18. Wahlperiode

Drucksache **18/106**

HESSISCHER LANDTAG

27. 02. 2009

Siebenunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2008
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 27. Februar 2009 · Ausgegeben am 24. März 2009
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 37. Tätigkeitsbericht

Register der Rechtsvorschriften zum 37. Tätigkeitsbericht

Kernpunkte

Abkürzungsverzeichnis zum 37. Tätigkeitsbericht

a.F.	alte Fassung
AAH-SDÜ	Allgemeine Anwendungshinweise zum Schengener Durchführungsübereinkommen
ABl.	Amtsblatt des Hessischen Kultusministeriums
ABlEG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AK	Arbeitskreis
ALG II	Arbeitslosengeld II
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ArbSchG	Arbeitsschutzgesetz
ARGE	Arbeitsgemeinschaften
Art.	Artikel
Az.	Aktenzeichen
BAB	Bundesautobahn
BAföG	Bundesausbildungsförderungsgesetz
BAnz.	Bundesanzeiger
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BIOS	**B**asic **I**nput/**O**utput **S**ystem
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern
BRDrucks.	Bundesratsdrucksache
BRRG	Beamtenrechtsrahmengesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
bzgl.	bezüglich
bzw.	beziehungsweise
CD	Compact Disc
d.h.	das heißt
d.J.	dieses Jahres
DFB	Deutscher Fußballbund
Drucks.	Drucksache
EDV	elektronische Datenverarbeitung
eFA	elektronische Fallakte
EG	Europäische Gemeinschaft
eGK	elektronische Gesundheitskarte
ELENA	**el**ektronischer **E**ntgelt**na**chweis
ELSTER	**el**ektronische **St**euer**er**klärung
ePA	elektronischer Personalausweis
ePass	elektronischer Reisepass
EU	Europäische Union
EU-Richtlinie	Richtlinie der Europäischen Union
EURODAC	Europäisches Fingerabdrucksystem (Européen und Dactyloscopie)
Eurojust	Europäische Stelle zur justiziellen Zusammenarbeit
EUROPOL	Europäisches Polizeiamt
evtl.	eventuell
ff.	fortfolgende/r/s
FIDIS	**F**uture of **Id**entity in the **I**nformation **S**ociety
gem.	gemäß
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
ggf.	gegebenenfalls
GK	Gemeinsame Kontrollinstanz
GMBl.	Gemeinsames Ministerialblatt
GMG	Gesundheitsmodernisierungsgesetz
GVBl.	Gesetz- und Verordnungsblatt
HAGTierSG	Hessisches Ausführungsgesetz zum Tierseuchengesetz
HArchivG	Hessisches Archivgesetz
HBA	Heilberufeausweis
HBG	Hessisches Beamtengesetz
HDSG	Hessisches Datenschutzgesetz
HessLStatG	Hessisches Landesstatistikgesetz
HessVGH	Hessischer Verwaltungsgerichtshof
HGO	Hessische Gemeindeordnung

HKHG	Hessisches Krankenhausgesetz
HKM	Hessisches Kultusministerium
HLKA	Hessisches Landeskriminalamt
HMDIS	Hessisches Ministerium des Innern und für Sport
HMDJ	Hessisches Ministerium der Justiz
HMG	Hessisches Meldegesetz
HMULV	Hessisches Ministerium für Umwelt, ländlichen Raum und Verbraucherschutz
HPRG	Hessisches Privatrundfunkgesetz
HPVG	Hessisches Personalvertretungsgesetz
HSchulG	Hessisches Schulgesetz
HSL	Hessisches Statistisches Landesamt
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HStiftG	Hessisches Stiftungsgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i.d.F.	in der Fassung
i.d.R.	in der Regel
i.R.d.	im Rahmen des/der
i.S.d.	im Sinne des/der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
ICAO	**I**nternational **C**ivil **A**viation **O**rganisation
IDAT	Identitätsdaten
inkl.	inklusive
IPF	Idiopathische Pulmonale Fibrose
ISO	**I**nternational **S**tandards **O**rganisation
IT	Informationstechnik
JMBl.	Justizministerialblatt
KIS	Klinikinformationssystem
KV Hessen	Kassenärztliche Vereinigung Hessen
LÄK	Landesärztekammer
LIMO	politisch links motivierter Straftäter
LTDrucks.	Landtagsdrucksache
LUSD	**L**ehrer- **u**nd **S**chüler-**D**atenbank
LWO	Landeswahlordnung
m.W.v.	mit Wirkung vom
MDAT	medizinische Daten
MDK	Medizinischer Dienst der Krankenversicherung
MDS	Medizinischer Dienst der Spitzenverbände der Krankenkassen
MeldDÜVO	Meldedatenübermittlungsverordnung
MVZ	Medizinisches Versorgungszentrum
Nr.	Nummer
o.Ä.	oder Ähnliches
o.g.	oben genannte/r/s
OCR	Optical Character Recognition
OFD	Oberfinanzdirektion
OWiG	Ordnungswidrigkeitengesetz
PC	Personal Computer
PassG	Passgesetz
PAuswG	Personalausweisgesetz
PDF/A	Portable Document Format für die Langzeitarchivierung
PID	**P**ersonally-**I**dentifiable **D**ata
PIN	**P**ersonal **I**dentification **N**umber (persönliche Geheimzahl)
PKI	**P**ublic **K**ey **I**nfrastruktur
PKW	Personenkraftwagen
POLAS	Polizeiliches Arbeitsplatzsystem
PStG	Personenstandsgesetz
PStV	Verordnung zur Ausführung des Personenstandsgesetzes
PTLV	Präsidium für Technik, Logistik und Verwaltung
PRIME	**Pr**ivacy and **I**dentity **M**anagement für **E**urope
PUK	**P**ersonal **U**nblocking **K**ey
QES	**q**ualifizierte **e**lektronische **S**ignatur
Rdnr.	Randnummer
RFID	**R**adio **f**requency **id**entification
RGebStV	Rundfunkgebührenstaatsvertrag
RP	Regierungspräsidium
s.	siehe
S.	Seite oder Satz
SAP R/3 HR	in der Hessischen Landesverwaltung eingesetztes DV-System zur Personaldatenverarbeitung

SDÜ	Schengener Durchführungsübereinkommen
sec	Sekunde/n
SFB	sozialmedizinische Fallberatung
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
SIS II	Schengener Informationssystem der zweiten Generation
sog.	sogenannte/r/s
StAnz.	Staatsanzeiger für das Land Hessen
Steuer-ID	Steueridentifikationsnummer
StPO	Strafprozessordnung
StVollzG	Strafvollzugsgesetz
TierSG	Tierseuchengesetz
TIFF	**T**agged **I**mage **F**ile **F**ormat
TMF	Telematikplattform für Medizinische Forschungsnetze
u.a.	unter anderem
USB	Universal Serial Bus (Schnittstelle bei Geräten)
VIS	(europäisches) Visa-Informationssystem
VO	Verordnung
VPS	Virtuelle Poststelle
XML	Extensible Markup Language
z.B.	zum Beispiel
z.T.	zum Teil
ZAG	Zentrum für Arbeit und Grundsicherung
Ziff.	Ziffer

Register der Rechtsvorschriften zum 37. Tätigkeitsbericht

AAH-SDÜ	Allgemeine Anwendungshinweise zum Schengener Durchführungsübereinkommen vom 28. Jan. 1998
AEUV	Vertrag über die Arbeitsweise der Europäischen Union i.d.F. des Vertrags von Lissabon vom 13. Dez. 2007 (ABlEG 2007/C 306/1)
AO	Abgabenordnung 1977 i.d.F. vom 1. Okt. 2002 (BGBl. I S. 3866), zuletzt geändert durch Art. 89 des Gesetzes vom 17. Dez. 2008 (BGBl. I S. 2586 m.W.v. 1- Sept. 2009)
ArbSchG	Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzgesetzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit (Arbeitsschutzgesetz) i.d.F. vom 7. Aug. 1996 (BGBl. I S. 1246), zuletzt geändert durch § 62 Abs. 16 des Gesetzes vom 17. Juni 2008 (BGBl. I S. 1010)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) i.d.F. vom 25. Feb. 2008 (BGBl. I S. 162), zuletzt geändert durch Art. 1 des Gesetzes vom 20. Dez. 2008 (BGBl. I S. 2846)
BGB	Bürgerliches Gesetzbuch i.d.F. vom 2. Jan. 2002 (BGBl. I S. 42; 2003 I S. 738), zuletzt geändert durch Art. 6 des Gesetzes vom 12. Aug. 2008 (BGBl. I S. 1666)
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Art. 1 des Gesetzes vom 25. Dez. 2008 (BGBl. I S. 3083)
BRRG	Rahmengesetz zur Vereinheitlichung des Beamtenrechts (Beamtenrechtsrahmengesetz) i.d.F. vom 31. März 1999 (BGBl. I S. 654), zuletzt geändert durch Gesetz vom 17. Juni 2008 (BGBl. I S. 1010)
Charta der Grundrechte der EU	Charta der Grundrechte der Europäischen Union vom 7. Dez. 2000 (ABlEG 2000/C 364/1), i.d.F. vom 12. Dez. 2007 (bislang nicht ratifiziert)
EG-Richtlinie Nr. 2002/58 bzw. Nr. 2006/24	Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2002 (Datenschutz-Richtlinie für elektronische Kommunikation; ABlEG 2002/L 201/27), geändert durch die Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden vom 15. März 2006 (ABlEG 2006/L 105/54)
EG-Richtlinie Nr. 2004/82	Richtlinie des Rates über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln vom 29. Apr. 2004 (ABlEG 2004/L 261/24)
EG-Richtlinie Nr. 2007/2	Richtlinie des Europäischen Parlaments und des Rates zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE) vom 14. März 2007 (ABlEG 2007/L 108/1)
EG-Verordnung Nr. 2725/2000	Verordnung des Europäischen Rates vom 11. Dez. 2000 über die Einrichtung von "Eurodac" für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens (ABlEG 2000/L 316/1)
EG-Verordnung Nr. 2252/2004	Verordnung des Europäischen Rates vom 13. Dez. 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (ABlEG 2004/L 385/1)

EU-Vertrag	Vertrag über die Europäische Union vom 25. März 1957 (Rom; ABlEG 2002/C 325/33), i.d.F. des Vertrags von Maastricht vom 7. Feb. 1992 (ABlEG 1992/C 191/1), i.d.F. des Vertrags von Amsterdam vom 2. Okt. 1997 (ABlEG 1997/C 340/1), i.d.F. des Vertrags von Nizza vom 26. Feb. 2001 (ABlEG 2001/C 80/1), i.d.F. des Vertrags von Lissabon vom 13. Dez. 2007 (ABlEG 2007/C 306/1)
GG	Grundgesetz für die Bundesrepublik Deutschland i.d.F. vom 23. Mai 1949 (BGBl. I S. 1), zuletzt geändert durch Gesetz vom 28. Aug. 2006 (BGBl. I S. 2034)
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz) i.d.F. vom 14. Nov. 2003 (BGBl. I S. 2190), zuletzt geändert durch Art. 1 des Gesetz vom 15. Dez. 2004 (BGBl. I. S. 3445)
HAGTierSG	Hessisches Ausführungsgesetz zum Tierseuchengesetz i.d.F. vom 22. Dez. 2000 (BGBl. I S. 624), zuletzt geändert durch Art. 6 des Gesetzes vom 29. Nov. 2005 (GVBl. I S. 769)
HArchivG	Hessisches Archivgesetz vom 18. Okt. 1989 (GVBl. I S. 270), zuletzt geändert durch Gesetz vom 5. Juli 2007 (GVBl. I S. 380)
HBG	Hessisches Beamtengesetz i.d.F. vom 11. Jan. 1989 (GVBl. I S. 25), zuletzt geändert durch Art. 4 des Gesetzes vom 5. Juli 2007 (GVBl. I S. 378)
HDSG	Hessisches Datenschutzgesetz i.d.F. vom 7. Jan. 1999 (GVBl. I S. 98)
HessLStatG	Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz) vom 19. Mai 1987 (GVBl. I S. 67), zuletzt geändert durch Art. 1 des Gesetzes vom 11. Dez. 2007 (GVBl. I S. 921)
HGO	Hessische Gemeindeordnung i.d.F. vom 7. März 2005 (GVBl. I S. 142); zuletzt geändert durch Art. 32b des Gesetzes vom 17. Okt. 2005 (GVBl. I S. 674)
HKHG	Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2002) vom 6. Nov. 2002 (GVBl. I S. 662), zuletzt geändert durch Gesetz vom 17. Dez. 2007 (GVBl. I S. 908)
HMG	Hessisches Meldegesetz i.d.F. vom 10. März 2006 (GVBl. I S. 66)
HPRG	Gesetz über den privaten Rundfunk in Hessen (Hessisches Privatrundfunkgesetz) i.d.F. vom 25. Jan. 1995 (GVBl. I S. 87), zuletzt geändert durch Art. 2 Nr. 9 des Gesetzes vom 10. Juni 2008 (GVBl. I S. 740)
HPVG	Hessisches Personalvertretungsgesetz vom 24. März 1988 (GVBl. I S. 103), zuletzt geändert durch Gesetz vom 6. Juli 1999 (GVBl. I S. 338)
HSchulG	Hessisches Schulgesetz i.d.F. vom 14. Juni 2005 (GVBl. I S. 442), zuletzt geändert durch Gesetz vom 5. Juni 2008 (GVBl. I S. 761)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i.d.F. vom 14. Jan. 2005 (GVBl. I S. 14); zuletzt geändert durch Urteil des BVerfG vom 11. März 2008 (BGBl. I S. 541)
HStiftG	Hessisches Stiftungsgesetz vom 4. Apr. 1966 (GVBl. I S. 77), zuletzt geändert durch Gesetz vom 6. Sept. 2007 (GVBl. I S. 546)
MeldDÜVO	Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (Meldedaten-Übermittlungsverordnung) vom 6. Juli 2006 (GVBl. I S. 427), zuletzt geändert durch die Zweite Verordnung vom 22. Sept. 2008 (GVBl. I S. 883)
OWiG	Gesetz über Ordnungswidrigkeiten i.d.F. der Bekanntmachung vom 19. Feb. 1987 (BGBl. I S. 602), zuletzt geändert durch Art. 2 des Gesetzes vom 7. Aug. 2007 (BGBl. I S. 1786)

