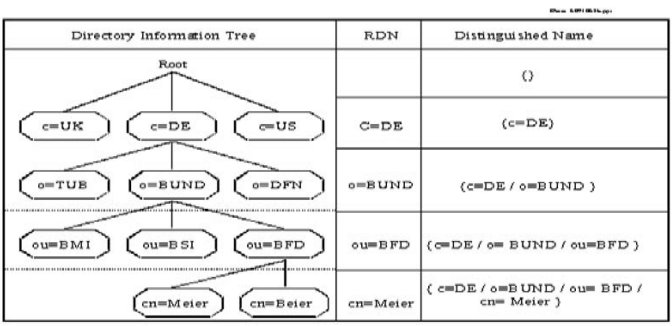
durch das *Lightweight Directory Access Protocol (LDAP)* als stark vereinfachtes Zugriffsprotokoll ersetzt.
Das Directory besteht aus mehreren kooperierenden *Directory System Agents* (DSA), die auf verschiedenen Rechnern realisiert sein können.*



Die Informationen, die das Verzeichnis bereitstellt, sind physikalisch über die DSAs verteilt, erscheinen jedoch für den Benutzer als eine logische Datenbasis. Die Gesamtheit aller Informationen über Objekte, die im Verzeichnis bekannt sind, wird als *Directory Information Base* (DIB) bezeichnet. Jedes Objekt wird darin durch einen Verzeichnis-Eintrag repräsentiert, der die für das Objekt relevanten Daten enthält. Die Einträge der Datenbasis sind hierarchisch angeordnet. Die logische Sicht auf die Datenbasis erscheint als Baumstruktur.** Diese Baumstruktur bildet die Grundlage einer eindeutigen Namensgebung innerhalb des Verzeichnisses. Die Namen der Einträge werden gemäß einer mehrstufigen hierarchischen Namenskonvention gebildet. Ein Directory-Name (*Distinguished Name - DN*) setzt sich aus einer geordneten Folge einzelner Komponenten (*Relative Distinguished Name - RDN*) zusammen.

* Für die Kommunikation innerhalb des Directory-Systems wird das Directory System Protocol (DSP) verwendet.

** Die Directory Information Base stellt sich somit als Directory Information Tree (DIT) dar.



Die Namen von Einträgen der DIB sind eindeutig, d. h., jeder Name bezeichnet genau ein Objekt. Dieses wird dadurch erreicht, daß jede Namensgeberautorität (naming authority) innerhalb einer Hierarchiestufe unterschiedliche RDNs verwendet.
Jeder Eintrag im Directory besteht aus mehreren Informationen (Attributen). Ein Attribut wird durch einen Attributtyp und einen bzw. mehreren Attributwerte definiert. Ein Beispiel hierfür ist ein Personeneintrag der folgendes Aussehen haben könnte:

Name des Eintrags (DN): {c=DE / o=BUND / ou=BFD / cn=Meier}

Attributtyp	Attributwert(e)
Name	Meier
Nachname	Meier
Postanschrift	Musterstr, 1000 Musterstadt
Telefonnummer	+49 099 12345678 +49 099 11223344
Faxnummer	+49 230 99999999
Email	mzn@muster.de
favourite drink	Sekt extra dry

Die im Verzeichnis gespeicherten Daten müssen gegen unautorisierten Zugriff geschützt werden. Hierzu wurde in der Norm X.509 die Sicherung der im Verzeichnis durchgeführten Kommunikation beschrieben. Die dargestellten Verfahren unterscheiden zwischen schwacher und starker Authentifizierung. Die schwache Auth entifizierungsprozedur basiert auf dem eindeutigen Namen (DN) und einem Passwort. Die starke Authentifizierung arbeitet mit einem asymmetrischen Kryptosystem (z.B. dem RSA-Algorithmus). Für die Zugriffskontrolle existiert ein generelles Zugriffskontroll-Modell, das die Anwendung einer bestimmten Sicherheitspolitik (security policy), die jedoch nicht durch das Verzeichnis vorgeschrieben wird, erlaubt.

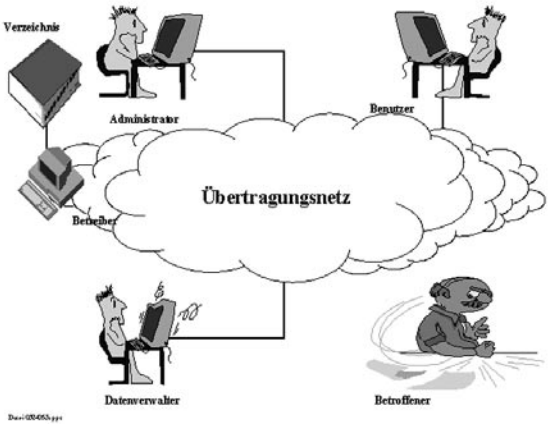
Als Basis wird ein Zugriffskontroll-Schema definiert, das auf Zugriffskontroll-Listen (Access Control Lists, ACL) basiert. Über die Zugriffskontroll-Listen wird festgelegt, wer auf welche Daten in einem Eintrag in welcher Weise (beispielsweise lesend, schreibend) zugreifen kann. Die Normung des Zugriffskontrollmechanismus erfolgte im X.500-Standard erst 1993.

2.2 Network Directory System (NDS)

Das Network Directory System (NDS) ist ein von Novell entwickelter Verzeichnisdienst. Es wurde als verteilte Datenbank konzipiert und ist für die Verwaltung von Netzwerken geeignet. NDS verwaltet Informationen über alle Komponenten im Netzwerk, z.b. Benutzer, Benutzergruppen und Drucker. Ein NDS-Objekt besteht aus einer Vielzahl von Informationen - Properties genannt - und den dazugehörenden Daten, die diese Properties haben können. Es existieren Objekte mit deren Hilfe eine Baumstruktur ähnlich wie bei X.500 aufgebaut werden kann. Für jedes Objekt können Zugriffsberechtigungen vergeben werden. Dieses wird über Access Control Lists realisiert. Die Funktionalität von NDS umfasst weniger die Bereitstellung der Telefonbuchfunktionalität, sondern eher die Verwaltung von allen Objekten in großen Netzwerken.

3. Komponenten und Beteiligte

Ein Verzeichnisdienst stellt in der Regel nur eine Unterstützungsfunktion innerhalb eines anderen Verfahrens oder Dienstes bereit, beispielsweise die Bereitstellung von Kommunikationsadressen, Telefonnummern und öffentliche Schlüssel bei der Telekommunikation. Allerdings sind auch Lösungen vorstellbar, in denen die Verzeichnisdienste die Verwaltung und Organisation von anderen Datenbeständen übernehmen. In der Regel werden heute Verzeichnisdienste zur Verwaltung der



Objekte in großen Netzwerken (Intranet) eingesetzt (Administration). In beiden Fällen werden für den Betrieb des Dienstes gewisse Grundkomponenten - ein Übertragungsnetz, Knotenrechner, eine verteilte Datenbank etc. - benötigt. Auch treten in allen Fällen die gleichen Beteiligten auf, die entweder den Betrieb des Verzeichnisses sicherstellen oder als Betroffener mitwirken.