PassG	Passgesetz vom 19. Apr. 1986 (BGBl. I S. 537), zuletzt geändert durch Art. 11 des Gesetzes vom 26. Feb. 2008 (BGBl. I S. 215)
PassVwV	Allgemeine Verwaltungsvorschriften zur Durchführung des Passgesetzes vom 3. Juli 2000 (GMBl. S. 587/BAnz. S. 18859)
PersAuswG	Gesetz über Personalausweise i.d.F. vom 21. April 1986 (BGBl. I S. 548), zuletzt geändert durch Art. 2 des Gesetzes vom 20. Juli 2007 (BGBl. I S. 1566)
PStG	Personenstandsgesetz in der im BGBl. III, Gliederungsnummer 211-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 3 des Gesetzes vom 4. Juli 2008 (BGBl. I S. 1188) Aufgehoben durch Art. 5 Abs. 2 des Gesetzes (PStRG) vom 19. Feb. 2007 mit Wirkung vom 1. Jan. 2009 (BGBl. I S. 122)
PStRG	Gesetz zur Reform des Personenstandsrechts i.d.F. vom 19. Febr. 2007 (BGBl. I S. 122), zuletzt geändert durch Gesetz vom 13. März 2008 (BGBl. I S. 313) Tritt gem. Art. 5 Abs. 2 des Gesetzes am 01.01.2009 in Kraft.
PStV	Verordnung zur Ausführung des Personenstandsgesetzes vom 22. Nov. 2008 (BGBl. I S. 2263)
RGebStV	Rundfunkgebührenstaatsvertrag vom 31. August 1991, zuletzt geändert durch Art. 5 des Zehnten Rundfunkänderungsstaatsvertrags vom 18. Juni 2008 (GVBl. I S. 742)
SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 19. Juni 1990 - Schengener Durchführungsübereinkommen (GVBl. 1993 II S. 1010), zuletzt geändert durch EG-Verordnung Nr. 1931 des Europäischen Parlaments und des Rates vom 20. Dez. 2006 (ABlEG 2006/L 405/1)
SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dez. 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes vom 24. Sept. 2008 (BGBl. I S. 1856)
SGB II	Zweites Buch Sozialgesetzbuch - Grundsicherung für Arbeitsuchende - vom 24. Dez. 2003 (BGBl. I S. 2954), zuletzt geändert durch Art. 2a des Gesetzes vom 24. Sept. 2008 (BGBl. I S. 1856)
SGB V	Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dez. 1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 6 des Gesetzes vom 21. Dez. 2008 (BGBl. I S. 2940)
SGB VII	Siebtes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung - i.d.F. vom 7. Aug. 1996 (BGBl. I S. 1254), zuletzt geändert durch § 62 Abs. 19 des Gesetzes vom 17. Juni 2008 (BGBl. I S. 1010)
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - i.d.F. vom 18. Jan. 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 2c des Gesetzes vom 24. Sept. 2008 (BGBl. I S. 1856)
StGB	Strafgesetzbuch i.d.F. vom 13. Nov. 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 1 des Gesetzes vom 13. Aug. 2008 (BGBl. I S. 1690)
StPO	Strafprozessordnung i.d.F. der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 2 des Gesetzes vom 31. Okt. 2008 (BGBl. I S. 2149)
StVollzG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung (Strafvollzugsgesetz) vom 16. März 1976 (BGBl. I S. 581), zuletzt geändert durch § 62 Abs. 10 des Gesetzes vom 17. Juni 2008 (BGBl. I S. 1010)

TierSG	Tierseuchengesetz i.d.F. vom 22. Juni 2004 (BGBl. I S. 1260, 3588), zuletzt geändert durch Art. 1 des Gesetzes vom 13. Dez. 2007 (BGBl. I S. 2930)
TMG	Telemediengesetz vom 26. Feb. 2007 (BGBl. I S. 179)
Vertrag von Amsterdam	Vertrag zur Änderung des Vertrags über die Europäische Union, der Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte vom 2. Okt. 1997 (ABlEG 1997/C 340/1)
Vertrag von Lissabon	Vertrag zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft vom 13. Dez. 2007 (ABlEG 2007/C 306/1)
Vertrag von Nizza	Vertrag zur Änderung des Vertrags über die Europäische Union, der Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte vom 26. Feb. 2001 (ABlEG 2001/C 80/1)
Vertrag von Prüm	Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich vom 27. Mai 2005 (BGBl. 2006 I S. 1458)

Kernpunkte

1. Hessen hat seine Vorreiterrolle auf dem Gebiet des Datenschutzes eingebüßt. Die übrigen Länder und der Bund zogen insoweit nach. Mehr noch: Der deutsche, zum Teil auch der hessische Datenschutz sieht sich gegenwärtig dem Vorwurf ausgesetzt, gegen Europarecht zu verstoßen. Bezogen auf die gemeinschaftsrechtlich gebotene Unabhängigkeit des (gesamten) Datenschutzes ist wieder das hessische Vorbild gefragt. Gemeinschaftsrechtliche Bedenken ließen sich unter Wahrung des deutschen Verfassungsrechts ausräumen, wenn dem HDSB unter Beibehaltung seiner Unabhängigkeit auch der private Bereich in der Zuständigkeit des Landes übertragen und dabei die parlamentarische Verantwortlichkeit des HDSB verstärkt würde (Ziff. 1.1).

2. Durch zahlreiche Gerichtsentscheidungen wurde der Datenschutz im Berichtszeitraum bekräftigt. Besondere Beachtung verdienen die Entscheidungen des Bundesverfassungsgerichts vom 27. Februar 2008 zur "Online-Durchsuchung" und - unmittelbar auf Hessen bezogen - vom 11. März 2008 zu Kfz-Kennzeichenerfassungen. Diese Entscheidungen betreffen die Abwehrkomponente des Datenschutzes gegen staatliche Eingriffe. Die Datenskandale im privaten Bereich haben aber gezeigt, dass vor allem die Schutzkomponente (Datenschutz durch den Staat) an Bedeutung gewinnt (Ziff. 1.2 und 1.3.2).

3. Dass sich der öffentliche und private Bereich nicht trennen lassen, zeigt sich auf dem Gebiet der Daseinsvorsorge. Hier bedient sich der Staat Privater oder privatrechtlicher Rechtsformen zur Erfüllung öffentlicher Aufgaben. Am Charakter der Aufgaben ändert sich dadurch nichts. Daher fällt die Daseinsvorsorge in den öffentlichen Bereich mit der Rechtsfolge, dass der HDSB für den Datenschutz bei der hessischen Daseinsvorsorge zuständig ist (Ziff. 1.4).

4. Die Bundesrepublik Deutschland hat u.a. zur Erhöhung der Sicherheitsstandards neue Identitätsdokumente eingeführt (ePass) bzw. plant dieses (ePersonalausweis). Der neue elektronische Personalausweis wird neben der Funktion als Identitätsdokument und der neuen Möglichkeit, Fingerabdrücke zu speichern, gleichzeitig als multifunktionale Bürgerkarte einsetzbar sein. Das Grobkonzept des Bundesinnenministeriums enthält Schwachstellen, weil insbesondere die Risiken der angebotenen Möglichkeiten nicht hinreichend abgeklärt waren. Teilweise sind diese durch das im Dezember verabschiedete Gesetz ausgeräumt (Ziff. 3.1). Wird auf die Sicherheit von Identitätsdokumenten wirklich Wert gelegt, muss die Bundesdruckerei vor der Herstellung von Reisepässen die Signatur prüfen, mit der die Übermittlung der Daten von den Passbehörden an sie authentisiert und gesichert wird (Ziff. 5.2.2).

5. Die Videoüberwachung wird vielfältig eingesetzt. Sie dient nicht nur der Überwachung von Kriminalitätsschwerpunkten, wie z.B. der Konstablerwache in Frankfurt (Ziff. 4.1.1.2), sondern auch der Verbesserung der Sicherheit von Großveranstaltungen, wie z.B. Bundesligaspielen (Ziff. 4.1.1.1), der Verkehrssteuerung (Ziff. 4.1.1.3) und -überwachung (Ziff. 4.1.1.4) und wird auch in Justizvollzugsanstalten zur Besuchskontrolle eingesetzt (Ziff. 4.2.2). Für einen datenschutzgerechten Einsatz sind dabei je nach dem Zweck und den Nutzenden unterschiedliche Restriktionen zu beachten. Meine Beratung vor dem Einsatz dieser Technik ist zunehmend gefragt.

6. Werden Informationen ins Internet eingestellt, ohne zu bedenken, dass diese auch schützenswerte personenbezogene Daten enthalten, so kann dem Recht der Betroffenen auf Löschung der Daten nur aufwändig und - wenn die Daten von Suchmaschinen abgegriffen wurden - meist nicht vollständig Rechnung getragen werden (Ziff. 4.1.2). Werden dagegen bereits bei der Konzeption von Verfahren, die der Bereitstellung auch personenbezogener Informationen im Internet dienen, Datenschutzanforderungen berücksichtigt, steht der Nutzung dieses Veröffentlichungsmediums nichts im Weg (Ziff. 6.1).

7. Bereits mehrfach hatte ich die Novellierung des HSOG angemahnt. Auch der Hessische Gesetzgeber ist aufgefordert, die Rechtsprechung des Bundesverfassungsgerichts insbesondere zum Schutz des Kernbereichs privater Lebensführung und zur Kennzeichenerkennung umzusetzen. Die bisherigen Entwürfe für eine Überarbeitung des HSOG genügen dem nicht (Ziff. 4.3.1).

8. Die Polizei in Frankfurt speicherte zu einer Vielzahl vorübergehend festgenommener Teilnehmer der Demonstrationen gegen die Einführung von Studiengebühren Daten. Dabei wurden u.a. die Merkmale "gewalttätig" und "politisch links motivierte Straftäter" gespeichert - auch wenn keine konkreten Tatbeteiligungen vorgeworfen werden konnten. Die unzulässigen Datenspeicherungen wurden auf meine Intervention hin gelöscht (Ziff. 4.3.2).

9. Leider sind die bereits 2004 festgestellten Fehler und Versäumnisse der hessischen Ausländerbehörden bei den Ausschreibungen zum schengenweiten Wiedereinreiseverbot von Ausländern auch heute noch anzutreffen. Dies hat die in der Gemeinsamen Kontrollinstanz für das Schengener Informationssystem verabredete und im Geltungsbereich des Schengenabkommens einheitlich vorgenommene Prüfung auch bei zwei hessischen Ausländerbehörden ergeben (Ziff. 4.4.1).

10. Im Gesundheitsbereich stehen Datenschutzfragen im Mittelpunkt, weil höchst sensible personenbezogene Daten verarbeitet werden. Bei dem datenschutzgerechten Austausch von Patientendaten zwischen Ärzten, Krankenhäusern und Krankenkassen und bei der Gestaltung der Patienteninformationen und den technischen Lösungen sind komplexe Strukturen und Verantwortlichkeiten zu berücksichtigen. Umfassende Beratungen waren deshalb beim Aufbau einrichtungsübergreifender elektronischer Fallakten (Ziff. 4.7.1) und sicheren Netzwerken zwischen Ärzten und Krankenhäusern (Ziff. 4.7.2) sowie bei der zunehmenden Kooperation zwischen Medizinischen Versorgungszentren und Kliniken (Ziff. 4.7.4) erforderlich. Auch bei der Erstellung des Datenschutzkonzepts für einen europäischen Forschungsverbund zu speziellen Lungenerkrankungen fand intensive Beratung statt (Ziff. 4.7.3).

11. Ein Dauerbrenner sind die datenschutzrechtlichen Fragestellungen, die im Zusammenhang mit der Gewährung von Sozialleistungen entstehen, sei es zur Verhältnismäßigkeit von Maßnahmen zur Bekämpfung von Leistungsmissbrauch (Ziff. 4.8.1), der Auskunftspflichten gegenüber Sozialbehörden (Ziff. 4.8.2 - Träger der freien Wohlfahrtspflege gegenüber Hartz IV-Stellen; Ziff. 4.10 - Finanzbehörden gegenüber Arbeitslosengeld II-Stellen) oder den Nachweispflichten für eine Rundfunkgebührenbefreiung (Ziff. 7.1.1).

12. Melderegisterauskünfte als Sammelauskünfte an Adresshändler sind bei der derzeitigen Rechtslage nur schwer zu begrenzen. Zwar dürfen schon heute Sammelauskünfte nur erteilt werden, wenn schutzwürdige Belange Betroffener nicht beeinträchtigt werden. Dies ist in der Praxis nicht zu gewährleisten, weil nicht erkennbar ist für welche Zwecke und ggf. für welche Auftraggeber die Auskünfte begehrt werden. Deshalb sind dringend Änderungen im Hessischen Meldegesetz erforderlich. Die um Sammelauskünfte Ersuchenden müssen zur Angabe des Auftraggebers und des Zwecks und zur Einhaltung der Zweckbindung verpflichtet und für die Betroffenen muss mindestens ein Widerspruchsrecht gegen die Datenweitergabe zu Direktwerbezwecken vorgesehen werden (Ziff. 5.3).

1. Einführung

1.1 Allgemeines

Wer mobil sein will, hinterlässt eine Vielzahl von Spuren. Das war schon früher so und war immer riskant. Daher gibt es den alten Spruch von Laotse "Gut geht, wer ohne Spuren geht". Wer heute unbeobachtet mobil sein möchte, ist auf Sicherheitspfade angewiesen. Solche Pfade eröffnet ihm der Datenschutz. Der moderne Datenschutz entstand bekanntlich in Hessen. Die hessischen Regelungen entfalteten bis ins Ausland Vorbildwirkung. Mittlerweile haben Bund, Länder und die Europäische Gemeinschaft auf dem Gebiet des Datenschutzes nachgezogen und teilweise im Hinblick auf den Datenzugangsschutz (Informationsfreiheit) überholt. Mehr noch: der deutsche Datenschutz steht gegenwärtig auf dem gemeinschaftsrechtlichen Prüfstand. Bezogen auf die gemeinschaftsrechtlich gebotene Unabhängigkeit des (gesamten) Datenschutzes ist wieder ein hessisches Vorbild gefragt. Das Problem liegt in der Kollision von institutioneller Unabhängigkeit des Datenschutzes und der Ministerialverantwortlichkeit. Einen ministerialfreien Datenschutz gibt es in Deutschland aus verfassungsrechtlichen Gründen, d.h. mit Rücksicht auf die nationale Ausgestaltung der Gewaltenteilung, aus verständlichen Gründen nicht. Bei einer Zusammenführung von privatem und öffentlichem Bereich ließe sich die Gewaltenteilung jedoch auch jenseits der Ministerialverantwortlichkeit wahren. Es kommt nur darauf an, Unabhängigkeitsprinzip und Verantwortlichkeitsprinzip zu harmonisieren. Aus der Sicht des Hessischen Datenschutzbeauftragten ist das realisierbar, wenn dem HDSB unter Beibehaltung seiner Unabhängigkeit auch der private Bereich in der Zuständigkeit des Landes übertragen und dabei seine parlamentarische Verantwortlichkeit verstärkt würde. Zu denken wäre an eine parlamentarische Kontrollkommission nach dem Vorbild etwa der G10-Kommission. Eine derartige Kommission bietet sich mit Rücksicht auf den Grundrechtsschutz an. Das Modell hat den Vorteil, dass auf dem Gebiet des Datenschutzes die Rechte des Parlaments gravierend verstärkt würden. Die Einzelheiten bedürfen noch sorgfältiger Prüfung. Der Gesetzgeber verfügt hinsichtlich der konkreten Ausformung des Datenschutzes über eine weitgehende Gestaltungsfreiheit. Der materielle Datenschutz ist im Übrigen grundrechtlich verbürgt, ohne dass es einer Änderung des Grundgesetzes oder der Hessischen Verfassung bedürfte. Allerdings ist das Grundrecht auf informationelle Selbstbestimmung nicht ausdrücklich dort aufgeführt. Vielmehr handelt es sich um ein unbenanntes Grundrecht, das durch das Volkszählungs-Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65,1) getauft wurde. Aus diesem Grund veranstaltete die Konferenz der Datenschutzbeauftragten am 15. Dezember 2008 zusammen mit dem Bundesverfassungsgericht in Karlsruhe eine Feier "25 Jahre Volkszählungsurteil", auf der die deutsche Vorreiterrolle auf dem Gebiet des Datenschutzes noch einmal deutlich hervortrat. Wie alle Grundrechte hat das unbenannte Grundrecht auf informationelle Selbstbestimmung mehrere Dimensionen. Auch der vorliegende Tätigkeitsbericht beginnt mit nach den Hauptstoßrichtungen des Datenschutzes unterscheidenden allgemeinen Bemerkungen. Daran anknüpfend wird auf die Rechtsentwicklung des Datenschutzes im Berichtszeitraum sowie auf die Rechtsstellung des Hessischen Datenschutzbeauftragten eingegangen. Es folgen Überblicke über die Entwicklungen des Datenschutzes auf europäischer Ebene und auf der Ebene des Bundes, namentlich über die die Rechtsprechung des Bundesverfassungsgerichts. Den Schwerpunkt dieses Tätigkeitsberichts bilden landesspezifische datenschutzrechtlich relevante Fragestellungen und Entwicklungen im Zusammenhang mit der Videoüberwachung und der Bereitstellung von Daten im Internet, im Bereich der Justiz, der Polizei, des Ausländerrechts, der Schulen und Schulverwaltung, des Gesundheitswesens, des Sozialwesens, des Personal- und Finanzwesens, der Kommunen und sonstigen Selbstverwaltungskörperschaften. Bei den Prüfungen und Beratungen ist die Untersuchung der eingesetzten oder geplanten Technik und die Abschätzung von deren Folgen oft unverzichtbare Voraussetzung für die Beurteilung, ob das Recht auf informationelle Selbstbestimmung beeinträchtigt ist. Rechtliche und technische Bewertungen verzahnen sich zunehmend. Der Bilanzbericht und die vom Hessischen Datenschutzbeauftragten mitgetragenen Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließen wiederum den Tätigkeitsbericht ab.

1.2 Datenschutz

Im Jahr 2008 ergingen einige richtungweisende Entscheidungen des Bundesverfassungsgerichts zum Datenschutz. Am spektakulärsten war das Urteil vom 27. Februar 2008 zur "Online-Durchsuchung" (1 BvR 370/07 und 1 BvR 595/07, NJW 2008, 1042 mit Anm. Kutscha, NJW 2008, 1042 ff.), mit dem das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kreierte (kritisch Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411 ff.; Sachs/Krings, Das neue "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008,481 ff., positiv Hirsch, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, NJOZ 2008, 2902 ff.; Leisner, Das neue "Kommunikationsgrundrecht" - Nicht Alibi für mehr, sondern Mahnung zu weniger staatlicher Überwachung, NJW 2008, 2902 ff.). Unmittelbar auf Hessen bezogen war das Urteil vom 11. März 2008 (1 BvR 2074/05, 1 BvR 1254/07, NJW 2008, 1505, hierzu Besprechung durch Roßnagel, Verfassungsrechtliche Grenzen polizeilicher Kfz-Kennzeichenerfassungen, NJW 2008, 2547 ff.), mit der die Regelung des § 14 Abs. 4 HSOG über die automatisierte Erfassung von Autokennzeichen aufgehoben wurde. Im Streit um die Vorratsdatenspeicherung ergingen bereits Entscheidungen über Eilanträge (Beschluss vom 15. Oktober 2008, 2 BvR 236/08, 237/08, DVBl. 2008, 1566 sowie Beschluss vom 28. Oktober 2008, 1 BvR 256/08, DVBl. 2008, 1669). Ein Überblick über die datenschutzrechtlich relevante Rechtsprechung findet sich unter Ziff. 1.3.2.

1.2.1 Abwehrkomponente

Die Abwehrkomponente des Datenschutzes richtet sich gegen die öffentliche Gewalt. Im Verfassungsstaat gilt für das Verhältnis von Staatsgewalt und Gewaltunterworfenen das Verteilungsprinzip. Danach ist die Freiheit der Einzelnen als etwas vom Staat Gegebenes prinzipiell unbegrenzt, während die Möglichkeiten des Staates zu Eingriffen in diese Sphäre prinzipiell begrenzt sind. Eingriffsmöglichkeiten muss sich der Staat durch Erlass von Befugnisnormen erst schaffen, wobei er den verfassungsmäßigen Bindungen bei Grundrechtsbeschränkungen unterliegt. Dies gilt auch für Eingriffe in die informationelle Selbstbestimmung durch den Staat. Auch hier benötigen Eingriffe Befugnisnormen, bei deren Erlass und Anwendung die allgemeinen (verfassungskonkretisierenden) Datenschutzgrundsätze zu beachten sind. Demzufolge ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, eine Rechtsvorschrift ordnet sie an oder lässt sie zu

oder der Betroffene willigt hierzu ohne jeden Zweifel ein (repressives Verbot mit Zulassungsvorbehalt). Die Einwilligung muss ohne jeden Zwang erfolgen, wobei der Zwang insbesondere bei der elektronischen Kommunikation so erdrückend empfunden werden kann, dass die Einwilligung nur in Form einer positiven Abgabe einer Einwilligungserklärung ausgesprochen werden kann (zu den Anforderungen an die Freiwilligkeit BGH, Urteil vom 16. Juli 2008, VIII ZR 348/06, NJW 2008, 3055, 3056). Die Zulassung der Verarbeitung personenbezogener Daten muss dann für festgelegte, eindeutige und rechtmäßige Zwecke erfolgen (Zweckbindungsgrundsatz). Die Verarbeitung personenbezogener Daten ist ferner nur zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der Daten verarbeitenden Stelle für den jeweils damit verbundenen Zweck erforderlich ist (Erforderlichkeitsgrundsatz). Der Erforderlichkeitsgrundsatz wird schließlich dahingehend erweitert, dass bei der automatisierten Verarbeitung personenbezogener Daten das Verfahren auszuwählen oder zu entwickelt ist, das die zur Zweckerreichung nötige Menge personenbezogener Daten so gering wie möglich hält.

1.2.2 Schutzkomponente

Die Schutzkomponente erlangte Brisanz in den "Datenskandalen", die im Berichtszeitraum die Öffentlichkeit bewegten und den Bemühungen um eine Aktualisierung des BDSG den nötigen Motivationsschub verliehen. Ließen die gemeinsamen Mitarbeiterkontrollen bei Lidl, Telekom, Lufthansa und Gerling sich durch fehlendes Unrechtsbewusstsein erklären (vgl. Dann/Gastell, Gemeinsame Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, NJW 2008, 2945 ff.), so beruhte die Kreditkarten-Datenpanne im Dezember 2008 auf grobem Fehlverhalten. Die Panne entstand, als ein Kurier die Datensätze, die auf Mikrofiches gespeichert waren, vom Kreditkarten-Dienstleister Atos Worldline in Frankfurt am Main zur Berliner Landesbank verbringen sollte. Die Datensätze wurden dann aber in einem Paket bei der "Frankfurter Rundschau" aufgefunden. Die in diesem Zusammenhang von Bundespolitikern ausgesprochenen Schuldzuweisungen an Kontrollorgane der Länder entbehrten zwar der Grundlage, die Pannen zeigen jedoch auch, dass die staatlichen Kontrollmöglichkeiten verbesserungsbedürftig sind. Die erwähnten Pannen betrafen zwar schwerpunktmäßig den privaten Bereich, wirkten sich aber auch auf den öffentlichen Bereich aus. Dies ist ein weiterer Beleg dafür, dass die Trennung von öffentlichem und privatem Bereich nicht mehr zeitgemäß ist.

1.2.3 Datenzugangsschutz

Das Grundrecht auf informationelle Selbstbestimmung umfasst auch einen Anspruch des Einzelnen auf Information über seine bei der Behörde gespeicherten persönlichen Daten (vgl. BVerwG, Urteil vom 28. November 2007, 6 A 2.07, DÖV 2008, 276, Auskunftsanspruch gegenüber dem Bundesnachrichtendienst). Der G10-Kommission steht bei der Festlegung des richtigen Zeitpunkts der Mitteilung der Telefonüberwachung an den Betroffenen eine Beurteilungsermächtigung zu (BVerwG, Urteil vom 23. Januar 2008, 6 A 1.07, DVBl. 2008, 850).

1.3 Rechtsentwicklung

1.3.1 Überblick

Die Gesetzgeber in Bund und Land und auf Gemeinschaftsebene waren auch im vorliegenden Berichtszeitraum rührig und erließen eine Vielzahl datenschutzrechtlich relevanter Vorschriften (vgl. den Bericht von Gola/Klug, Die Entwicklung des Datenschutzrechts, NJW 2008, 2481 ff.) Diese sind im jeweiligen Sachzusammenhang gewürdigt. Die dem Datenschutz immer wieder entgegengehaltenen Belange der Abwehr von Kriminalität und Terrorismus beeinflussten vor allem das Strafprozessrecht, wo nach einem "stimmigen System" der Beweisverbote gesucht wird (hierzu Wolfgang Mitsch, Strafprozessuale Beweisverbote im Spannungsfeld zwischen Jurisprudenz und realer Gefahr, NJW 2008, 2295 ff.) Mit der beliebten Forderung auf Verankerung des Datenschutzes im Grundgesetz (vgl. nur Renate Künast, "Meine Daten gehören mir" - und der Datenschutz gehört ins Grundgesetz, ZRP 2008, 201) lassen sich derartige Entwicklungen nicht besser steuern als nach der gegebenen Verfassungsrechtlage (skeptisch nunmehr auch Hans Peter Bull, Neue Bewegung im Datenschutz, ZRP 2008, 233 ff., 236). Denn auch ein neues Grundrecht könnte nicht schrankenlos formuliert werden. Eher würden solche Schranken die Rechtsprechung an einer flexiblen und zeitgemäßen Rechtsfortbildung hindern.

1.3.2 Rechtsprechung

Das in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete Grundrecht auf informationelle Selbstbestimmung umfasst auch die Befugnis des Einzelnen, grundsätzlich zu bestimmen, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Auch die Veröffentlichung der Vergütung der Vorstände gesetzlicher Krankenkassen wird vom Schutzbereich des Grundrechts umfasst. Das Grundrecht auf informationelle Selbstbestimmung ist jedoch nicht schrankenlos gewährleistet. Beschränkungen auf einer verfassungsmäßigen gesetzlichen Grundlage, die insbesondere dem Grundsatz der Verhältnismäßigkeit genügen, sind zulässig. Eine derartige Grundlage stellt nach Ansicht der 1. Kammer des Ersten Senats des BVerfG § 35a Abs. 4 Satz 2 SGB IV dar. (Beschluss vom 25. Februar 2008, 1 BvR 3255/07, NJW 2008, 1435), der den legitimen Zweck verfolgt, die Beitragszahler und die Öffentlichkeit über den Einsatz öffentlicher Mittel, die auf gesetzlicher Grundlage erhoben werden, zu informieren. Recht rigide ging die 1. Kammer des Zweiten Senats mit einem Beamten um, dessen Steuerhinterziehung dem Dienstherrn durch die Weitergabe von in Selbstanzeige offenbarten Steuerdaten zur Kenntnis gebracht worden war. Danach ist Beschränkung der informationellen Selbstbestimmung durch § 125c Abs. 4 und 6 Satz 2 BRRG, § 30 Abs. 4 Nr. 5 AO verfassungskonform (Beschluss vom 6. Mai 2008, 2 BvR 336/07, NJW 2008, 3489). Der Datenschutz wird verstärkt durch den Beschluss der 3. Kammer des Zweiten Senats vom 5. Mai 2008 (2 BvR 1801/06, NJW 2008, 2422), der die Durchsuchung einer Rechtsanwaltskanzlei nur unter engen Voraussetzungen für zulässig erklärte und dabei den Schutz von Berufsgeheimnisträgern in Beziehung zur informationellen Selbstbestimmung setzte (zur Durchsuchung einer Arztpraxis BVerfG, Beschluss vom 21. Januar 2008, 2 BvR 121/07, BeckRS 2008, 31921). Ähnlich argumentierte der EGMR (Urteil vom 16. Oktober 2007, 74336/01, Wieser u. Bicos Beteiligungen GmbH/Österreich, NJW 2008, 3409 mit Anm. Stefanie Schork). Eine unnötige Beschneidung des Landesgesetzgebers bedeutet die Interpretation der Regelungs-

reichweite von § 203 StGB durch das OLG Koblenz (Beschluss vom 3. Juni 2008, 1 Ss 13/08, NJW 2008, 2794). Auch für die hessische Verwaltung bedeutsam ist die Entscheidung des OLG Oldenburg vom 20. Mai 2008 (13 WF 93/108, NJW 2008, 3508), wonach ein Detektiv für eine illegale GPS-Observierung keine Kostenerstattung verlangen kann. Im Verhältnis zwischen Datenschutz und Pressefreiheit entschied der EuGH im Urteil vom 16. Dezember 2008 (Rs C73/07 - Tietosujavaltuutettu/Satakunnan Markkinapörssi Oy u. a) zugunsten der Pressefreiheit.

1.4 Daseinsvorsorge

1.4.1 Herleitung

"Daseinsvorsorge" ist schon deshalb ein Rechtsbegriff, weil der Ausdruck in die Gesetzsprache und Rechtsprechung eingegangen ist. Im Schrifttum wird zwar gelegentlich noch die rechtliche Relevanz der Daseinsvorsorge bestritten (vgl. Krajewski, Rechtsbegriff Daseinsvorsorge?, VerwArch 2008, 174 ff.; Maurer Allgemeines Verwatungsrecht, 17. Aufl. 2009, § 1 Rn 16a). Der Rechtsbegriff der Daseinsvorsorge dagegen hat die Struktur eines Rechtssatzes. Ein Rechtssatz formuliert Tatbestand und Rechtsfolge einer Norm. Der Tatbestand besteht in der Regel in der abstrakten Beschreibung eines Lebenssachverhalts. Bei der Daseinsvorsorge fallen abstrakte Beschreibung des Daseinsvorsorgegegenstandes und Begriff im Tatbestand zusammen. Abstrakt bezieht sich der Begriff der Daseinsvorsorge auf im allgemeinen Interesse liegende Aufgaben. Welche Aufgaben das im Einzelnen sind, lässt sich nicht ein für allemal festlegen, weil es keinen abschließenden Katalog der öffentlichen Aufgaben gibt. Generell steht aber fest, dass es für den Alltag in einem zivilisierten Verfassungsstaat unverzichtbare und damit staatlich zu garantierende Leistungen geben muss; Leistungen für die ein Versorgungsbedürfnis der Allgemeinheit besteht. Das Versorgungsbedürfnis der Bevölkerung richtet sich nach dem allgemeinen Lebensstandard. Das gilt für den Gegenstand der Vorsorge wie auch für die qualitativen Anforderungen an ihre Erfüllung. Die daraus folgende Unbestimmtheit, die immer wieder dem Rechtsbegriff der Daseinsvorsorge entgegengehalten wird, bedeutet gerade seine Stärke, nämlich die Entwicklungsoffenheit.

1.4.2 Anwendungsbereich

Erfasst werden Bereiche

- der Versorgungswirtschaft (Ver- und Entsorgung),
- des Verkehrswesens (Infrastruktur, Verkehrswirtschaft),
- des Rundfunks ("Grundversorgung"),
- der Telekommunikation ("Universaldienste") und
- des Kreditwesens, ferner
- Bildungs-, Sozial-, Gesundheits-, Kultur- und Freizeiteinrichtungen.

1.4.3 Rechtsfolgen

Die Daseinsvorsorge ist als "Vorsorge zur optimalen Freiheitsverwirklichung" essenzielle staatliche Aufgabe. Das bedeutet jedoch nicht, dass der Staat diese Aufgabe selbst erfüllen müsste. Ein Gutteil der Daseinssicherung, kann jedoch ebenso (oder besser) durch Private erfolgen. Der Staat muss hier lediglich durch Intervention oder auf sonstige Weise gewährleisten, dass die Daseinssicherung tatsächlich erfolgt. Von wem die Leistung erbracht wird, spielt keine Rolle. Auch das Wie, d.h. in welcher Rechtsform die Aufgaben der Daseinsvorsorge wahrgenommen werden, ist nachrangig. Wie Daseinsvorsorge im Wettbewerb möglich ist, kommt eine Daseinsvorsorge durch Wettbewerb in Betracht. Auch im Wettbewerb darf der Staat die Leistungsaufgaben der Daseinsvorsorge nicht dem freien Spiel der Kräfte überlassen. Bedient sich der Staat zur Erfüllung seiner Aufgaben oder zur eigenen Betätigung der Formen und Regelungen des Privatrechts, bleibt er an das Gemeinwohl gebunden. Daseinsvorsorge bedeutet, dass selbst beim Handeln in Privatrechtsform öffentlich-rechtliche Grundsätze gelten. Der Begriff der Daseinsvorsorge dient somit dazu, in den leistenden Funktionen des modernen Staates, ein öffentlich-rechtliches Element aufzuweisen. Es kommt zulasten der Privatautonomie zu einer Entprivatisierung des Privatrechts. Die Gemeinwohlbindung geht privaten Interessen vor. Die Grundrechte gelten unmittelbar. Datenschutzrechtlich zählen die Leistungen der Daseinsvorsorge zum öffentlichen Bereich.