4. Problemdarstellung Datenschutz

In Verzeichnisdiensten wird der eindeutige Teilnehmername (Distinguished Name, DN) definiert. Dieser Name dient als Adresse im Verzeichnis, mit der Personen gefunden werden können. Um das Verzeichnis in einer benutzerfreundlichen Weise zu organisieren, wird zur Identifizierung eine Kette von Namen und Namensteilen verlangt. Dies führt dazu, daß eine Person eindeutig identifiziert werden kann. In Verbindung mit der Möglichkeit beliebige Informationen zu einer Person zu speichern, erwachsen hieraus besondere datenschutzrechtliche Gefahren. Hierbei ist insbesondere die einfache Zusammenführung bisher getrennt gespeicherter Daten zu sehen. Die Verbindung von verteilt vorliegenden Informationen und eventuell existierender Kopien (Repliken) kann zu Problemen hinsichtlich der Aktualität der Daten führen.* Dies stellt insbesondere für die datenschutzrechtlichen Anforderungen bei der Berichtigung und Löschung ein Problem dar.

Darüber hinaus bieten sich zudem noch Verknüpfungsmöglichkeiten mit anderen elektronisch vorliegenden Daten, z. B. Telefonbuch auf CD-ROM, Adressbuch auf CD-ROM etc. Dieses ermöglicht die Erstellung von sehr detaillierten Profilen, deren Umfang nicht absehbar ist.
Üblicherweise wird der Verzeichnisdienst als Unterstützungsfunktion in bestehende Verfahren integriert. Damit muss sichergestellt sein, daß der Zugriff auf Informationen in Einträgen nur auf das für die Aufgabenerledigung Notwendige beschränkt wird.

Gefahren für das informationelle Selbstbestimmungsrecht erwachsen auch aus dem komplexen Zusammenspiel der verschiedenen Komponenten, die für den Betrieb des Verzeichnisdienstes benötigt werden. Jede Komponente für sich ist dabei einer Vielzahl von Bedrohungen ausgesetzt. Für jede einzelne Komponente kann dabei von den üblichen Bedrohungspotentialen ausgegangen werden, z. B. Manipulation der Einträge auf den Telekommunikationsleitungen, Zugriffe Unberechtigter (Mithören), Zerstörung der Infrastruktur, Einspielen alter Versionen des Dienstes, Virenbefall

* Die Möglichkeit der Replikationen ist wesentlicher Bestandteil der Funktionalität eines Verzeichnisdienstes

etc.
Neben diesen allgemeinen Bedrohungen gibt es allerdings auch verzeichnisspezifische. Das Bedrohungspotential ist abhängig vom Verbreitungsgrad und den Zugriffsmöglichkeiten auf die Inhalte. Ein Beispiel ist die Einführung eines Verzeichnisdienstes in einem Intranet, in dem nur die Adressdaten der Mitarbeiter aufgenommen wurden und das ausschließlich zur Verbesserung der internen Kommunikation dienen soll. Die Verbreitung der Adressen über das eigene Netz hinaus ist nicht vorgesehen. Damit ist das Verzeichnis als eine Art "hausinternes elektronisches Telefonbuch" zu bewerten. Die Bedrohung ist als sehr gering zu bewerten.

Verzeichnisdienste können durch Nutzung von systemimmanenten Replikationsmechanismen oder durch automatisiertes Abfragen zur Bildung von zeitabhängigen Profilen missbraucht werden. Dies sollte vor allem bedacht werden, wenn Verzeichnisdienste bereitgestellt werden, da die Auswerteverfahren und –werkzeuge dann nicht kontrollierbar sind.

4.1 Rechtliche Einordnung von Verzeichnisdiensten

Soweit Verzeichnisdienste nur im Intranet einer datenverarbeitenden Stelle angeboten werden, handelt es sich weder um einen Tele- noch einen Mediendienst. Es liegt somit kein „Angebot" i. S. d. §§ 2 Abs. 2 TDG bzw. MDSTV vor. Die Zulässigkeit derartiger Verzeichnisdienste richtet sich daher allein nach den allgemeinen datenschutzrechtlichen Bestimmungen für Dienst- und Arbeitsverhältnisse.

Wird der Verzeichnisdienst als Basis von Personalinformationssystemen genutzt oder gar ausgebaut, ist der Personalrat (und im Bereich der Privatwirtschaft der Betriebsrat) aufgefordert, durch Nutzung seiner Mitbestimmungsrechte und Abschluss von Dienst- und Betriebsvereinbarungen die Zusammenführung von Daten zu unterbinden bzw. zu kontrollieren.

4.2 Veröffentlichung von Klarnamen

Grundsätzlich sollte allen Bediensteten, die keine herausgehobene Funktion innehaben, ein Wahlrecht dahin gehend eingeräumt werden, ob sie mit ihrem Klarnamen oder mit einem selbstgewählten Pseudonym in ein über das Intranet abrufbares Verzeichnis eingestellt werden wollen. Dieses Modell könnte auch genutzt werden, um die Zusammenführung von verschiedenen Verzeichnissen zu unterbinden, wenn der Betroffene verschiedene rollenspezifische Pseudonyme wählt. Auf diese Weise könnten auch die Risiken einer unkontrollierten Sammlung personenbezogener Informationen durch Suchmaschinen begrenzt werden.

4.3 Beschäftigtendaten in Verzeichnisdiensten

Die Verarbeitung von Personaldaten ist im Bund und in den Ländern unterschiedlich geregelt. Zum Teil enthalten die allgemeinen Datenschutzgesetze einschlägige Bestimmungen, zum Teil wird die Verarbeitung in den Beamtengesetzen angesprochen, wobei einige Landesbeamtengesetze diese Regelungen im Tarifbereich für entsprechend anwendbar erklären. Das Bundesbeamtengesetz (BBG) enthält keine umfassenden Vorschriften über die Verarbeitung von Personaldaten, sondern lediglich Regelungen über die Datenerhebung und den Umgang mit Personalaktendaten. Inhaltlich stimmen alle Regelungen darin überein, daß Beschäftigtendaten verarbeitet werden dürfen, wenn dies u. a. zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.
Soweit auf den Verzeichnisdienst nur Mitarbeiter der eigenen Verwaltung zugreifen können, dürfen die erforderlichen Angaben über sämtliche Mitarbeiter zur Verfügung gestellt werden. Erstreckt sich die Zugriffsmöglichkeit auch auf andere Stellen im jeweiligen Bundesland, dürfen Familienname, dienstliche Telefonnummer und Hinweise auf den Aufgabenbereich von solchen Personen in den Verzeichnisdienst aufgenommen werden, die den Anschluss aus dienstlichen Gründen nutzen müssen und bei denen die Erreichbarkeit zu ihrer dienstlichen Aufgabe gehört.

Unterschiedlich ist die Frage zu beurteilen, ob über diese Angaben hinaus die Amtsbezeichnung oder der Vorname in den Verzeichnisdienst eingestellt werden darf. Hier greifen unterschiedliche Regelungen in den einzelnen Bundesländern, so dass auf die gültige Rechtslage verwiesen wird.

Für Bedienstete, die in der Regel keinen unmittelbaren Kontakt außerhalb der eigenen Dienststelle haben (z. B. Angehörige interner Dienste, wie des Schreib- oder Botendienstes), ist die Bekanntgabe ihrer Daten nicht erforderlich. Deren Aufnahme in den Verzeichnisdienst wäre -C:\Lnxwork\0007119-2000.Doc soweit er über ein internes Verzeichnis hinaus geht - nur mit Einwilligung zulässig. Landesrechtliche Besonderheiten sind zu berücksichtigen.