2. Europa

2.1 Gemeinsame Kontrollinstanzen für das Schengener Informationssystem und für EUROPOL

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrnehmung der Interessen der Länderdatenschutzbeauftragten in den europäischen Kontrollinstanzen für Schengen und EUROPOL übertragen. Der Beitrag stellt die Arbeitsschwerpunkte der Sitzungen der Kontrollinstanzen im Berichtszeitraum dar.

2.1.1 Gemeinsame Kontrollinstanz Schengen

Im 36. Tätigkeitsbericht (Ziff. 3.1) hatte ich berichtet, dass die bereits zum 1. Mai 2004 der EU beigetretenen Staaten mit Ausnahme Zyperns seit Ende 2007 auch an dem erweiterten Schengener Informationssystem (SIS I Plus) teilnehmen. Rumänien und Bulgarien haben derzeit noch Beobachterstatus, da das Schengener Durchführungsübereinkommen (SDÜ) ihnen gegenüber noch nicht in Kraft gesetzt wurde. Seit November 2008 sind auch die Schweiz und Liechtenstein - als nicht zur EU gehörig - vollwertige Schengen-Staaten.

Die Erweiterung des Schengenraums um die neuen europäischen Länder hat zu einer Zunahme der Datensätze im SIS um ca. 23 v.H. auf fast 23 Millionen geführt.

Die Gemeinsame Kontrollinstanz (GK) prüft in regelmäßigen Abständen, ob Datenspeicherungen von mittlerweile zu EU-Bürgern gewordenen Personen im SIS enthalten sind.

2.1.1.1 Schengener Informationssystem der zweiten Generation (SIS II)

In den letzten Tätigkeitsberichten (36. Tätigkeitsbericht, Ziff. 3.1; 35. Tätigkeitsbericht, Ziff. 3.1.1) hatte ich berichtet, dass das SIS ausgebaut werden soll, da dessen Technik auch mit SIS I Plus angesichts des rasant angestiegenen Datenumfangs durch den erweiterten Teilnehmerkreis an seine Grenzen stößt. Die von mir beschriebenen neuen Rechtsgrundlagen für das SIS II sind zwar veröffentlicht, finden aber erst dann Anwendung, wenn das SIS II in Echtbetrieb - voraussichtlich Anfang 2009 - geht.

Die GK wurde in die Vorbereitung zur Implementierung von SIS II eingebunden. Sie hat sich zu verschiedenen Fragen der Migration von Daten aus SIS I Plus in SIS II geäußert. Vor allem ging es um datenschutzrechtliche Anforderungen, die an einen derartigen Testlauf gestellt werden, insbesondere die Sicherstellung der Anonymisierung der dort verwandten Daten.

Weitere Aufgabe der GK wird es in der nächsten Zeit sein, den reibungslosen Übergang ihrer Kontrolltätigkeiten auf die in den neuen Rechtsgrundlagen vorgesehenen Kontrollinstanzen zu gewährleisten. Demnächst wird die Kontrolle durch den Europäischen Datenschutzbeauftragten hinsichtlich des zentralen Teils des SIS und der damit zusammenhängenden Fragen vorgenommen werden. Hinzu kommen die nationalen Kontrollinstanzen in den einzelnen Schengen-Staaten, deren Zusammenarbeit durch die in den Rechtsakten vorgesehenen gemeinsamen Sitzungen formalisiert wird.

2.1.1.2 Ausschreibungen zur verdeckten Registrierung

Die GK hatte sich mit der Frage auseinanderzusetzen, ob - wie vom Rat gewünscht - das SIS zum Austausch von Informationen über sog. Unruhestifter (troublemakers) bei politischen Gipfeltreffen oder Massenveranstaltungen genutzt werden kann. Als Rechtsgrundlage für die Speicherung sollte nach den Plänen des Rates Art. 99 SDÜ hinzugezogen werden.

Art. 99 SDÜ

(1) Daten in Bezug auf Personen … werden nach Maßgabe des nationalen Rechts des ausschreibenden Mitgliedstaats zur verdeckten Registrierung aufgenommen.

(2) Eine Ausschreibung dieser Art ist zulässig zur Strafverfolgung und zur Abwehr von Gefahren für die öffentliche Sicherheit, wenn

a) konkrete Anhaltspunkte dafür vorliegen, dass der Betroffene in erheblichem Umfang außergewöhnlich schwere Straftaten plant oder begeht, oder
b) die Gesamtbeurteilung des Betroffenen, insbesondere aufgrund der bisher von ihm begangenen Straftaten, erwarten lässt, dass er auch künftig außergewöhnlich schwere Straftaten begehen wird.

Voraussetzung ist also sowohl im Fall der Strafverfolgung als auch bei der Gefahrenabwehr, dass es um "außergewöhnlich schwere Straftaten" geht. Diese Anforderung sah die GK bei den sog. Unruhestiftern nicht als gegeben an. Sie hatte vielmehr die Befürchtung, dass die Zulassung dieser Ausschreibungskategorie dazu führt, dass auch unverdächtige Personen im SIS ausgeschrieben werden könnten. Hinzu kommt, dass die GK grundlegende Zweifel an der Wahl der Ausschreibungskategorie hatte. Während die Ausschreibung zur verdeckten Registrierung nach Art. 99 SDÜ das Ziel verfolgt, beispielsweise die Reisewege einer Person zu registrieren und der verdeckte Charakter der Maßnahme gewahrt bleiben soll, kommt es bei dem Vorhaben des Rats gerade darauf an, bestimmte Personen von einer Veranstaltung fernzuhalten und evtl. festzunehmen.

2.1.1.3 Gemeinsame Überprüfung der Ausschreibungen von Dritt-Ausländern zur Einreiseverweigerung

Im Jahr 2004 hatte die GK eine europaweit koordinierte Prüfung von Ausschreibungen zur Einreiseverweigerung nach Art. 96 SDÜ initiiert. Über das Ergebnis der Kontrollen durch die jeweiligen Datenschutzbeauftragten in den Schengen-Staaten habe ich im 33. Tätigkeitsbericht (Ziff. 3.2) berichtet.

Art. 96 SDÜ

(1) Die Daten bezüglich Drittausländern, die zur Einreiseverweigerung ausgeschrieben sind, werden aufgrund einer nationalen Ausschreibung gespeichert, die auf Entscheidungen der zuständigen Verwaltungsbehörden und Gerichten beruht, wobei die Verfahrensregeln des nationalen Rechts zu beachten sind.

(2) Die Entscheidungen können auf die Gefahr für die öffentliche Sicherheit und Ordnung oder die nationale Sicherheit, die die Anwesenheit eines Drittausländers auf dem Hoheitsgebiet der Vertragspartei bedeutet, gestützt werden. …

(3) Die Entscheidungen können ebenso darauf beruhen, dass der Drittausländer ausgewiesen, zurückgewiesen oder abgeschoben worden ist, wobei die Maßnahme nicht aufgeschoben oder aufgehoben worden sein darf, ein Verbot der Einreise oder des Aufenthaltes enthalten oder davon begleitet sein muss und auf der Nichtbeachtung des nationalen Rechts über die Einreise oder den Aufenthalt von Ausländern beruhen muss.

Im März d.J. beschloss die GK, einen follow-up-check der damaligen Feststellungen vorzunehmen, um zu prüfen, ob die seinerzeit festgestellten Defizite weiterhin bestehen. Die Ausschreibungen nach Art. 96 SDÜ machen immer noch ca. 90 v.H. der personenbezogenen Ausschreibungen im SIS aus. Mängel bei dieser Ausschreibungskategorie wirken sich deshalb besonders auf die Fehlerquote des SIS insgesamt aus. Festzustellen waren zum einen Fehler, die die Voraussetzungen der Speicherung selbst betreffen. Zum anderen ging es vor allem um die Einhaltung der vorgesehenen Überprüfungs- und Löschungsfristen sowie Dokumentationspflichten. Deutschland hat die Überprüfung mittlerweile abgeschlossen (die Prüfung in Hessen wird unter Ziff. 4.4.1 dargestellt). Auch eine Vielzahl anderer Schengen-Länder haben ihre Prüfberichte erstellt und dem Sekretariat der GK übermittelt. Derzeit wird von diesem eine Synthese der Ergebnisse erstellt, um dann Verbesserungsvorschläge auszuarbeiten.

2.1.1.4 Gemeinsame Überprüfung der Ausschreibungen zur vorläufigen in Gewahrsamnahme und zur Wohnsitz- und Aufenthaltsermittlung

Die GK unternimmt zur Zeit eine weitere gemeinsame Überprüfung von Ausschreibungen im SIS. Dabei geht es zum einen u.a. um Vermisste und andere Personen sowie Minderjährige.

Art. 97 SDÜ

Daten in Bezug auf Vermisste oder Personen, die im Interesse ihres eigenen Schutzes oder zur Gefahrenabwehr auf Ersuchen der zuständigen Behörde oder des zuständigen Gerichts der ausschreibenden Vertragspartei vorläufig in Gewahrsam genommen werden müssen, werden aufgenommen, damit die Polizeibehörden den Aufenthalt der ausschreibenden Vertragspartei mitteilen oder die Person in Gewahrsam nehmen können, um deren Weiterreise zu verhindern, soweit es das nationale Recht erlaubt. Dies gilt insbesondere für Minderjährige und Personen, die aufgrund einer Anordnung einer zuständigen Stelle zwangsweise untergebracht werden müssen. …

Die andere Ausschreibungskategorie betrifft u.a. Zeugen im Strafverfahren.

Art. 98 Abs. 1 SDÜ

Daten in Bezug auf Zeugen sowie auf Personen, die im Rahmen eines Strafverfahrens wegen Taten vor Gericht erscheinen müssen, derentwegen sie verfolgt werden oder Personen, denen ein Strafurteil oder die Ladung zum Antritt einer Freiheitsentziehung zugestellt werden muss, werden auf Ersuchen der zuständigen Justizbehörden im Hinblick auf die Mitteilung des Wohnsitzes oder des Aufenthalts aufgenommen.

Beide Ausschreibungskategorien zusammen ergaben immerhin in Deutschland Speicherungen zu ca. 4.000 Personen.

Die GK hat einen Fragebogen ausgearbeitet, der in allen Mitgliedstaaten bearbeitet wird. Derzeit werden die Rechtsgrundlagen für die Ausschreibungen und die Praxis in den Schengen-Staaten zusammengetragen. In einem weiteren Schritt soll die Rechtmäßigkeit der Ausschreibungen mittels festgelegten Kriterien geprüft werden.

2.1.2 Gemeinsame Kontrollinstanz EUROPOL

2.1.2.1 Neue Rechtsgrundlage für EUROPOL

In den letzten Tätigkeitsberichten (36. Tätigkeitsbericht, Ziff. 3.2.1; 35. Tätigkeitsbericht, Ziff. 3.2.1) hatte ich berichtet, dass das völkerrechtliche EUROPOL-Abkommen durch einen Ratsbeschluss nach Art. 34 Abs. 2c EU-Vertrag ersetzt werden soll. Anders als damals angenommen, ist der Beschluss noch nicht verabschiedet. Allerdings ist eine politische Einigung auf die im 36. Tätigkeitsbericht (Ziff. 3.2.1) beschriebenen Inhalte erfolgt (Beschluss des Rates zur Errichtung zu Europäischen Polizeiamts vom 24. Juni 2008, 8706/08). Es ist weiterhin vorgesehen, dass der Ratsbeschluss Anfang 2010 in Kraft tritt.

2.1.2.2 Stellungnahme zu Analysedateien

Bevor EUROPOL personenbezogene Daten zu einem bestimmten Ermittlungskomplex in einer automatisierten Datei speichern darf, ist eine Errichtungsanordnung zu erstellen.

Art. 12 EUROPOL-Abkommen - Errichtungsanordnung

(1) EUROPOL hat für jede nach Art. 10 bei ihm zur Erfüllung seiner Aufgaben geführte automatisierte Datei mit personenbezogenen Daten in einer Errichtungsanordnung, die der Zustimmung des Verwaltungsrates bedarf, festzulegen:

1. Bezeichnung der Datei,
2. Zweck der Datei,
3. Personenkreis, über den Daten gespeichert werden,
4. Art der zu speichernden Daten …
5. …
6. …
7. Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden dürfen,
8. Prüffristen und Speicherungsdauer
9. Protokollierung

Die GK wird regelmäßig vor der Errichtung neuer Analysedateien informiert und nimmt dazu Stellung. Die deutsche Delegation ist in der Arbeitsgruppe, auf die die GK einen Teil der Arbeit delegiert hat, vertreten. Einzelheiten können aufgrund des vertraulichen Inhalts der Dokumente nicht mitgeteilt werden. Derzeit unterhält EUROPOL 18 Analysedateien.

2.1.2.3 Teilnahme von Experten aus Drittstaaten in Analysegruppen von EUROPOL

Aufgrund einer Änderung des EUROPOL-Übereinkommens durch das dänische Protokoll (s. dazu 36. Tätigkeitsbericht, Ziff. 3.2.1) dürfen Experten von Drittstaaten bzw. Nicht-EU-Stellen unter bestimmten Voraussetzungen an der Tätigkeit von Analysegruppen von EUROPOL teilnehmen.

Grundlage dafür ist eine Vereinbarung zwischen EUROPOL und dem Drittstaat bzw. der anderen Behörde, in der Einzelheiten der Tätigkeit der Mitarbeiter sowie der Datenverarbeitung geregelt werden. Der GK wurden eine Reihe derartiger Vereinbarungen, u.a. mit Australien, Kroatien, USA, Schweiz, Interpol und Eurojust, zur Stellungnahme übersandt. Dabei wurde festgestellt, dass einige der Vereinbarungen schon seit 2007 existieren und es versäumt wurde, die GK im Vorfeld zu informieren.

2.1.2.4 Prüfung der Datenschutzberichte von Russland und Israel

EUROPOL kann aufgrund eines Ratsbeschlusses vom 27. März 2000 (ABlEG 2000/C 106/1 vom 13. April 2000) Vereinbarungen mit Drittstaaten und nicht EU-Stellen über den Austausch operativer, strategischer oder technischer Informationen einschließlich personenbezogener Daten abschließen. Dies gilt für Staaten und Organisationen, die der Rat nach einem bestimmten Verfahren ausgewählt hat. Die Befugnis zum Abschluss von Vereinbarungen findet sich in Art. 23 des Entwurfs für einen Ratsbeschluss zu EUROPOL wieder. Voraussetzung für den Beginn derartiger Verhandlungen ist u.a. ein Bericht über das Datenschutzniveau in dem betreffenden Land. EUROPOL hat bisher derartige Datenschutzberichte zu Russland und Israel erstellt. Die Berichte wurden der GK in einer ihrer Sitzungen von Mitarbeitern von EUROPOL vorgestellt. Die GK hat zunächst zu entscheiden, ob der Stand des Datenschutzes in Russland und Israel die Aufnahme von Verhandlungen über eine Vereinbarung zur Übermittlung personenbezogener Daten durch EUROPOL erlaubt oder nicht. Es geht also noch nicht darum, zu entscheiden, ob bestimmte personenbezogene Daten übermittelt werden dürfen. Die GK hat noch grundsätzliche Fragen, insbesondere zur Qualität der Datenschutzgesetzgebung und der Existenz von Datenschutzkontrollinstanzen, die zunächst beantwortet werden müssen.

2.2 EURODAC - Koordinierung der Kontrolle

Der Europäische Datenschutzbeauftragte und die nationalen Kontrollinstanzen haben eine Koordinierungsgruppe gegründet, um die Kontrollen des Europäischen Fingerabdrucksystems EURODAC besser abzustimmen. Der Hessische Datenschutzbeauftragte ist als Vertreter der Landesdatenschutzbeauftragten Mitglied der deutschen Delegation.

In der Zentralen Datenbank von EURODAC in Luxemburg werden die Fingerabdrücke aller Asylbewerber gespeichert, die einen Antrag in einem der Mitgliedstaaten der EU gestellt haben. Ziel ist es zum einen, zu verhindern, dass Anträge auf Asyl nacheinander in verschiedenen europäischen Staaten gestellt werden. Vorgesehen ist weiterhin der Abgleich des zentralen Datenbestands mit Daten von an der Grenze aufgegriffenen oder sich illegal in dem Mitgliedstaat aufhaltenden Ausländern.

Nach der EURODAC-Verordnung (EG Nr. 2725/2000 vom 11. Dezember 2000, ABlEG L 316/1) als Instrument der ersten Säule der EU ist der Europäische Datenschutzbeauftragte für die Kontrolle der Zentralen Datenbank in Luxemburg zuständig. Die Kontrolle bei den Stellen, die in den einzelnen Mitgliedstaaten die EURODAC-Verordnung umsetzen (in Deutschland: u.a. BKA, Bundesamt für Migration und Flüchtlinge, Polizeidienststellen), obliegt den nationalen Kontrollstellen. Um die Kontrolle besser aufeinander abzustimmen und beispielsweise die Kontrollschwerpunkte in allen Mitgliedstaaten zu vereinheitlichen, wurden die bisher schon stattfindenden Arbeitstreffen zwischen dem Europäischen Datenschutzbeauftragten und den nationalen Kontrollinstanzen in einer Koordinierungsgruppe formalisiert. Im Berichtszeitraum hat die Koordinierungsgruppe zweimal getagt. Es wurden insbesondere die bisherigen Kontrollergebnisse in den einzelnen Mitgliedstaaten vorgestellt sowie gemeinsame Kriterien für zukünftige Kontrollen entwickelt.

Man einigte sich auf drei Schwerpunkte:

Zum einen soll geprüft werden, inwieweit die Mitgliedstaaten der in Art. 18 EURODAC-Verordnung enthaltenen Unterrichtungspflicht nachkommen.

Art. 18 EURODAC-Verordnung

(1) Der Herkunftsmitgliedstaat unterrichtet die Personen, die unter diese Verordnung fallen, über

a) die Identität des für die Verarbeitung Verantwortlichen und ggf. seines Vertreters,

b) die Zwecke der Verarbeitung der Daten im Rahmen von Eurodac,

c) die Empfänger der Daten,

d) die Verpflichtung zur Fingerabdrucknahme bei Personen im Sinne des Artikels 4 oder Artikels 8,

e) die Auskunfts- und Berichtigungsrechte bezüglich sie betreffender Daten.

Ein weiteres Thema soll die Speicherung von Daten Minderjähriger sein. Hier geht es vor allem darum nachzuprüfen, ob - anders als in der EURODAC-Verordnung vorgesehen - auch schon Daten von unter 14-Jährigen gespeichert werden. Zum anderen sollen die unterschiedlichen von den Mitgliedstaaten angewandten Methoden zur Feststellung des Alters des minderjährigen Asylbewerbers untersucht werden.

Das dritte Thema umfasst Probleme, die sich bei der Anwendung von Dubli-Net ergeben. Dies ist das Netz, über das die Daten zur Bestimmung der zuständigen Asylbehörde zwischen den Mitgliedstaaten ausgetauscht werden.

Der Europäische Datenschutzbeauftragte hat berichtet, dass bei der Kontrolle der Zentralen Datenbank in Luxemburg bisher keine datenschutzrechtlichen Verstöße festgestellt wurden.

2.3 Auswirkungen des Vertrags von Lissabon auf den Datenschutz

Vor gut einem Jahr unterzeichneten die Staats- und Regierungschefs der 27 Mitgliedsländer der EU den Vertrag von Lissabon (ABlEG 2007/C 306/01), der eine grundlegende Umgestaltung der Gemeinschaftsverträge vorsieht. Auch wenn das Inkrafttreten noch nicht absehbar ist, wird es in irgendeiner Form zu Reformen kommen. Für den Datenschutz sieht der Vertrag von Lissabon eine Reihe wichtiger Änderungen vor.

Art. 16 des Vertrags über die Arbeitsweise der EU (AEUV), der den Vertrag über die EG (EGV) abändert, enthält eine Aufgabenzuweisung und einen Auftrag für die europäischen Gesetzgebungsorgane zum Erlass von Datenschutzvorschriften. Neu dabei ist, dass dies nicht nur für die Verarbeitung von personenbezogenen Daten durch europäische Organe und Einrichtungen gilt, sondern auch für die Datenverarbeitung durch die Mitgliedstaaten.

Art. 16 Abs. 2 AEUV

Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.

Eine weitere Neuerung ist, dass diese Regelung als allgemein geltende Bestimmung im Vertrag von Lissabon u.a. auch für die polizeiliche und justizielle Zusammenarbeit gilt. Durch den Wegfall der Säulenkonstruktion wird der ehemals der 3. Säule zufallende Bereich der polizeilichen und justiziellen Zusammenarbeit vergemeinschaftet und fällt damit grundsätzlich in den Anwendungsbereich von Art. 16 AEUV.

Dies kann zum einen Auswirkungen auf den Anwendungsbereich der Datenschutzrichtlinie (Richtlinie der EG 1995/46 vom 24. Oktober 1995) haben. Dort wird die Anwendung der Richtlinie u.a. für Tätigkeiten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, ausgeschlossen. Da die polizeiliche und justizielle Zusammenarbeit aber im Vertrag von Lissabon gerade vergemeinschaftet wird, ist jedenfalls eine Anwendung der Richtlinie auch auf diesen Bereich zu prüfen.

Es stellt sich weiterhin die Frage, ob der Ende November verabschiedete Rahmenbeschluss für den Datenschutz in der 3. Säule der EU (Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden vom 12. Dezember 2007, 16069/07) den Anforderungen von Art. 16 Abs. 2 AEUV genügt. Nach wie vor umfasst der Anwendungsbereich dieses Rahmenbeschlusses nicht die Datenverarbeitung in den Mitgliedstaaten, obwohl dies immer wieder von den Datenschutzbeauftragten der Mitgliedstaaten (s. Entschließung Ziff. 10.15) und erst kürzlich vom Europäischen Parlament (Bericht des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres vom 23. Juli 2008) angemahnt wurde.

Eine weitere wichtige Änderung durch den Vertrag von Lissabon bringt das erstmalig auf europäischer Ebene rechtsverbindlich ausgestaltete Grundrecht auf Datenschutz. Es findet sich in Art. 8 der Charta der Grundrechte der EU.

Art. 8 Charta der Grundrechte der EU

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betreffenden Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

In der Schlussakte des Vertrags von Lissabon wird in einer Erklärung auf die Charta der Grundrechte der EU verwiesen und die dort postulierten Grundrechte werden als rechtsverbindlich anerkannt. Für die Bürgerinnen und Bürger in Europa, die sich bei Maßnahmen durch europäische Organe oder Einrichtungen auf ein explizites Grundrecht auf Datenschutz berufen können, ist dies sicher von Vorteil. Die Entwicklung wird zeigen, ob und welche Auswirkungen die Ausformung des Europäischen Grundrechts auf die Rechtsprechung zum Datenschutz in Deutschland hat. Diese ist gehalten, darauf zu achten, dass das Europäische Grundrecht das hier maßgebliche Grundrecht auf informationelle Selbstbestimmung ergänzt, aber nicht verdrängt. Der hohe deutsche Datenschutzstandard wird vom Integrationsvorbehalt des Art. 23 Abs. 1 GG erfasst und kann durch EU-Recht nicht abgesenkt werden.

Art. 23 Abs. 1 GG

Zur Verwirklichung eines vereinten Europas wirkt die Bundesrepublik Deutschland bei der Entwicklung der Europäischen Union mit, die demokratischen, rechtsstaatlichen, sozialen und föderativen Grundsätzen und dem Grundsatz der Subsidiari-

tät verpflichtet ist und einen diesem Grundgesetz im wesentlichen vergleichbaren Grundrechtsschutz gewährleistet. Der Bund kann hierzu durch Gesetz mit Zustimmung des Bundesrates Hoheitsrechte übertragen. Für die Begründung der Europäischen Union sowie für Änderungen ihrer vertraglichen Grundlagen und vergleichbare Regelungen, durch die dieses Grundgesetz seinem Inhalt nach geändert oder ergänzt wird oder solche Änderungen oder Ergänzungen ermöglicht werden, gilt Artikel 79 Abs. 2 und 3.

Die aufgeworfenen Fragen waren Gegenstand einer Tagung, die der Hessische Datenschutzbeauftragte gemeinsam mit der Goethe-Universität Frankfurt zum Thema: "Datenschutz in Deutschland nach dem Vertrag von Lissabon" am 9. Dezember 2008 durchgeführt hat. Die Beiträge werden in einer Broschüre veröffentlicht und sind demnächst erhältlich.

3. Bund

3.1 Grobkonzept zum elektronischen Personalausweis

Das vom BMI vorgelegte Grobkonzept zum elektronischen Personalausweis, zu dem ich Gelegenheit hatte, gegenüber dem BMI eine Stellungnahme abzugeben, enthielt Schwachstellen, die auch das inzwischen verabschiedete Gesetz noch teilweise beinhaltet. Das Konzept verfolgt die Schaffung einer multifunktionalen Bürgerkarte, ohne allerdings die Risiken der angebotenen Möglichkeiten ausreichend zu beleuchten.

3.1.1 Der neue Personalausweis

3.1.1.1 Gründe der Bundesregierung für Änderungen am Personalausweis

Bei den Überlegungen, wie ein zukünftiger Personalausweis aussehen kann, hat die Bundesregierung versucht, mehrere Ziele unter einen Hut zu bringen.

Der Personalausweis soll weiterhin als hoheitliches Dokument dem Identitätsnachweis dienen und in Europa als Reisedokument gültig sein. Es wurde auch die Notwendigkeit gesehen, neue Sicherheitsvorkehrungen gegen eine unbefugte Nutzung oder Fälschungen zu ergreifen.

Eine ganz wesentliche Überlegung war aber, dem Bürger ein neues Instrument für die Nutzung des Internets zur Verfügung zu stellen. Die Bundesregierung will den Bürger bestärken, das Internet im Kontakt zur Wirtschaft (eCommerce) und zur Verwaltung (eGovernment) zu nutzen. Bisher gibt es dabei im Vergleich zu den herkömmlichen Abläufen aber wesentliche Probleme. Während man sich gegenüber der Verwaltung und in Geschäften heute durch Vorlage seines Personalausweises identifizieren kann, gibt es derzeit im Internet keine vergleichbare Möglichkeit. Ähnlich sieht es mit der Unterschrift aus. Hier existiert zwar das elektronische Äquivalent in Form der qualifizierten elektronischen Signatur, aber sie ist längst noch nicht verbreitet.

Der neue elektronische Personalausweis (ePA) soll für all diese Szenarien die richtige Lösung bieten.

3.1.1.2 Das Grobkonzept

Die Überlegungen wurden in einem Grobkonzept konkretisiert, das Mitte 2008 in der Version 2.0 zur Kommentierung veröffentlicht wurde.

3.1.1.2.1 Funktionen

Bisher diente der Personalausweis als Identitätsnachweis in verschiedenen Lebenslagen (z.B. als Reisedokument bei hoheitlichen Kontrollen, gegenüber Behörden und auch im Geschäftsverkehr, insbesondere für den Altersnachweis und für andere Nachweise). Diese Funktionen sollen weiterhin durch den ePA erfüllt werden, der bezüglich der Sicherheitsfunktionen an den elektronischen Reisepass (ePass) angeglichen wird. Darüber hinaus will die Bundesregierung, dass die Identifizierung im Geschäftsverkehr über das Internet unterstützt wird, sodass auch im Internet rechtsverbindlich Verträge abgeschlossen werden können. Weiterhin soll im Internet die Möglichkeit der pseudonymen Nutzung unterstützt werden.

Verpflichtend soll nur eine Ausweisfunktion analog dem bisherigen Personalausweis sein. Andere Funktionen sollen dem Bürger als Option angeboten werden:

- Er kann auf dem ePA seine Fingerabdrücke speichern lassen.
  Diese wären nur bei hoheitlichen Kontrollen - beispielsweise bei der Einreise - im Zugriff.
- Er kann die Funktion "Identifizierung im Internet-Geschäftsverkehr" nutzen.
  Wenn der Kommunikationspartner im Internet - dies kann eine Firma oder eine Verwaltung sein - für diese Funktion zugelassen ist, kann er damit einen Identitätsnachweis führen.
- Er kann eine qualifizierte elektronische Signatur auf den Ausweis aufbringen lassen.
  Hiermit kann er in elektronischer Form Verträge abschließen, die der Schriftform bedürfen.

3.1.1.2.2 Technik

Technisch betrachtet soll es sich beim ePA um eine Chipkarte mit kontaktloser Schnittstelle, eine sogenannte RFID-Technik (vgl. 34. Tätigkeitsbericht, Ziff. 4.2), nach ISO 14443 handeln. Auf der Vorder- und der Rückseite werden wie beim bisherigen Personalausweis das Lichtbild und die Daten zur Person gedruckt. Außerdem soll eine Zugangsnummer aufgebracht werden.

Über die kontaktlose Schnittstelle kann mit einem Lesegerät der Chip angesprochen werden. Der Chip ist dabei als ein Kleinstrechner zu betrachten, auf dem Daten gespeichert und verarbeitet werden und der die Zugriffe auf die Daten kontrolliert. Um auf die Daten zugreifen zu können, werden Berechtigungszertifikate benötigt, an denen der Chip erkennt, welche Funktion genutzt werden soll. Im Prinzip werden vier Funktionen unterschieden: hoheitliche Identitätsfeststellung unter Zugriff auf die Fingerabdrücke, Zugriff durch Behörden bei vorgelegtem Ausweis, eGovernment und eBusiness. Eine fünfte Funktion, die elektronische Signatur, arbeitet zwar auch mit Zertifikaten bei der Signaturerstellung, jedoch sind damit keine Zugriffsberechtigungen von außen verbunden.

Definition

Ein Berechtigungszertifikat ist eine Datei, die von einer dazu vorgesehenen Stelle ausgegeben wird und die zulässigen Zugriffsrechte beschreibt. Es ist entweder im Lesegerät gespeichert und weist dieses als berechtigt aus, oder es wird über das Internet präsentiert. Die Chipkarte kann die Echtheit prüfen und dann die entsprechenden Daten für den Zugriff freigeben.

Für die Funktionen sollen die Zugriffe auf Daten wie folgt kontrolliert und freigegeben werden.

- Identitätsfeststellung im Rahmen einer hoheitlichen Maßnahme mit Zugriff auf die Fingerabdrücke:
  Ein Beispiel hierfür sind Grenzkontrollen. Berechtigungszertifikate für diese Funktion werden nur restriktiv vergeben. Mit ihnen kann auf die gespeicherten Ausweisdaten und, soweit die Speicherung gewünscht wurde, die Fingerabdrücke zugegriffen werden.