Soweit die Auffassung vertreten wird, dass Name, Dienst-, Funktionsbezeichnung und Organisationseinheit von Bediensteten wegen ihres engen Bezuges zur amtlichen Tätigkeit nicht deren grundsätzlicher Verfügungsbefugnis und damit ihrem Recht auf informationelle Selbstbestimmung unterfallen (Amtswaltertheorie), ergeben sich keine anderen Ergebnisse.

Das Erfordernis, die genannten Daten für dienstliche Zwecke einzusetzen, dürfte sich regelmäßig auf das jeweilige Bundesland beschränken. Bei einer über den Landesbereich hinausgehenden Bereitstellung von Daten, beispielsweise bei einer

Verbindung zweier öffentlicher Netze, empfiehlt sich – wie allgemein in Zweifelsfällen – der Abschluss einer Dienstvereinbarung.

5. Maßnahmen

Aus datenschutzrechtlicher Sicht sind beim Betrieb eines Verzeichnisdienstes technische und organisatorische Maßnahmen vorzunehmen, die geeignet sind, den aufgeführten Gefahren und Bedrohungen entgegenzuwirken.
Für die Komponenten, auf die der Verzeichnisdienst aufsetzt, sind hinreichende und angemessene technische und organisatorische Datenschutzmaßnahmen zu realisieren. Allgemeine Empfehlungen finden sich in entsprechenden Orientierungshilfen (z. B. Unix-Systeme, PCs, Mail-Systeme oder Datenträger) oder auch im BSI-Grundschutzhandbuch, UNIX-Leitfaden des Hamburger Datenschutzbeauftragen und Checklisten des Landesbeauftragten für den Datenschutz in Niedersachsen.

Über die grundlegenden Maßnahmen hinaus ist beim Einsatz von Verzeichnisdiensten folgendes zu beachten:

- Der Verzeichniseintrag ist auf die notwendigen Angaben zu beschränken, beispielsweise E-Mail-Adresse, Telefonnummer, Fax-Nummer, Öffentliche Schlüssel etc. Andere Information wie beispielsweise Hinweise auf Zuständigkeiten, Aufgaben-bereiche, Tätigkeitsfelder, Arbeitszeiten, Örtlichkeiten etc. sollten, soweit nicht für die Aufgabenerledigung notwendig, nicht in das Verzeichnis aufgenommen werden.
- Die Zugriffsregelungen sind so eng wie möglich fassen. Die Verantwortung hierzu muss eindeutig und durch eine hierfür verantwortliche Stelle vorgenommen werden. Grundsätzlich sollten starke Authentifizierungsmechanismen (Digitale Signatur, biometrische Verfahren) zum Einsatz kommen (siehe Kapitel 2.1). Produkte, die lediglich dem X.500-Standard entsprechen, sind nicht einzusetzen.
- Die Organisation des Verzeichnisdienstes muss so gestaltet werden, dass sicherstellt ist, dass die Einträge des Verzeichnisdienstes immer in möglichst zeitnaher Aktualität vorliegen. Dies schließt auch Kopien des Verzeichnisses (Repliken) ein.
- Die Neueinrichtung, Änderung und Löschung von Verzeichniseinträgen sowie die Erstellung und Verbreitung von Repliken sind zu Zwecken der Revision und Datenschutzkontrolle zu protokollieren. Sofern die Protokollierung kein Bestandteil des Produkts ist, muss eine ausreichende Protokollierung durch andere Komponenten, beispielsweise das Betriebssystem, sichergestellt werden.
- Es ist zu prüfen, zu welchen Personen Angaben im Verzeichnisdienst zur Verfügung gestellt werden dürfen.
- Der Verzeichniseintrag ist auf die Angaben zu beschränken, die in der ausgeübten Funktion für die Nutzer des Verzeichnisses relevant sind.

- Vor „Veröffentlichung“ des Eintrags im Verzeichnis müssen dem Betroffenen die Daten des Eintrags zur Einsichtnahme und/oder Korrektur vorgelegt werden. Anhand von Attributen ist eine Filterung der Verzeichniseinträge nach dem Gesichtspunkt der internen/externen Bereitstellung zu ermöglichen, oder die Möglichkeit zu schaffen, dass die Betroffenen selbst eine Sperrung oder Freischaltung bestimmter Attribute vornehmen können.
- Zur Sicherung der Integrität sind bei der Übertragung grundsätzlich kryptographische Verfahren einzusetzen. Ist die Vertraulichkeit von Verzeichnisdaten zu gewährleisten, z. B. bei Abfragen oder Replikation über unsichere Leitungen, so sind auch hierfür geeignete kryptographische Methoden zu benutzen. Dazu stehen auch Werkzeuge außerhalb des Verzeichnisdienstes (etwa zur Verbindungsverschlüsselung) zur Verfügung.

15 Vortrags- und Schulungstätigkeit

In diesem Jahr nicht belegt.

16 Materialien

16.1 Entschließung zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Anlasslose DNA-Analyse aller Männer verfassungswidrig

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den Vorschlag zurück, den „genetischen Fingerabdruck“ aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potenzielle Straftäter behandelt, ist verfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

16.2 Entschließung zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Veröffentlichung von Insolvenzinformationen im Internet

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen - vor allem in Verbraucherinsolvenzverfahren - künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, aufgrund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde,

gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 9. März 1988 - 1 BvL 49/86 - zu einem vergleichbaren Sachverhalt einbezogen werden.
Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckun gsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

16.3 Entschließung zwischen der 61. und 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Entwurf der Telekommunikations-Überwachungsverordnung

Das Bundesministerium für Wirtschaft und Technologie hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung (TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Betriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technische Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße „Surfen“ zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine

Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

16.4 Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z. B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese

verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

16.5 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster zur gesetzlichen Regelung von genetischen Untersuchungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung – in der Strafprozessordnung bereits normiert – sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;

- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Anlage zu der Entschließung

Vorschläge zur Sicherung der Selbstbestimmung bei genetischen Untersuchungen

Allgemeines

Gegenstand

Zu regeln ist die Zulässigkeit genetischer Untersuchungen beim Menschen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten. Neben allgemeinen Regelungen sind besondere Bestimmungen zu genetischen Untersuchungen
1. zu medizinischen Zwecken
2. im Zusammenhang mit Arbeits- und Versicherungsverhältnissen
3. zur Abstammungsklärung und Identifizierung außerhalb der Strafverfolgung
4. zu Forschungszwecken

zu treffen.

Ziel, Benachteiligungsverbot

(1) Ziel der Regelungen ist der Schutz der Menschenwürde, der Persönlichkeit und der informationellen Selbstbestimmung der Betroffenen bei genetischen Untersuchungen.
(2) Niemand darf wegen seiner Erbanlagen oder wegen der Weigerung, eine genetische Untersuchung bei sich durchführen zu lassen, benachteiligt werden.