- Sonstige Zugriffe durch Behörden bei Vorlage des Ausweises
  Andere Behörden (z.B. Sozialamt/Gewerbeamt) sollen für eine Identitätsfeststellung ebenfalls Zugriff auf die Ausweisdaten erhalten. Diese Behörden haben ein Berechtigungszertifikat, mit dem sie nach Eingabe der Zugangsnummer die Ausweisdaten lesen können, ohne dass sie Zugriff auf die Fingerabdrücke erhalten.

- Nachweise im Internet
  Für Identitätsnachweise oder Altersnachweise im Internet sollen Behörden (eGovernment) oder Firmen (eBusiness) als Diensteanbieter Berechtigungszertifikate erhalten können; die Unterschiede zwischen den beiden Formen liegen dabei im Zulassungsverfahren. In diesen Berechtigungszertifikaten sind insbesondere Name und Anschrift des Diensteanbieters, Kategorien der zu übermittelnden Daten, Zweck der Übermittlung, Datenschutzkontrollbehörde und letzter Tag der Gültigkeitsdauer gespeichert.

  Wenn ein Diensteanbieter die Funktion nutzen will, muss er dem Bürger die o.g. Daten anzeigen. Der Bürger kann die laut Zertifikat zu übermittelnden Daten akzeptieren. Er kann auch teilweise Daten von der Übermittlung streichen, wenn es für den Anbieter keine Pflichtfelder sind. Gibt er anschließend seine PIN ein, so generiert der Ausweis aus den freigegebenen Daten den gemäß dem Zertifikat gewünschten Nachweis und übermittelt diesen an den Diensteanbieter.

  Diese Funktion "Identifizierung im Internet" muss auf dem Ausweis aktiviert sein. Bei volljährigen Personen ist im Konzept vorgesehen, den Ausweis mit der aktivierten Funktion auszuliefern, sodass der Bürger sie deaktivieren lassen muss. Bei nicht volljährigen Personen soll sie bei Auslieferung deaktiviert sein. Sie kann dann auf Wunsch aktiviert werden.

- Erzeugen einer Signatur:
  Es gibt eine eigene Signatur-PIN, die der Bürger eingeben muss, wenn eine Signatur erzeugt werden soll.
  Die Möglichkeit der elektronischen Signatur muss der Bürger beantragen.

3.1.2 Fragestellungen und Probleme

Auch wenn das Konzept als solches bürgerfreundlich erscheint, bleiben Schwachstellen. Angesichts der rechtlichen, organisatorischen und technischen Komplexität des Vorhabens stellt sich bereits die Frage, ob der Ansatz sinnvoll ist. Dass der Bürger einen Ausweis besitzen soll, damit er seine Identität nachweisen kann, ist unstreitig. Es werden jedoch nur die tatsächlichen oder angenommenen Vorteile des Ansatzes im Konzept beschrieben, während eine Betrachtung der Risiken fehlt. Da praktisch jeder Bürger den ePA erhalten wird, müssen auch die Probleme betrachtet werden. Unter der Annahme, dass der Ansatz wie beschrieben weiter verfolgt wird, sehe ich folgende Probleme:

3.1.2.1 Freiwilligkeit

Bei drei Komponenten kann sich der Bürger entscheiden, ob er sie nutzen will. Dies betrifft die qualifizierte elektronische Signatur (QES), die Speicherung von Fingerabdrücken und die Möglichkeit des Identitätsnachweises im Internet.

Bei der qualifizierten elektronischen Signatur (QES) kann man von einer echten Freiwilligkeit ausgehen. Es gibt keinen Zwang QES zu nutzen. Falls Bürger diese Funktion jedoch wünschen, müssen sie sich diese nicht auf dem ePA zur Verfügung stellen lassen. Es gibt eine Reihe von etablierten oder kommenden Alternativen. Beispiele sind Signaturkarten von akkreditierten Zertifizierungsdiensteanbietern, die EC-Karte der Sparkassen und die geplante Gesundheitskarte.

Die Freiwilligkeit bei der Speicherung von Fingerabdrücken oder der Funktion "Identifizierung im Internet" ist zumindest nicht zwangsläufig gegeben. Es ist denkbar, dass zukünftig Kontrollen länger dauern, wenn ein Ausweis ohne Fingerabdrücke vorgelegt wird. Genauso ist es vorstellbar, dass jemand ungünstigere Konditionen erhält, wenn er sich nicht mit dem ePA im Internet identifiziert.

Zur Sicherstellung der Freiwilligkeit muss gewährleistet sein, dass:

- es bei Kontrollen keine Verschlechterung der bisherigen Rechtslage gibt, wenn Fingerabdrücke nicht gespeichert sind.
- die Funktion "Identifizierung im Internet" bei der Auslieferung deaktiviert ist, damit sie erst auf ausdrücklichen Wunsch des Bürgers aktiviert wird.

3.1.2.2 RFID

Beim jetzigen elektronischen Reisepass sehe ich aufgrund der Sicherheitsvorkehrungen keine massiven Sicherheitsprobleme durch den Einsatz von Chipkarten mit einer RFID-Technik auf Basis von ISO 14443. Dies habe ich in meinem 34. Tätigkeitsbericht (Ziff. 4.2) beschrieben. Diese Einschätzung lässt sich für den ePA nur treffen, wenn tatsächlich vergleichbare Sicherheitsmaßnahmen ergriffen werden.

3.1.2.3 Speicherung von Fingerabdrücken; Biometrie

Ziel der Speicherung von Fingerabdrücken ist es nicht, Fälschungen von Personalausweisen zu verhindern, da diese bereits heute kaum auftreten und in der Regel schnell erkannt werden. Es soll vielmehr verhindert werden, dass ähnlich aussehende Personen den ePA verwenden und damit eine fremde Identität missbrauchen. Durch den Abgleich der präsentierten Fingerabdrücke mit den auf dem ePA gespeicherten Merkmalen soll sichergestellt werden, dass die Person, die den Ausweis verwendet, tatsächlich der Ausweiseigentümer ist. Der ePA soll so als Identitätsnachweis dienen.

Wenn eine missbräuchliche Nutzung, wie im Konzept festgestellt, mit an Sicherheit grenzender Wahrscheinlichkeit aufgedeckt wird, ist zwangsläufig die Rate der fälschlich nicht erkannten Übereinstimmungen zwischen gespeichertem und präsentiertem Fingerabdruck groß. In dem Konzept wird nicht auf Probleme eingegangen, die sich durch fälschliche Zurückweisung von Ausweisinhabern oder gefälschte Fingerabdrücke ergeben. Diese Punkte müssen aber berücksichtigt werden, wenn die Konsequenzen des Einsatzes der Biometrie im Zuge von Kontrollen geregelt werden, bei denen es zu technikbedingten fehlerbehafteten Ergebnissen kommt.

Ich halte es für sinnvoll, die Erfahrungen mit dem ePass abzuwarten und zu evaluieren, bevor die Entscheidung für die Speicherung von Fingerabdrücken im Personalausweis getroffen wird.

Dies gilt umso mehr, als der Fingerabdruck ein Überwachungspotenzial besitzt. Während man seinen Fingerabdruck an vielen Stellen hinterlässt, sind andere biometrische Merkmale datenschutzfreundlicher. Dies gilt beispielsweise für die Iris oder das Venenmuster. Sie können ebenfalls zur Identifizierung genutzt werden, haben aber kein oder nur ein geringes Überwachungspotenzial. Die Entscheidung für den Fingerabdruck fiel, um an Grenzkontrollstellen eine einheitliche Technik für ePA und ePass einzuführen. Insofern erbt der ePA die Schwächen des ePass.

3.1.2.4 Identitätsnachweis im Internet und PIN

Die Identifizierung im Geschäftsverkehr über das Internet soll durch Freigabe von Daten mittels einer PIN erfolgen. Die Probleme der PIN-Nutzung sind, insbesondere seit der Einführung der elektronischen Gesundheitskarte, in den dortigen Testregionen bekannt: es gibt Bevölkerungsgruppen, die mit der Technik nicht angemessen umgehen können. Diese Gruppen können dann auch nicht problemlos die Funktion des ePA nutzen. Falls sich wie unter Ziff. 3.1.2.1 dargestellt ein faktischer Zwang ergibt, können die betroffenen Bürger nur mit Einschränkungen am Geschäftsverkehr im Internet mittels des ePA teilnehmen.

3.1.2.5 Zugriffe auf Daten und Zertifikate

Der Datenzugriff wird nach dem Konzept weitgehend über Berechtigungszertifikate, also elektronische Zugriffsberechtigungsnachweise geregelt (vgl. Ziff. 3.1.1.2.2). Die Zertifikate lassen sich dabei zwei Bereichen zuordnen:

- Verwaltungsinterne Zertifikate
  Hierbei handelt es sich um die Zertifikate für hoheitliche Kontrollen, für Zugriffe mit Eingabe der aufgedruckten Zugangsnummer und für eGovernment-Anwendungen. In diesen Fällen kann zumindest für deutsche Behörden die zugreifende Stelle als bekannt und zuverlässig vorausgesetzt werden.
  Aus dem Konzept geht nicht hervor, ob Stellen aus anderen Staaten der EU oder staatliche Stellen außerhalb der EU Zertifikate erhalten und wenn ja, für welche Zugriffe diese zugelassen sein sollen. Dies sollte auch noch im Detail für deutsche Behörden beschrieben werden.
- Berechtigungszertifikate für Geschäftszwecke
  Diese Zertifikate sollen auf Antrag vergeben werden. Es soll dabei im Zertifikat auch festgelegt sein, welche Daten für den beantragten Geschäftszweck erfragt werden.
  Es ist unklar, welche Stelle(n) aufgrund von welchen Informationen und nach welchen Kriterien die Zertifikate vergeben oder verweigern können. Hier ist eine konkretisierende Norm erforderlich.

3.1.2.6 Löschen von Daten

Fingerabdrücke, die während des Antragverfahrens im IT-System der Behörde gespeichert werden, sind frühestmöglich zu löschen. Diese Forderung ist bereits heute für den ePass umgesetzt (vgl. Ziff. 5.2).

Da die Fingerabdrücke nur als Option gespeichert werden, müssen sie im ePA gelöscht werden, wenn ein Bürger die Speicherung nicht mehr wünscht. Dies ist ein Unterschied zum ePass. Aber auch alle anderen fakultativen Daten wie die Signaturzertifikate müssen gelöscht werden, wenn der Bürger dies verlangt.
Diese Daten müssen auch gelöscht werden, wenn der ePA zurückgegeben wird.

3.1.2.7 Verlust

Zusammen mit einem PIN/PUK-Brief soll der Ausweisinhaber das Sperrkennwort erhalten, mit dem er bei Abhandenkommen des Ausweises die Funktion "Identifizierung im Internet" sperren lassen kann. Bisher ist eine telefonische Sperre vorgesehen, ohne dass klar ist, wie die Abläufe genau aussehen.

Für die qualifizierte Signatur würde sich ein anderer Ablauf ergeben. Analog zu Signaturkarten muss bei dem Zertifizierungsdienstanbieter, der die Signaturzertifikate ausgestellt hat, der Verlust gemeldet werden. Von dort würde die Sperrung des Zertifikats vorgenommen.

Die Abläufe bei einem Verlust oder Diebstahl des Ausweises müssen noch detaillierter geregelt und beschrieben werden. Insbesondere benötigt der Bürger eine Beschreibung, wie er in diesen Fällen vorgehen muss.

3.1.2.8 Technik

Die Konzeption des BMI sieht eine kontaktlose Schnittstelle (beispielsweise wie bei Zutrittskontrollsystemen) vor, um die gleiche Infrastruktur wie beim elektronischen Reisepass nutzen zu können. Dadurch kommt es zu einer Konkurrenz mit den weit verbreiteten Chipkarten die kontaktbehaftet arbeiten, denn bisher sind keine Kartenlesegeräte verfügbar die beide Schnittstellen unterstützen. Für den Bürger heißt das, dass er vor der Situation steht, entweder auf die Funktionalitäten des ePA verzichten zu müssen oder ggf. zwei Lesegeräte anzuschaffen. Da bisher an Kunden fast nur kontaktbehaftete Karten wie EC-Karten oder Signaturkarten ausgegeben wurden und auch die eGK (elektronische Gesundheitskarte) kontaktbehaftet sein wird, wäre es naheliegend gewesen, darauf aufzubauen.

Es ist im Konzept kein Vergleich zwischen den beiden Techniken bezüglich ihrer Vor- und Nachteile erfolgt. Das gilt auch für den Bereich IT- Sicherheit. Dies ist ein Manko, da gerade die RFID-Schnittstelle Angriffsflächen bietet. Selbst wenn man - wie ich - gegen die hoheitliche Identitätsfeststellung mit den Sicherheitsmechanismen des ePass keine Bedenken hat, kann diese Feststellung nicht einfach auf den ePA und alle seine Funktionen übertragen werden. Hier sind weitergehende Betrachtungen und Bewertungen nötig. Dies gilt insbesondere, da derzeit nur kontaktbehaftete Chipkarten für QES zugelassen sind. Hier sind Lösungen auf Basis des vorhandenen Signaturgesetzes zu betrachten. Es ist im Konzept nicht ausreichend dargelegt, dass für alle Einsatzszenarien eine ausreichende IT-Sicherheit gegeben ist.

Damit das System wie konzipiert funktioniert, muss die Software die Spezifikationen einhalten. Das betrifft beispielsweise die Zugriffskontrolle durch die Karte, also die Zertifikatsprüfungen, aber auch die Funktion des Verweigerns von Datenübermittlungen. Es fehlt eine Festlegung, ob und welche Komponenten inkl. der Software zertifiziert werden, welche Kriterien gelten und durch wen die Zertifizierung erfolgt.

Es muss geregelt sein, wie zu verfahren ist, wenn der Chip defekt ist. Betroffene, die die Internet-Funktionen nutzen, müssen wissen, wie sie in diesem Fall verfahren sollen. Auch wenn die Maßnahmen weitgehend mit den bei einem Verlust des ePA zu veranlassenden identisch sein werden, ist eine Information erforderlich. Falls bei einer Kontrolle der Chip nicht funktioniert, stellt sich die Situation anders dar. Hier muss es wie im Fall von falschen Ergebnissen bei der Überprüfung mittels Biometrie (Ziff. 3.1.2.3) Regelungen und Hinweise sowie eine Handlungsanleitung für das Kontrollpersonal geben.

3.1.3 Umsetzung im Gesetz

Am 18. Dezember 2008 hat der Deutsche Bundestag das auf dem Grobkonzept basierende Personalausweisgesetz (PAuswG) verabschiedet. Dabei sind einige meiner Kritikpunkte entschärft bzw. ausgeräumt worden.

Zur Freiwilligkeit gibt es Klarstellungen. Aufgrund der Beschlussempfehlung des Innenausschusses vom 17. Dezember 2008 ist in § 9 Abs. 3 PAuswG explizit formuliert worden, dass dem Ausweisinhaber keine Nachteile durch den Verzicht auf Aufnahme der Fingerabdrücke in den Ausweis entstehen dürfen. Meine grundsätzlichen Vorbehalte gegen die Aufnahme von Fingerabdrücken als biometrisches Merkmal, die ich in meiner Stellungnahme erläutert hatte, bestehen weiterhin. Es war auch der Wille, für die Funktion "Identifizierung im Internet" die Freiwilligkeit sicherzustellen. Leider ist für volljährige Personen weiterhin bei Auslieferung die Funktion aktiv und wird nur auf Wunsch deaktiviert. Allerdings muss die antragstellende Person schriftlich nach § 11 PAuswG über diese Funktion informiert werden, diese Unterrichtung schriftlich bestätigen und nach § 10 Abs. 1 PAuswG schriftlich erklären, dass sie die Funktion nutzen will. Die antragstellende Person ist zumindest informiert und kann sich dann entscheiden. Sie muss aber vor allem auch ihre Pflichten nach § 27 PAuswG beachten, die sie praktisch zum vorsichtigen Umgang mit dem Ausweis zwingt. Inwieweit dies in der Praxis immer gelingen kann, vor allem da immer wieder Ausweise hinterlegt werden sollen, sei dahingestellt.

Ausführungen, wie beim Verlust eines Ausweises zu verfahren ist, finden sich an vielen Stellen des Gesetzes. Dies sind beispielsweise die §§ 10, 11 und 27 PAuswG. Hierzu sollte es klarstellende, zusammenfassende Informationen geben, die Teil des Informationsmaterials sein könnten, das der antragstellenden Person nach § 10 Abs. 2 PAuswG zu übergeben ist.

Was die eingesetzte RFID-Technik, Fragen der Datensicherheit und andere Themen betrifft, so wird in § 34 PAuswG das BMI ermächtigt, Einzelheiten durch Rechtsverordnung zu regeln. Zu den von mir hierzu aufgeführten Problemen gibt es

daher noch keine neuen belastbaren Aussagen. Allerdings wird bei den Berechtigungszertifikaten nach § 2 Abs. 4 PAuswG nur noch zwischen hoheitlichen Berechtigungszertifikaten, die ausschließlich für die hoheitliche Tätigkeit der Identitätsfeststellung zu verwenden sind, und sonstigen Berechtigungszertifikaten unterschieden. Insofern wird es gegenüber dem Konzept Änderungen bei der Ausgestaltung von Zugriffsrechten geben. Die Vergabe der nicht hoheitlichen Berechtigungszertifikate ist in § 21 PAuswG behandelt, wobei Einzelheiten zur Vergabe von Berechtigungen und Berechtigungszertifikaten aber wiederum erst in den nach § 34 PAuswG vorgesehen Rechtsverordnungen geregelt werden.

Eine Aussage halte ich im Zusammenhang mit technischen Problemen für wichtig. § 28 Abs. 3 PAuswG lautet: "Störungen der Funktionsfähigkeit des elektronischen Speicher- und Verarbeitungsmediums berühren nicht die Gültigkeit des Personalausweises."

Durch die im Gesetz getroffenen Regelungen gibt es somit Klarstellungen und Verbesserungen bei der Freiwilligkeit und der Transparenz der möglichen Datenverarbeitungen. Eine Beurteilung der Technik und technische Details ist aber noch nicht abschließend möglich.

3.1.4 Fazit

Der elektronische Personalausweis kann neue technische Möglichkeiten eröffnen und dem Bürger auch im täglichen Leben helfen. Die nach dem Konzept wesentlichen Punkte müssen aber erfüllt werden:

- Die Freiwilligkeit der Funktion "Identifizierung im Internet" muss gegeben sein.
- Die Technik muss wie vorgesehen funktionieren.
- Unbefugte Zugriffe auf Daten müssen sicher verhindert werden.
- Der Bürger muss über die Funktionen des ePA so informiert werden, dass er in Kenntnis möglicher Chancen und Risiken sich für optionale Funktionen entscheiden kann.

3.2 Neuorganisation der Durchführung des SGB II - Zentren für Arbeit und Grundsicherung

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat auf die Bestrebung des Bundesarbeitsministeriums hingewiesen, die vom Bundesverfassungsgericht für verfassungswidrig erklärten Arbeitsgemeinschaften (von Kommunen und Arbeitsagenturen) durch Zentren für Arbeit und Grundsicherung zu ersetzen. Die bisherige Datenschutzkontrolle durch die Landesbeauftragten für den Datenschutz soll entfallen. Ein solcher Ausschluss der Landesbeauftragten von der Datenschutzkontrolle wäre jedoch datenschutzrechtlich verfehlt und verfassungswidrig.

Nach Angaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ist geplant, an die Stelle der bisherigen, vom BVerfG (Urteil vom 20. Dezember 2007 - 2 BvR 2434/04) für verfassungswidrig erklärten Arbeitsgemeinschaften von Kommunen und Arbeitsagenturen (ARGE, § 44b SGB II) sog. Zentren für Arbeit und Grundsicherung (ZAG) treten zu lassen. Der Zweite Senat des BVerfG hat mit knapper Mehrheit (5 : 3) gerügt, die ARGE als Gemeinschaftseinrichtungen seien von der Kompetenzordnung des GG nicht gedeckt und stünden mit dem Grundsatz eigenverantwortlicher Aufgabenwahrnehmung von Bund und Ländern nicht im Einklang. Es liege eine unzulässige und damit verfassungswidrige Mischverwaltung von Bund und Ländern vor. Vor diesem Hintergrund plant das Bundesarbeitsministerium, anstelle der bisherigen ARGE zukünftig ZAG zu errichten. Soweit die ZAG Leistungen für die Bundesagentur für Arbeit erbringen, soll der Bund die Rechts- und Fachaufsicht innehaben, im Übrigen soll für die Leistungen der Kommunen die Aufsicht bei den Ländern liegen. Eine grundgesetzliche Bestimmung soll die verfassungsrechtliche Basis liefern.

Die datenschutzrechtliche Brisanz der Reformüberlegungen liegt darin begründet, dass für die Datenschutzkontrolle zukünftig anders als bisher ausschließlich der BfDI zuständig sein soll, obwohl die Länder (Kommunen) bei den ZAG involviert sein werden.

Ein solcher Ausschluss der Kontrollrechte der LfD würde auf eine gravierende Verschlechterung des Datenschutzes hinauslaufen. Die bisherige und mittlerweile gut eingespielte Kooperation von BfDI und LfD bei den ARGE würde entfallen. Allein kann der BfDI an Datenschutzkontrolle nicht das schultern, was in Zusammenarbeit und vor allem durch Arbeitsteilung mit den LfD möglich ist. Außerdem würde die Effektivität der behördlichen Datenschutzbeauftragten gemindert, weil deren Zusammenwirken mit den LfD praktikabler ist als die Abstimmung mit dem BfDI.

Datenschutzrechtlich wäre wünschenswert, dass die derzeitige Konstellation durch eine entsprechende verfassungsrechtliche Regelung ausdrücklich gestattet und die bisherige Tätigkeit des BfDI und der LfD gesetzlich festgeschrieben wird. Dies bedeutet etwa beim Einsatz einer einheitlichen Informationstechnik für die ZAG die Zuständigkeit des BfDI; die Überprüfung beispielsweise des Außendienstes (§ 6 SGB II) fiele in die Zuständigkeit der LfD (vgl. zum Außendienst Ziff. 4.8.1).

Eine ausschließliche Zuständigkeit des BfDI und die damit einhergehende Verdrängung der LfD muss auch an der Vorgabe des Art. 30 GG gemessen werden.

Art. 30 GG

Die Ausübung der staatlichen Befugnisse und die Erfüllung der staatlichen Aufgaben ist Sache der Länder, soweit dieses Grundgesetz keine andere Regelung trifft oder zulässt.

Anhaltspunkte, die die alleinige Zuständigkeit des BfDI rechtfertigen könnten, liefert das Grundgesetz nicht. Offenkundig dürfte sein, dass der BfDI zuständig ist, soweit es ausschließlich um die eigene Verwaltung des Bundes geht (Art. 86 ff.

GG). Im vorliegenden Kontext geht es aber gerade darum nicht. Vielmehr ist die Konstellation mit Blick auf die Finanzverfassung so, dass die Länder das SGB II nicht als eigene Angelegenheit (Art. 83, 84 GG), sondern im Auftrag des Bundes (Art. 85 GG) auszuführen haben. Das ergibt sich aus der Verteilung der Finanzlast. Art. 104a Abs. 3 GG weist nämlich die Durchführung eines Gesetzes, das bestimmt, dass der Bund die Hälfte der Ausgaben oder mehr trägt, der Auftragsverwaltung gemäß Art. 85 GG zu. Nach alledem wird deutlich: Hinweise, die die exklusive Zuständigkeit des BfDI für die ZAG rechtfertigen könnten, bietet die Verfassung nicht. Im Gegenteil: Gerade nach der Föderalismus-Reform, mit der die Länder gestärkt werden sollen, wäre es widersinnig, die LfD zu verdrängen, obwohl die Länder bei den ZAG involviert sind.

Vor diesem Hintergrund habe ich mich gegenüber dem BfDI für die weitere Zuständigkeit der LfD betreffend das SGB II ausgesprochen. Diese Position wird auch vom BfDI vertreten.

4. Land

4.1 Querschnitt

4.1.1 Entwicklungen im Bereich Videoüberwachung

Bereits im vergangenen Jahr hatte ich über Videoüberwachungsprojekte in den verschiedensten Bereichen der Landes- und Kommunalverwaltung berichtet. Auch in diesem Jahr sah ich mich in diesem Bereich mit verschiedenen neuen Projekten konfrontiert, die ich einer datenschutzrechtlichen Bewertung unterzogen habe.

4.1.1.1 Einsatz von Videoüberwachungsanlagen in Fußballstadien

Die Polizei kann auf Grundlage des HSOG Videotechnik nicht nur zur Überwachung von Kriminalitätsbrennpunkten einsetzen. Ein weiteres häufiges Einsatzfeld sind große Sportveranstaltungen, insbesondere Fußballspiele. Der Deutsche Fußball-Bund hat Richtlinien zur Verbesserung der Sicherheit bei Bundesligaspielen aufgestellt, in denen u.a. Vorgaben zum Einsatz von Videoüberwachungsmaßnahmen enthalten sind.

§ 10 Abs. 5 DFB Richtlinie zur Verbesserung der Sicherheit bei Bundesligaspielen vom 11. Mai 2007

Innerhalb der Platzanlage und mit Blick auf den Umgriff, die Zuschauerwege und auf die Zuschauerplätze sowie in den Außenbereichen vor den Eingängen sind Videokameras mit Zoom-Einrichtungen zu installieren. Die Anlage sollte von der Befehlsstelle der Polizei zu bedienen, an die Polizeimonitore angeschlossen sein und die Möglichkeit der Standbildaufnahme zur Identifikation von Personen bieten.

Diese Regelung besagt nichts dazu, auf welcher Rechtsgrundlage und von wem diese Kameras genutzt werden können. In den Stadien ist nicht nur die Polizei präsent, vielmehr obliegt zunächst die Verantwortung für die Sicherheit während des Spieles dem Ausrichter, d.h. dem Sportverein. Dieser bedient sich dazu in der Regel externer Ordnungsdienste.

Soweit die Polizei die Videotechnik im Stadion nutzt, handelt sie im Rahmen ihrer Befugnisse zur Datenerhebung und sonstigen Datenverarbeitung an öffentlichen Orten und besonders gefährdeten öffentlichen Einrichtungen nach § 14 Abs. 1 HSOG.

§ 14 Abs. 1 HSOG

Die Polizeibehörden können personenbezogene Daten auch über andere als die in den §§ 6 und 7 genannten Personen bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass bei oder im Zusammenhang mit der Veranstaltung oder Ansammlung Straftaten oder nicht geringfügige Ordnungswidrigkeiten drohen. Die Unterlagen sind spätestens zwei Monate nach Beendigung der Veranstaltung oder Ansammlung zu vernichten, soweit sie nicht zur Abwehr einer Gefahr, zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden.

Darüber hinaus gibt es jedoch auch weitere Interessen zur Nutzung der Videoanlagen für den Ordnungsdienst ebenso wie außerhalb von Spieltagen im Rahmen der Objektsicherung.

Daher sind bei der Festlegung der datenschutzrechtlichen Anforderungen an die Nutzung dieser Anlagen eine Vielzahl von Beteiligten einzubeziehen. Neben der Polizei und dem Verein können dazu Stadionbetreiber und weitere externe Servicefirmen wie Hausmeister oder EDV-Dienstleister gehören. Je nach Rechtsform der Beteiligten sind dabei unterschiedliche Rechtsgrundlagen anzuwenden.

Dies hat zur Konsequenz, dass die Polizei verschiedene Vereinbarungen zu treffen hat. Außerdem müssen die Details in einem Verfahrensverzeichnis beschrieben sein.

Für das Stadion in Wiesbaden, in dem der SV Wehen Wiesbaden seine Heimspiele in der 2. Bundesliga austrägt, habe ich dieses Thema exemplarisch aufgegriffen und in Kooperation mit der Aufsichtsbehörde für den Datenschutz beim Regierungspräsidium in Darmstadt versucht, die Anforderungen an die unterschiedlichen Nutzungen zu beschreiben.

Für die datenschutzrechtliche Bewertung der Nutzung durch die Polizei kommt es zunächst nicht auf die Eigentumsverhältnisse der Anlage bzw. der in diesem Kontext eingesetzten Technik an. Entscheidend ist, dass die Polizei während ihrer

Nutzung der Videoanlage Daten verarbeitende Stelle ist und somit die Verantwortung dafür trägt, dass die nach dem HSOG sowie dem HDSG notwendigen Sicherungen eingehalten werden.

Soweit die Polizei die Anlage nutzt - und die Kameras steuert -, erhebt sie die Daten und ist verantwortlich. Die Erhebung der Daten durch die Polizei beginnt in dem Moment, in dem sie die Daten (Videobilder) in ihren "Hoheitsbereich" holt, d.h. auf den Monitoren in der Befehlsstelle anzeigt bzw. auf einem Server (zwischen-)speichert. Eine Übermittlung an Dritte außerhalb des öffentlichen Bereiches ist grundsätzlich zulässig, soweit die Voraussetzungen des § 23 HSOG im Einzelfall vorliegen.

§ 23 Abs. 1 HSOG

Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies zur

1. Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben,
2. Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder
3. Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person

erforderlich ist.

Um sicherzustellen, dass die rechtlichen Rahmenbedingungen eingehalten werden, ist eine konkrete Vereinbarung notwendig, die regelt, wer wann die Steuerung der Kameras übernimmt - ausgehend davon, dass die Steuerung durch die Polizei Priorität hat.

Da die Videoüberwachung durch die Polizei auf Grundlage des § 14 Abs. 1 HSOG erfolgt, ist grundsätzlich auch eine Beobachtung des Straßenraums im Zusammenhang mit Liga-Spielen zulässig. Allerdings ist für die Kameras, die ein Gebäude mit einer Gaststätte erfassen, eine Änderung insoweit notwendig, dass die vermieteten Räume ab dem ersten Stockwerk nicht einsehbar sein dürfen. Hier ist eine Begründung zur Erfassung aus dem Zusammenhang mit der Beobachtung rund um das Spiel nicht ersichtlich. Die zeitliche Dauer (Vor- und Nachlauf zum eigentlichen Spiel) bestimmt die Polizei nach den tatsächlichen Notwendigkeiten.

In das zu erstellende Verfahrensverzeichnis sind die entsprechenden Festlegungen ebenso aufzunehmen wie die Aufbewahrungsfristen und die getroffenen technischen und organisatorischen Sicherungsmaßnahmen für die gesamte von der Polizei in diesem Kontext genutzte technische Infrastruktur.

Da die Geräte, zum Teil auch die Server, mit denen die von der Polizei angestoßenen Aufzeichnungen erfolgen, vom Stadionbetreiber gestellt werden, muss es sowohl eine Vereinbarung zur Nutzungsüberlassung als auch zur Auftragsdatenvereinbarung geben. In diesem Vertrag müssen auch Festlegungen zum Unterauftragsverhältnis mit der Firma enthalten sein, die die konkrete Betreuung der EDV einschließlich der Administration übernimmt. Dies bezieht sich sowohl auf den Server als auch auf die Aufzeichnungstechnik. In diesem Kontext ist auch festzulegen, dass die Auftragnehmer die Polizei unterstützen bei der Darstellung der zu treffenden Maßnahmen für das Verfahrensverzeichnis.