Begriffe

1. *Genetische Untersuchungen:* Untersuchungen auf Chromosomen-, Genprodukt- oder molekularer DNS / RNS-Ebene, die darauf abzielen, Informationen über das Erbgut zu erhalten;
2. *Prädiktive Untersuchungen:* vor- oder nachgeburtliche genetische Untersuchungen mit dem Ziel, Erbanlagen einer Person, insbesondere Krankheitsanlagen vor dem Auftreten von Symptomen oder einen Überträgerstatus, zu erkennen;
3. *Überträgerstatus:* Erbanlagen, die erst in Verbindung mit entsprechenden Erbanlagen eines Partners oder einer Partnerin eine Krankheitsanlage bei den gemeinsamen Nachkommen ausbilden.
4. *Pränatale Untersuchungen:* vorgeburtliche genetische Untersuchungen mit dem Ziel, während der Schwangerschaft Informationen über das Erbgut des Embryos oder des Fötus zu gewinnen;
5. *Reihenuntersuchung:* genetische Untersuchungen, die systematisch der gesamten Bevölkerung oder bestimmten Gruppen der Bevölkerung angeboten werden, ohne dass bei den Betroffenen Anhaltspunkte dafür bestehen, dass die gesuchten Erbanlagen bei ihnen vorhanden sind;
6. *Diagnostische genetische Untersuchungen:* genetische Untersuchungen zur Abklärung der Diagnose einer manifesten Erkrankung oder zur Vorbereitung oder Verlaufskontrolle einer Behandlung;
7. *Probe:* die für eine genetische Untersuchung vorgesehene oder genutzte biologische Substanz;
8. *Genetische Daten:* im Zusammenhang mit genetischen Untersuchungen erlangte Informationen über eine Person;
9. *Betroffene Person:* die Person, von der eine Probe vorliegt oder deren genetische Daten erhoben, verarbeitet oder genutzt werden; bei pränatalen Untersuchungen auch die schwangere Frau.
10. *Verarbeiten:* das Speichern, Verändern, Übermitteln, Sperren und Löschen erhobener personenbezogener genetischer Daten.

Zulässigkeit genetischer Untersuchungen

Genetische Untersuchungen, der Umgang mit Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten bedürfen der freiwilligen, schriftlichen Einwilligung der betroffenen Person nach Aufklärung. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen zu regelnden und in der Strafprozessordnung geregelten Ausnahmen.

Zulassung zur Durchführung genetischer Untersuchungen

(1) Wer genetische Untersuchungen durchführen will, bedarf hierfür der Zulassung

durch die zuständige Aufsichtsbehörde des Landes.

(2) Die Zulassung wird erteilt, wenn Gewähr dafür besteht, dass
- die Untersuchungen und ihre Auswertungen sorgfältig und nach dem Stand von Wissenschaft und Technik durchgeführt werden,
- die Regelungen gemäß diesen Vorschlägen eingehalten, insbesondere Information und Beratung der betroffenen Person und die Datensicherheit gewährleistet werden und
- in der antragstellenden Person die berufsrechtlichen und gewerberechtlichen Voraussetzungen vorliegen.

(3) Das Nähere regelt die Bundesregierung durch Rechtsverordnung.

Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen

Genetische Testverfahren dürfen nur für den Gebrauch durch Ärztinnen, Ärzte oder Labors eingeführt oder in Verkehr gebracht werden. Das öffentliche Angebot, genetische Untersuchungen zu medizinischen Zwecken ohne individuelle Beratung der betroffenen Person durchzuführen, ist unzulässig. Die Berufsfreiheit, Artikel 12 Absatz 1 Satz 2 Grundgesetz, wird insoweit eingeschränkt.

Zweckbindung

Die für die genetische Untersuchung vorgesehene oder genutzte Probe und die genetischen Daten dürfen nur für den Zweck verwandt und für die Dauer aufbewahrt werden, zu denen die betroffene Person ihre Einwilligung erklärt hat oder zu denen ein Gericht oder eine Verwaltungsbehörde eine Anordnung getroffen hat. Vorbehalten bleiben die in einem Gesetz über genetische Untersuchungen geregelten Ausnahmen.

Datensicherheit

(1) Proben und genetische Daten sind vor dem Zugriff unbefugter Dritter wirksam zu schützen. Dies gilt auch in Bezug auf Mitarbeiterinnen und Mitarbeiter der untersuchenden und datenverarbeitenden Stelle, die an der genetischen Untersuchung, Aufklärung und Beratung nicht beteiligt sind oder waren.
(2) Genetische Daten sind von anderen Datenarten gesondert zu speichern.
(3) Im Übrigen gilt hinsichtlich der genetischen Daten die Bestimmung des Bundes datenschutzgesetzes über die technischen und organisatorischen Maßnahmen der Datensicherheit in der jeweils geltenden Fassung.

Einsichts- und Auskunftsrecht

Die betroffene Person hat das Recht, unentgeltlich Einsicht in die Dokumentationen zur genetischen Untersuchung einschließlich Aufklärung und Beratung zu nehmen und Auskunft über die zu ihr gespeicherten Daten zu verlangen.

Genetische Untersuchungen zu medizinischen Zwecken

Grundsatz

(1) Zu medizinischen Zwecken dürfen prädiktive Untersuchungen nur durchgeführt werden,
wenn sie nach ärztlicher Indikation der Vorsorge, der Behandlung oder der Familienplanung der betroffenen Person dienen.
(2) Eine genetische Untersuchung zum Erkennen eines Überträgerstatus ist nur zu Zwecken der konkreten Familienplanung zulässig.
(3) Für diagnostische genetische Untersuchungen gelten nur die Anforderungen gemäß dem Arztvorbehalt (siehe unten) und an diagnostische genetische Untersuchungen bei behinderten Personen (siehe am Ende dieses Abschnitts).

Pränatale Untersuchungen

Pränatale Untersuchungen sind auf das Erkennen solcher Krankheiten zu richten, die vorgeburtlich behandelt werden können. Für darüber hinausgehende genetische Untersuchungen gelten die Richtlinien der Bundesärztekammer zur pränatalen Diagnostik. Das Geschlecht darf gezielt nur zu medizinischen Zwecken festgestellt werden.

Ob darüber hinaus auch schwere Behinderungen und Anlagen für schwere, nicht behandelbare Krankheiten Ziele pränataler DNA-Untersuchungen sein dürfen, muss der gesellschaftspolitischen Diskussion, der fachmedizinischen Bewertung und der Verantwortung des Gesetzgebers überlassen bleiben.

Genetische Untersuchungen bei Minderjährigen und nicht einsichtsfähigen Erwachsenen

(1) Genetische Untersuchungen bei Minderjährigen sind nur zulässig, wenn ihre Durchführung vor Erreichen der Volljährigkeit erforderlich ist, um den Ausbruch einer Krankheit zu vermeiden oder zu verzögern, eine Heilung oder Verlaufsmilderung zu erreichen oder spätere besonders belastende Untersuchungen zu vermeiden. Bei Aufklärung, Beratung und Einwilligung (siehe unten) ist die Einsichtsfähigkeit der betroffenen minderjährigen Person zu berücksichtigen.
(2) Prädiktive Untersuchungen bei nicht einsichtsfähigen Erwachsenen dürfen sich nur auf das Erkennen von Krankheiten richten, deren Ausbruch vermieden oder verzögert oder bei denen eine Heilung oder Verlaufsmilderung erreicht werden kann. Die Einwilligung obliegt dem gesetzlichen Vertreter.

Reihenuntersuchungen

(1) Genetische Reihenuntersuchungen bedürfen der Zulassung durch die zuständige Landesbehörde.
(2) Voraussetzung für die Zulassung ist, dass
- die Reihenuntersuchung gerichtet ist auf das Erkennen von verbreiteten oder schweren Krankheiten, die unverzüglich nach dem Untersuchungsergebnis behandelt werden können, oder von Krankheiten, deren Ausbruch verhindert werden kann,
- die Untersuchungsmethode eindeutige Ergebnisse liefert,
- die Freiwilligkeit der Teilnahme und die genetische Beratung gewährleistet und
- der Datenschutz gesichert ist.

Arztvorbehalt

(1) Prädiktive Untersuchungen dürfen nur von Fachärztinnen und Fachärzten für Humangenetik veranlasst werden. Diagnostische genetische Untersuchungen dürfen auch von anderen zur Berufsausübung zugelassenen Ärztinnen und Ärzten veranlasst werden.
(2) Die veranlassende Ärztin oder der veranlassende Arzt hat die Aufklärung und Beratung (siehe nachstehend) und die Einholung und Dokumentation der Einwilligung (siehe unten) sicherzustellen.

Aufklärung und Beratung

(1) Vor und nach einer prädiktiven genetischen Untersuchung ist die betroffene Person umfassend aufzuklären und zu beraten, um ihr eine selbstbestimmte Entscheidung gemäß den Anforderungen an die Einwilligung (siehe unten) zu ermöglichen.
(2) Die betroffene Person und gegebenenfalls ihr gesetzlicher Vertreter muss insbesondere aufgeklärt werden über
- Ziel, Art, Aussagekraft und Risiko der Untersuchung und die Folgen ihrer Unterlassung;
- mögliche, auch unerwartete Ergebnisse der Untersuchung;
- mögliche Folgen des Untersuchungsergebnisses, einschließlich physischer und psychischer Belastungen der betroffenen Person oder ihrer Familie,
- Behandlungsmöglichkeiten für die gesuchte Krankheit,
- den geplanten Umgang mit der Probe und den genetischen Daten einschließlich des Orts und der Dauer der Aufbewahrung bzw. Speicherung,
- die Einflussmöglichkeiten und Datenschutzrechte der betroffenen Person,
- weitere Beratungs- und Unterstützungsmöglichkeiten.

(3) Aufklärung und Beratung dürfen nur der individuellen und familiären Situation der betroffenen Person und den möglichen psychosozialen Auswirkungen des Untersuchungsergebnisses auf sie und ihre Familie Rechnung tragen.
(4) Bei Reihenuntersuchungen kann in begründeten Ausnahmefällen die Aufklärung in standardisierter Form erfolgen, wenn zugleich die Möglichkeit einer zusätzlichen individuellen Beratung angeboten wird.
(5) Bei pränatalen Untersuchungen ist der Partner der betroffenen Frau in die Beratung einzubeziehen, sofern die Frau einwilligt. Auf Stellen der Schwangersc haftskonfliktberatung ist hinzuweisen.
(6) Bei genetischen Untersuchungen zum Erkennen eines Überträgerstatus soll der Partner oder die Partnerin der betroffenen Person in die Aufklärung und Beratung einbezogen werden.

Einwilligung

(1) Nach der Aufklärung und Beratung entscheidet die betroffene Person nach angemessener Bedenkzeit in freier Selbstbestimmung darüber,
- ob die genetische Untersuchung durchgeführt werden soll,
- welches Ziel die genetische Untersuchung hat,
- ob sie auch unvermeidbare weitere Untersuchungsergebnisse zur Kenntnis nehmen will,
- wie gegebenenfalls mit der Probe und den genetischen Daten weiter verfahren werden soll.

Soweit die betroffene Person vom Ergebnis, auf das die Untersuchung zielt, keine Kenntnis nehmen will, soll außer bei Reihenuntersuchungen grundsätzlich auf die genetische Untersuchung verzichtet werden.

(2) Die betroffene Person oder ihr gesetzlicher Vertreter hat die vorherige Aufklärung und Beratung schriftlich zu bestätigen und die Einwilligung in die genetische Untersuchung und in den vereinbarten Umgang mit der Probe und den genetischen Daten schriftlich zu erklären.
(3) Die Einwilligung kann widerrufen werden mit der Folge, dass noch nicht erfolgte Maßnahmen unterbleiben, schon vorliegende Proben vernichtet und die im Zusammenhang mit der Untersuchung erhobenen und gespeicherten Daten gelöscht werden.

Unterrichtung über das Untersuchungsergebnis

(1) Die veranlassende Ärztin oder der veranlassende Arzt teilt das Ergebnis der genetischen Untersuchung nur der betroffenen Person, bei Minderjährigen auch oder nur ihrem gesetzlichen Vertreter mit und berät über die möglichen Folgen und Entscheidungsalternativen.
(2) Ist das Ergebnis nach ärztlicher Erkenntnis auch für Verwandte der betroffenen

Person von Bedeutung, hat die Ärztin oder der Arzt bei der nachgehenden Beratung der betroffenen Person auch auf das Recht der Verwandten hinzuweisen, ihre Erbanlagen nicht zur Kenntnis zu nehmen. Will die betroffene Person die Verwandten gleichwohl unterrichten, soll die Beratung auch die Möglichkeit umfassen, die Ärztin oder den Arzt mit der Unterrichtung von Verwandten der betroffenen Person zu beauftragen.

(3) Gegen den Willen der betroffenen Person oder ihres gesetzlichen Vertreters darf die veranlassende Ärztin oder der veranlassende Arzt Verwandte oder Partner der betroffenen Person nur dann von dem Untersuchungsergebnis unterrichten, wenn und soweit dies zur Wahrung erheblich überwiegender Interessen dieser Personen erforderlich ist.

Diagnostische genetische Untersuchung bei behinderten Personen

Bei diagnostischen genetischen Untersuchungen, die sich auf die Ursache einer Behinderung der betreffenden Person beziehen, gelten die Anforderungen an die Einwilligung und Unterrichtung über das Untersuchungsergebnis entsprechend.

Genetische Untersuchungen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen

Grundsatz

Arbeitgebern und Versicherern ist es verboten, als Voraussetzung für einen Vertragsabschluss oder während des Vertragsverhältnisses prädiktive genetische Untersuchungen an betroffenen Arbeits- oder Versicherungsvertragsbewerbern oder Vertragspartnern durchzuführen oder zu veranlassen oder Ergebnisse von genetischen Untersuchungen zu verlangen, entgegenzunehmen oder sonst zu nutzen. Aus einer wahrheitswidrigen Beantwortung können Arbeitgeber oder Versicherer grundsätzlich keine Rechte ableiten (Ausnahmen siehe unten).

Arbeitsverhältnis

Bleibt der Arbeitsplatz trotz vorrangiger Arbeitsschutzmaßnahmen mit einer erhöhten Erkrankungs- oder Unfallgefahr verbunden, für deren Eintritt nach dem Stand der Wissenschaft eine bestimmte Genstruktur der Betroffenen von Bedeutung ist, ist eine Arbeitsplatzbewerberin oder ein Arbeitsplatzbewerber hierauf hinzuweisen. Die Betriebsärztin oder der Betriebsarzt soll die betroffene Person hinsichtlich einer geeigneten genetischen Untersuchung beraten und ihr dafür zugelassene Ärztinnen oder Ärzte benennen.

Ausnahmen für das Versicherungsverhältnis

(1) Strebt die betroffene Person eine Versicherung mit einer Leistungssumme über 250.000 € an, ist der Versicherer berechtigt zu fragen, ob und gegebenenfalls wann bei der betroffenen Person eine prädiktive genetische Untersuchung durchgeführt wurde. Bei arglistigem Verschweigen kann der Versicherer den Versicherungsvertrag kündigen.
(2) Bestehen konkrete Anhaltspunkte, insbesondere aufgrund des Zeitabstandes zwischen genetischer Untersuchung und Versicherungsantrag, dafür, dass die Höhe der gewünschten Versicherungsleistung mit dem Ergebnis der genetischen Untersuchung zusammenhängt, kann der Versicherer das Ergebnis der genetischen Untersuchung verlangen. Dies gilt nicht für eine genetische Untersuchung, die bei der betroffenen Person pränatal oder während der Minderjährigkeit oder einer Einsichtsunfähigkeit durchgeführt wurde. In diesen Fällen darf der Versicherer das Ergebnis der genetischen Untersuchung von der betroffenen Person entgegennehmen.

Genetische Untersuchungen zur Abstammungsklärung und zur Identifizierung außerhalb der Strafverfolgung

Grundsatz

(1) Zu Zwecken der Abstammungsklärung und der Identifizierung dürfen nur die dazu geeigneten und erforderlichen genetischen Untersuchungen (DNA-Identifizierungsmuster) durchgeführt werden. Diagnostische oder prädiktive Untersuchungen nach Krankheitsanlagen oder Merkmalen der betroffenen Person sind unzulässig. Abgesehen vom Merkmal Geschlecht sind unvermeidliche Überschussinformationen so früh wie möglich zu vernichten.
(2) Die untersuchende Stelle hat selbst die Proben bei der betroffenen Person zu entnehmen und dies zu dokumentieren.
(3) Die Proben sind zu vernichten, wenn die betroffene Person dies wünscht oder ein Gericht die Vernichtung anordnet, im Übrigen wenn die genetische Untersuchung durchgeführt ist. Die Dokumentation ist 10 Jahre aufzubewahren.

Einwilligung

Genetische Untersuchungen zu Zwecken der Abstammungsklärung oder Identifizierung dürfen nur mit schriftlicher Einwilligung der betroffenen Person oder ihres gesetzlichen Vertreters oder auf gerichtliche oder behördliche Anordnung durchgeführt werden. Für genetische Untersuchungen zur Abstammungsklärung bei Minderjährigen gilt § 1629 BGB.

Anordnung genetischer Untersuchungen zu Identifizierungszwecken

(1) In gerichtlichen und Verwaltungsverfahren kann das Gericht bzw. die Verwaltungsbehörde eine genetische Untersuchung zu Identifizierungszwecken anordnen, wenn die Identität einer Partei, eines Beteiligten oder einer für das Verfahren wichtigen dritten Person oder Leiche in Zweifel steht und nicht auf andere Weise geklärt werden kann. Ist die Identitätsfeststellung Voraussetzung für die Gewährung von behördlichen Genehmigungen oder Leistungen an die betroffene Person, ist die genetische Untersuchung nur mit ihrer Einwilligung zulässig.
(2) Die Anordnung hat die Art der Probe, das Ziel der Untersuchung sowie den Zeitpunkt der Vernichtung der Probe und der Löschung der genetischen Daten festzulegen. Bei lebenden Personen ist die Probe ohne Eingriff in die körperliche Unversehrtheit zu entnehmen, es sei denn, die betroffene Person willigt in einen Eingriff ein.

Genetische Untersuchungen zu Forschungszwecken

Konkrete, zeitlich befristete Forschungsvorhaben

(1) Für konkrete, zeitlich befristete Forschungsvorhaben ist die genetische Untersuchung von Proben und die Erhebung, Verarbeitung und Nutzung genetischer Daten zulässig, wenn
    1. die Proben und die genetischen Daten der betroffenen Person nicht mehr zugeordnet werden können oder
    2. im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert, die betroffene Person nach den Anforderungen für Forschungsvorhaben eingewilligt hat (siehe unten) oder
    3. im Falle, dass weder auf die Zuordnungsmöglichkeit verzichtet, noch die Einwilligung eingeholt werden kann, das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schützenswerten Interessen der betroffenen Person überwiegt und der Forschungszweck nicht auf andere Weise zu erreichen ist.

(2) In den Fällen der Ziffer (1) Nr. 2 und 3 sind bei Proben vor der Untersuchung, bei genetischen Daten vor der Verarbeitung oder Nutzung die Merkmale, mit denen ein Personenbezug hergestellt werden kann, gesondert zu speichern. Die Zuordnungsmöglichkeit ist aufzuheben, sobald der Forschungszweck es erlaubt und schutzwürdige Interessen der betroffenen Person gemäß der Regelung über deren Rechte (siehe unten) nicht entgegenstehen.

(3) Die Proben dürfen nur im Rahmen des Forschungsvorhabens untersucht, die genetischen Daten dürfen nur zu den Zwecken verarbeitet oder genutzt werden, für die sie im Rahmen des Forschungsvorhabens erhoben wurden.

(4) Mit Beendigung des Forschungsvorhabens sind die Proben zu vernichten und die genetischen Daten zu löschen. Ist ihre Aufbewahrung oder Speicherung zum Zwecke der Selbstkontrolle der Wissenschaft erforderlich, ist dies in pseudonymisierter Form für einen Zeitraum von längstens zehn Jahren zulässig.

(5) Konkrete, zeitlich befristete Forschungsvorhaben nach Ziffer (1) bedürfen der vorherigen Zustimmung der zuständigen Ethikkommission.

Sammlungen von Proben und genetischen Daten

(1) Das Sammeln von Proben einschließlich isolierter DNS oder RNS oder von genetischen Daten zu allgemeinen Forschungszwecken ist nur zulässig, wenn die betroffenen Personen über Zweck und Nutzungsmöglichkeiten der Sammlung aufgeklärt wurden und in die Entnahme der Probe sowie die Aufnahme von Probe und Daten in die Sammlung eingewilligt haben (siehe unten) Satz 1 gilt entsprechend für die Übernahme bereits vorhandener Proben oder genetischer Daten.

(2) Die Zuordnung der Probe und der genetischen Daten zur betroffenen Person ist vor der Aufnahme in die Sammlung aufzuheben. Erfordert der Zweck der Sammlung die Möglichkeit einer Zuordnung, sind die Proben und die genetischen Daten vor der Aufnahme in die Sammlung bei Treuhändern zu pseudonymisieren.

(3) Vor einer Weitergabe von Proben und einer Übermittlung genetischer Daten für konkrete Forschungsvorhaben ist die Möglichkeit der Zuordnung zur betroffenen Person aufzuheben oder, wenn der Forschungszweck dem entgegensteht, eine weitere Pseudonymisierung gemäß den Regelungen bei Treuhändern (siehe unten) vorzunehmen.

(4) Der Träger einer Sammlung hat eine kontinuierliche interne Datenschutzkontrolle sicherzustellen. Bei Trägerwechsel gehen alle Verpflichtungen aus diesem Gesetz auf den neuen Träger über. Soll eine Sammlung beendet werden, sind die Proben zu vernichten und die genetischen Daten sowie die beim Treuhänder (siehe unten) gespeicherten Daten zu löschen.

(5) Die Einrichtung einer neuen und die Übernahme einer bestehenden Sammlung nach Ziffer (1) bedürfen der Zustimmung durch die zuständige Ethikkommission. Die Einrichtung ist mit dem Votum der Ethikkommission und unter Darlegung

der in den Vorschlägen zur Sammlung von Proben und genetischen Daten, zur Aufklärung und Einwilligung, über die Rechte der betroffenen Person und über die Treuhänder geforderten Maßnahmen bei der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen. Betriebs- und Geschäftsgeheimnisse sind kenntlich zu machen. Die Anzeige ist jeweils nach fünf Jahren mit einer Begründung der weiteren Speicherung zu erneuern. Ebenso sind die Vernichtung oder Löschung von Sammlungen nach Ziffer (1), die Löschung der Zuordnungsmerkmale bei Treuhändern und Trägerwechsel nach Ziffer (4) anzuzeigen.

Aufklärung und Einwilligung

(1) Die betroffene Person ist vor ihrer Einwilligung im Falle, dass der Forschungszweck die Möglichkeit der Zuordnung erfordert (siehe oben), oder bei Sammlungen von Proben oder genetischen Daten (siehe oben) insbesondere aufzuklären über
- den verantwortlichen Träger des Forschungsvorhabens oder der Sammlung,
- das Ziel der Forschung oder bei Sammlungen die möglichen Forschungsrichtungen,
- ihre Rechte bei Patentanmeldungen und gewerblichen Nutzungen,
- die Dauer der Aufbewahrung von Proben und der Speicherung der genetischen Daten,
- Zeitpunkt und Art der Pseudonymisierung von Proben und genetischen Daten, sowie über die mögliche Wiederherstellung der Zuordnung zur betroffenen Person,
- ihr Recht - vorbehaltlich der pseudonymisierten Verarbeitung nach Beendigung des Forschungsvorhabens (siehe oben) - die Vernichtung der Probe und die Löschung der genetischen Daten oder die Aufhebung der Zuordnungsmöglichkeit zu verlangen, wenn sie die Einwilligung widerruft,
- ihr Recht, Ergebnisse von Untersuchungen nicht zur Kenntnis zu nehmen oder unter Nutzung eines darzustellenden Entpseudonymisierungsverfahrens zu erfahren,
- ihr Recht, Auskunft über die zu ihr gespeicherten genetischen Daten zu verlangen.

Die Aufklärung hat schriftlich und mündlich zu erfolgen.

(2) Die Einwilligung soll die Entscheidung darüber umfassen, ob die betroffene Person vom Ergebnis der Untersuchung Kenntnis nehmen will oder nicht.

(3) Die Einwilligung kann eine Schweigepflichtentbindung für zu benennende behandelnde Ärzte einschließen, wenn die betroffene Person über Art und Umfang

der Patientendaten informiert wird, die der Arzt für das Forschungsvorhaben (siehe oben) oder die Sammlung von Proben oder genetischen Daten (siehe oben) übermittelt.

Rechte der betroffenen Person

(1) Hinsichtlich der genetischen Daten stehen der betroffenen Person die im Bundesdatenschutzgesetz geregelten Rechte zu. Widerruft die betroffene Person ihre Einwilligung (siehe oben), sind entweder die Probe zu vernichten und die genetischen Daten zu löschen oder die Zuordnungsmerkmale zu löschen.

(2) Erbringt ein Forschungsvorhaben Ergebnisse, die für die betroffene Person von Bedeutung sind, veranlasst der Träger des Forschungsvorhabens eine Unterrichtung der betroffenen Person. Dies gilt nicht, wenn die betroffene Person erklärt hat, von dem Untersuchungsergebnis keine Kenntnis nehmen zu wollen (siehe oben).

Treuhänder

(1) Die Pseudonymisierung von Proben und genetischen Daten erfolgt durch einen Treuhänder. Er vergibt die Pseudonyme unverzüglich, verwahrt und verwaltet die Zuordnungsmerkmale und sichert die Rechte der betroffenen Person (siehe oben). Soweit erforderlich, kann er für diese Zwecke Kontakt mit der betroffenen Person aufnehmen. Er hat keinen Zugriff auf genetische Daten.

(2) Treuhänder kann eine natürliche Person sein, die von Berufs wegen einer besonderen Schweigepflicht unterliegt und vom Träger des Forschungsprojekts oder der Sammlung von Proben oder genetischen Daten unabhängig ist. Im Vertrag zwischen dem Treuhänder und dem Träger des Forschungsvorhabens oder der Sammlung von Proben oder genetischen Daten sind insbesondere die Anlässe und das Verfahren zur Wiederherstellung des Personenbezuges, die Nutzungsformen durch die Selbstkontrollgremien der Wissenschaft sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit festzulegen. Der Vertrag ist vorab der für die Datenschutzkontrolle zuständigen Behörde vorzulegen.

Schlussvorschläge

Ordnungswidrigkeit

Ordnungswidrig handelt, wer
- eine Reihenuntersuchung ohne die erforderliche Zulassung durchführt oder

- den Anzeigepflichten bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung von Proben oder genetischen Daten oder bei bestehenden Proben- oder genetischen Datensammlungen nicht fristgemäß nachkommt.

Straftaten

(1) Wer genetische Testverfahren unter Verstoß gegen die Anforderungen an das Inverkehrbringen genetischer Tests und Angebote von genetischen Untersuchungen einführt oder in Verkehr bringt oder genetische Untersuchungen ohne eine individuelle Beratung öffentlich anbietet, wird mit ... bestraft. Handelt die Täterin oder der Täter gewerbsmäßig, ist die Strafe ...

(2) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu medizinischen Zwecken durchführt, ohne
- Arzt oder Ärztin zu sein,
- die für die genetischen Untersuchungen zu medizinischen Zwecken festgelegten Beschränkungen der Untersuchungszwecke einzuhalten,
- die geforderte Aufklärung und Beratung unternommen bzw. sichergestellt zu haben oder
- die Einwilligung der betroffenen Person eingeholt zu haben,wird mit ... bestraft.

(3) Wer als Arbeitgeber oder als Versicherer gegen das Verbot genetischer Untersuchungen verstößt, ohne dass die vorgesehene Ausnahmeregelung eingreift, wird mit ... bestraft.

(4) Wer vorsätzlich oder fahrlässig eine genetische Untersuchung zu Zwecken der Abstammungsklärung oder Identifizierung in unzulässiger Weise auf prädiktive oder diagnostische Ziele ausrichtet oder ohne die geforderte Einwilligung durchführt, wird mit ... bestraft.

(5) Wer vorsätzlich oder fahrlässig personenbeziehbare Proben, DNS-/RNS-Teile oder genetische Daten entgegen den Regelungen für genetische Untersuchungen zu Forschungszwecken
- ohne Einwilligung oder Aufklärung zu Forschungszwecken nutzt oder
- in Sammlungen für Forschungszwecke zur Verfügung stellt,

wird mit ... bestraft.

Antrag

Die oben aufgeführten Straftaten werden nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person und die für die Datenschutzkontrolle zuständige Behörde.

Befristung

Die Regelungen sind auf zehn Jahre zu befristen. Acht Jahre nach In-Kraft-Treten haben die für die Datenschutzkontrolle zuständigen Behörden unter Federführung des Bundesbeauftragten für den Datenschutz dem Gesetzgeber einen Bericht über die Wirksamkeit der vorgeschlagenen Regelungen und über neue Gefährdungen für das Persönlichkeitsrecht sowie zu möglichen Rechtsvereinfachungen vorzulegen. Diesem Bericht sind Stellungnahmen des Ethikrates und der Deutschen Forschungsgemeinschaft beizufügen.

Übergangsvorschrift

Träger von bestehenden Proben- und genetischen Datensammlungen haben der Anzeigepflicht bei der Einrichtung einer neuen oder der Übernahme einer bestehenden Sammlung innerhalb von sechs Monaten nach In-Kraft-Treten dieses Gesetzes nachzukommen. Innerhalb dieser Frist ist den Anforderungen an die Einwilligung zu entsprechen. Vor In-Kraft-Treten dieses Gesetzes ohne Einwilligung gewonnene Proben und erhobene genetische Daten sind spätestens nach zwei Jahren zu vernichten bzw. zu löschen. Dies ist der für die Datenschutzkontrolle zuständigen Behörde anzuzeigen.

16.6 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster zu biometrischen Merkmalen in Personalausweisen und Pässen

Im Entwurf eines Terrorismusbekämpfungsgesetzes ist vorgesehen, die Möglichkeit zu eröffnen, in deutschen Personalausweisen und Pässen neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie zum Beispiel Fingerabdrücke, Handgeometrie, Gesichtsgeometrie u. a. aufzunehmen. Auch die Verwendung genetischer Daten wird nicht ausgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass diese Maßnahme schon allein wegen des technischen und zeitlichen Aufwandes, der mit der Einführung derartiger Dokumente verbunden wäre, keinen kurzfristigen Beitrag zur Lösung der mit dem internationalen Terrorismus derzeit verbundenen Probleme leisten kann, zumal Ausländerinnen und Ausländer, die sich in Deutschland aufhalten, nicht erfasst werden.

Die Nutzung biometrischer Merkmale in Personalausweisen und Pässen sowie die damit verbundenen Folgeprobleme (zum Beispiel Art und Ort der Speicherung von

Referenzdaten; Vermeidung von Überschussinformationen) werfen eine Vielzahl schwieriger Fragen auf, die einer ausführlichen Diskussion bedürfen. Die zuständigen Stellen werden hierzu aufgefordert, die Notwendigkeit und die rechtlichen und technischen Einzelheiten einer Realisierung dieser Maßnahmen darzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist bereit, sich unter diesen Voraussetzungen mit der Frage zu befassen, ob und wie es möglich ist, mit Hilfe geeigneter zusätzlicher Merkmale in Identifikationspapieren deren Missbrauch zu verhindern, ohne dabei die Grundsätze des Datenschutzes zu verletzen.

16.7 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster zu datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als *Pflichtkarte*. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über

Einsatz und Verwendung der Karte muss gewährleistet werden (*Grundsatz der Freiwilligkeit*).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,
- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
- welche ihrer Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und
- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem "Arzneimittelpass" keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den "Arzneimittelpass" auf der *Krankenversichertenkarte* gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die "Funktion Krankenversichertenkarte" von der "Funktion Arzneimittelpass" informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offenlegen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z. B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

16.8 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster zur Lkw-Maut auf Autobahnen und zur allgemeinen Maut auf privat errichteten Bundesfernstraßen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten. Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechungszwecke verwendet wird.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen. Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbeziehbarer Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.
- Es ist sicherzustellen, dass anfallende personenbezogenen Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

16.9 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster zur „Neuen Medienordnung“

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

16.10 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster: Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder

Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus - mit den Worten des Bundesverfassungsgerichts - auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

16.11 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster: Grundsätze zur Übermittlung von Telekommunikationsverbindungsdaten

Die Bundesregierung hat den Gesetzentwurf für eine Nachfolgeregelung zu § 12 FAG vorgelegt, der eine Reihe datenschutzrechtlich positiver Ansätze enthält.

Der Bundesrat hat sich demgegenüber in seiner Stellungnahme für eine Regelung ausgesprochen, die wesentlichen datenschutzrechtlichen Anforderungen nicht gerecht wird. Die Datenschutzbeauftragten des Bundes und der Länder lehnen den Vorschlag des Bundesrates entschieden ab.

Sie halten es für nicht vertretbar, Auskünfte über zurückliegende Aktivmeldungen von Mobiltelefonen auch bei reinem Stand-by-Betrieb zu erteilen und Diensteanbieter zur Aufzeichnung von Telekommunikationsverbindungsdaten eigens für Zwecke der Strafverfolgung zu verpflichten.

Auch die vom Bundesrat vorgeschlagene Regelung des § 18 a BVerfSchG zur Übermittlung von Telekommunikationsverbindungsdaten an die Verfassungsschutzbehörden halten die Datenschutzbeauftragten des Bundes und der Länder für nicht akzeptabel. Sie fordern eine deutliche Klarstellung im Wortlaut des Gesetzes, dass Verbindungsdaten an den Verfassungsschutz nur dann übermittelt werden dürfen, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine in § 3 Abs. 1 G 10 genannte Straftat plant, begeht oder begangen hat oder sonst an gewalttätigen Bestrebungen oder sicherheitsgefährdenden Tätigkeiten teilnimmt. Eine Übermittlung der Verbindungsdaten für den gesamten Aufgabenbereich des Verfassungsschutzes ginge dagegen erheblich zu weit.

Ferner halten es die Datenschutzbeauftragten für geboten, hinsichtlich der Kennzeichnung und Zweckbindung der Daten, der Mitteilungen an Betroffene und der parlamentarischen Kontrolle einen dem G 10 möglichst gleichwertigen Standard zu gewährleisten.

Die Bundesregierung und der Deutsche Bundestag werden gebeten, diese datenschutzrechtlichen Mindestanforderungen im weiteren Gesetzgebungsverfahren zu berücksichtigen.

16.12 Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster: EUROJUST - Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung

der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

- Informationsaustausch mit Partnern
  Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und -stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

- Verarbeitung personenbezogener Daten
  Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die

Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

- Ermittlungsindex und Dateien
  Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

- Auskunftsrecht
  Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinterese oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

- Änderung, Berichtigung und Löschung
  Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

- Speicherungsfristen
  Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z. B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

- Datensicherheit
  Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

- Gemeinsame Kontrollinstanz
  Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindenden Charakter haben.

- Rechtsschutz
  Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

- Rechtsetzungsbedarf
  Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.

  Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

16.13 Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002 in Mainz: Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. „know your customer principle“). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

16.14 Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002 in Mainz zu biometrischen Merkmalen in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

16.15 Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002 in Mainz zum Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikations diensten

Mit der rasch wachsenden Nutzung des Internets kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz „Für eine freie Telekommunikation in einer freien Gesellschaft“) darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikation sgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1.1.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z. B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.
In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

16.16 Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. März 2002 in Mainz zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internets am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet .

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internets am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen, und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internets am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internets müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.