Soweit die Kameras darüber hinaus auch für andere Zwecke - z. B. Objektsicherung in der Nacht - (teilweise) mitgenutzt werden sollen, muss sich die Polizei ein Informationsrecht einräumen lassen. Dies ist erforderlich, um kontrollieren zu können, dass die Anlage nicht manipuliert wird und so die getroffenen Sicherungen zur Verhinderung von unberechtigten Zugriffen auf die durch die Polizei verantwortete Nutzung umgangen werden.

Sobald alle Details geklärt sind - auch durch das Regierungspräsidium, soweit es um Maßnahmen der anderen Beteiligten im Rahmen des Bundesdatenschutzgesetzes geht -, soll das Konzept als Grundlage dienen für die Nutzung der Videotechnik in den anderen hessischen Stadien, in denen Liga-Spiele stattfinden.

4.1.1.2 Videoüberwachung an der Konstablerwache

Über die Kameras in Frankfurt hatte ich wiederholt berichtet. Probleme ergaben sich insbesondere daraus, dass seit Beginn des Kameraeinsatzes Balkone in einem Haus, das unmittelbar an der den Platz begrenzenden Straße liegt, im Blickfeld der Kameras sind. Ein vollständiges Verhindern der Einsicht durch technische Maßnahmen war mit den Ende 2000 in Betrieb genommenen Kameras nicht möglich. Daher hatte ich nach längerer Erörterung mit dem Polizeipräsidium Frankfurt schließlich akzeptiert, dass in einer Dienstanweisung geregelt wurde, dass die Beobachtung von Fensterfronten zu unterbleiben hat. Diese Regelung sollte gelten, bis neue Techniken die Ausblendung ermöglichen.

Schließlich wurden in diesem Jahr durch das Land neue Kameras beschafft, die die Umsetzung meiner o.g. Forderung ermöglichen sollten. Bei einer Nachkontrolle stellte sich jedoch heraus, dass auch weiterhin mindestens Teile der Balkone einsichtig waren. Eine vollständige Ausblendung war nur in der Weise möglich, dass dann auch die Straßenbahn- bzw. Bushaltestelle in der Mitte der Straße nicht mehr einsehbar war.

Offensichtlich war bei der Beschaffung der neuen Kameras nicht vorab ausreichend geprüft worden, dass die Ausblendung der sogenannten Privatschutzzonen flexibel genug gehandhabt werden kann.

Aufgrund dessen habe ich verlangt, die möglichen Ausblendungen auf jeden Fall so einzustellen, dass die Balkone nicht mehr beobachtet werden können, auch wenn dann einzelne Bereiche des Platzes bzw. der angrenzenden Straßen nicht mehr voll im Blickfeld sein können.

Dem ist das Polizeipräsidium dann nachgekommen.

4.1.1.3 Kameras an einer Ampelanlage - Verkehrssteuerung

Mit einer Eingabe wurde mir folgender Sachverhalt geschildert: Nach der Erneuerung einer innerörtlichen Ampelanlage entdeckten Bürger der Gemeinde, dass an der betroffenen Kreuzung im Zuge der Erneuerung der Ampelanlage auch vier Kameras angebracht worden waren. Sie vermuteten, dass diese Kameras die vier dort aufeinandertreffenden Straßen beobachten sollten. Die Ausrichtung der Kameras sei derart, dass neben den Zugängen zu Wohnhäusern auch die Eingangsbereiche eines Ladengeschäfts, zweier Arztpraxen sowie einer Rechtsanwaltskanzlei in den Aufnahmebereich falle. Aufgrund dieses Hinweises habe ich mit der zuständigen Straßenverkehrsbehörde Kontakt aufgenommen und darum gebeten, mir Sinn und Zweck dieser Kamerainstallierung zu erläutern.

Es ergab sich, dass es sich hier nicht um eine Videoüberwachungsmaßnahme im herkömmlichen Sinn handelte. Die vier Kameras dienen lediglich dazu, Induktionsschleifen zu ersetzen. Die Kameras haben eine feste Ausrichtung auf einen definierten Straßenabschnitt und sind nicht schwenk- oder zoombar. Mit Hilfe der Messfunktion der Kameras wird die Ampelanlage gesteuert, wie dies auch durch in den Straßenbelag eingelassene Induktionsschleifen geschieht. Es werden auch keinerlei Bilder auf Monitore übertragen. Allerdings können im Einzelfall Bilder erstellt werden. Auf diesen Bildern können dann der jeweilige Straßenabschnitt vor der Ampel und Fahrzeuge (soweit vorhanden) gesehen werden. Die Bildaufnahme ist aber nicht primärer Zweck der Anlage und wird in aller Regel auch nicht durchgeführt. Kennzeichen der Fahrzeuge sind auf den Bildern nicht lesbar. Da die Kameras auch nicht die Zugangsbereiche der angesprochenen Gebäude im Blick haben, bin ich zu der Bewertung gekommen, dass beim Betrieb der Anlage keine personenbezogenen Daten erhoben werden und es damit auch keine datenschutzrechtlichen Bedenken der Anlage gibt.

Allerdings habe ich der Straßenverkehrsbehörde empfohlen, künftig die Bevölkerung über derartige Maßnahmen rechtzeitig zu informieren und die Funktionsweise ausreichend zu erläutern. Eine offensive Informationspolitik hilft, in solchen Fällen Misstrauen zu verhindern und die Akzeptanz zu stärken.

4.1.1.4 Videokameras in der Frankfurter Verkehrsleitzentrale

4.1.1.4.1 Verkehrsüberwachung

Durch die Frankfurter Verkehrsleitzentrale werden zahlreiche große Kreuzungen in Frankfurt mittels Videotechnik überwacht. Diese Überwachung dient in erster Linie der Beobachtung des Verkehrsflusses. Bei der derzeit eingesetzten Videotechnik in der Verkehrsleitzentrale handelt es sich um eine inzwischen veraltete Technik, die ein Beschränken der Zoom- und Schwenkmöglichkeiten nicht zulässt. Damit ist je nach eingesetzter Kamera nicht auszuschließen, dass die Bediensteten in der Leitzentrale auch Bilder übertragen bekommen, auf denen Personen an Fenstern oder auf Balkonen wahrgenommen werden können. Damit ist die Kenntnisnahme personenbezogener Daten durchaus möglich.

Es ist geplant, dass die Verkehrsleitzentrale in Kürze ein anderes Domizil bezieht und dann auch die Technik so modernisiert wird, dass diese Privatzonen ausgeblendet werden können. Bis dahin habe ich die Erstellung einer Dienstanweisung gefordert, die die Bediensteten anweist, dass die Kameras nur im Rahmen der zur Verkehrslenkung notwendigen Anforderungen genutzt werden. Aus der Dienstanweisung hat sich insbesondere zu ergeben, dass das Beobachten von Fenstern und Balkonen unzulässig ist.

4.1.1.4.2 Übertragung der Bilder ins Internet

Ein Teil der Aufnahmen wird live im Internetangebot der Stadt bzw. über die Verkehrsleitzentrale Hessen öffentlich zugänglich gemacht. Nachts ist diese Funktion abgeschaltet. Eingestellt werden die Aufnahmen jeweils so, wie sie die Kameras liefern. Dabei werden einzelne Bilder mit ca. 45 sec Verzögerung zur Verfügung gestellt. Wenn in der Leitzentrale Bilder gezoomt werden und dadurch Personen etc. erkennbar sind, wird dies genauso ins Internet übertragen, es sei denn, die Übertragung wird manuell unterbrochen. Ich habe gegenüber der Stadt Frankfurt deutlich gemacht, dass Bilder, auf denen Personen erkennbar sind, nicht ins Internet gestellt werden dürfen. Ich habe deshalb gefordert, dass die regelmäßige manuelle Unterbrechung bei gezoomten Bildern in einer Dienstanweisung angeordnet werden muss. Für die neu zu errichtende Leitzentrale ist für diese Fälle eine technische Lösung anzustreben.

Von einigen Kameras präsentiert auch der Hessische Rundfunk Aufnahmen im Rahmen seiner Verkehrsmeldungsseiten. Diese werden technisch durch eine Kreuzweiche von der Leitung direkt abgegriffen. Daher ist auch hier die Übertragung gezoomter Bilder nicht ausgeschlossen.

Auch für die Übernahme der Bilder durch den Hessischen Rundfunk ist eine Lösung zu finden, die sicherstellt, dass keine gezoomten Bilder ins Internet übertragen werden können. Ich habe den Abschluss einer entsprechenden Vereinbarung mit dem Hessischen Rundfunk gefordert.

4.1.1.4.3 Zugriff der Polizei auf die Kamerasteuerung

Nachts wird die Steuerung der Kameras von der Polizei übernommen, da die Verkehrszentrale der Stadt zu dieser Zeit nicht besetzt ist. Tagsüber kann die Steuerung von der Polizei auf ausdrückliche Anforderung übernommen werden. Dies geschieht durch telefonische Kontaktaufnahme der Polizei mit der Leitzentrale, die dann die Übernahme freigeben muss.

Eine ausdrückliche (schriftliche) Regelung zu dieser Nutzung gibt es (derzeit) nicht, befindet sich allerdings im Abstimmungsverfahren.

4.1.2 Datenschutzprobleme bei der Bereitstellung des Staatsanzeigers im Internet

Die ungeschützte Einstellung des Staatsanzeigers ins Internet eröffnet zwar einfache Recherchemöglichkeiten, birgt aber auch die Gefahr von Datenschutzverletzungen, soweit personenbezogene Daten betroffen sind. Vor diesem Hintergrund waren Änderungen der bisherigen Praxis und Vorkehrungen gegen die zu Tage getretenen Datenschutzrisiken zu treffen. Die Bereitstellung des Staatsanzeigers als TIFF-Dokument im Internet ohne freie Recherchemöglichkeit - wie sie der Hessische Landtag für die Jahrgänge bis 2002 betreibt - ist dagegen datenschutzrechtlich nicht zu beanstanden.

Im Internet wird der Staatsanzeiger derzeit in den Jahrgängen bis 2002 vom Hessischen Landtag über die Internetadresse www.hessischer-landtag.de (Landtagsinformationssystem, Dokumentenarchiv) und ab den Jahrgängen 2003 vom HMDIS als Herausgeber des Staatsanzeigers (Internetadresse www.staatsanzeiger-hessen.de) zur Verfügung gestellt.

4.1.2.1 Veröffentlichung des Staatsanzeigers im Internet ab 2003 - Kollision mit dem Insolvenzrecht

Durch eine Eingabe wurde ich auf ein Problem der Bereitstellung des Staatsanzeigers im Internet aufmerksam. Der Betroffene hatte festgestellt, dass bei einer Internetrecherche zu seinem Namen seine bereits länger zurückliegende Funktion als Geschäftsführer einer Firma, die in Insolvenz gegangen war, angezeigt wurde. Datenquelle war die Veröffentlichung der Insolvenz im Staatsanzeiger. Der Betroffene befürchtete, dass dies auch nach der inzwischen vergangenen erheblichen Zeitspanne noch künftige potenzielle Arbeitgeber abschrecken könnte, ihn einzustellen.

Meine Recherche ergab, dass der Staatsanzeiger ab 2003 den Abonnenten, die ein Kombi-Abonnement haben, nicht nur in Papierform, sondern über eine Anmeldeprozedur auch elektronisch in vollständig recherchierbarer Form zur Verfügung gestellt wird. Parallel dazu wird eine Leseversion ohne den öffentlichen Anzeiger auch für Nicht-Abonnenten im Internet zur Verfügung gestellt. Nach Ablauf von sechs Monaten stellt der Verlag den kompletten Inhalt des Staatsanzeigers in einer Download-Version ins Internet ein. Das HMDIS als Herausgeber des Staatsanzeigers hatte offenbar die Datenschutzrisiken dieser Vorgehensweise nicht erkannt.

Wie ich bereits in meinem 36. Tätigkeitsbericht (Ziff. 5.1.2) dargestellt hatte, führt die ungeschützte Bereitstellung im Internet dazu, dass die Inhalte von Suchmaschinen ausgewertet werden können und eine Suche, z.B. über den Namen, noch Jahre später Ergebnisse aus der Veröffentlichung im Staatsanzeiger bringt. So war es auch hier. Eine auf die Information zu Namen spezialisierte Suchmaschine hatte im Internet zu dem Namen des Betroffenen auch die aus dem Jahr 2003 stammende Veröffentlichung der Insolvenz im Staatsanzeiger gefunden und zeigte diese als Ergebnis an.

Für die Bekanntmachung von Insolvenzen im Internet gibt es eine abschließende Regelung in § 9 Abs. 1 Insolvenzordnung i.V.m. § 2 der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet. Das für diese Bekanntmachungen im Internet (www.insolvenzbekanntmachungen.de) entwickelte Verfahren ist mit den Datenschutzbeauftragten abgestimmt. Es sieht Einschränkungen in der Suchfunktion vor. Die im Insolvenzrecht vorgeschriebenen Löschfristen sind umgesetzt. Gegen Auswertungen durch Suchmaschinen sind die Daten abgeschottet.

§ 9 Abs. 1 und 2 Insolvenzverordnung

(1) Die öffentliche Bekanntmachung erfolgt durch eine zentrale länderübergreifende Veröffentlichung im Internet; diese kann auszugsweise geschehen. Dabei ist der Schuldner genau zu bezeichnen, insbesondere sind seine Anschrift und sein Geschäftszweig anzugeben. Die Bekanntmachung gilt als bewirkt, sobald nach dem Tag der Veröffentlichung zwei weitere Tage verstrichen sind.

(2) Das Insolvenzgericht kann weitere Veröffentlichungen veranlassen, soweit dies landesrechtlich bestimmt ist. Das Bundesministerium der Justiz wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Einzelheiten der zentralen und länderübergreifenden Veröffentlichung im Internet zu regeln. Dabei sind insbesondere Löschungsfristen vorzusehen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen

1. unversehrt, vollständig und aktuell bleiben
2. jederzeit ihrem Ursprung nach zugeordnet werden können.

§ 2 Abs. 1 der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet

(1) Die Landesjustizverwaltung darf ein elektronisches Informations- und Kommunikationssystem zu Veröffentlichungen nach der Insolvenzordnung nur bestimmen, wenn durch geeignete technische und organisatorische Maßnahmen sichergestellt ist, dass die Daten

1. bei der elektronischen Übermittlung von dem Insolvenzgericht oder dem Insolvenzverwalter an die für die Veröffentlichung zuständige Stelle elektronisch signiert werden,
2. während der Veröffentlichung unversehrt, vollständig und aktuell bleiben,
3. spätestens nach dem Ablauf von zwei Wochen nach dem ersten Tag der Veröffentlichung nur noch abgerufen werden können, wenn die Abfrage den Sitz des Insolvenzgerichts und mindestens eine der folgenden Angaben enthält:
   a) den Familiennamen,
   b) die Firma,

c) den Sitz oder Wohnsitz des Schuldners oder
d) das Aktenzeichen des Insolvenzgerichts.

Die Angaben nach Satz 1 Nr. 3 Buchstabe a bis d können unvollständig sein, sofern sie Unterscheidungskraft besitzen. Nach dem Stand der Technik ist dafür Sorge zu tragen, dass die genannten Daten durch Dritte elektronisch nicht kopiert werden können.

Seit der Gesetzesnovelle 2001 können nach § 9 Abs. 2 Insolvenzordnung weitere Veröffentlichungen von Insolvenzen auf dem herkömmlichen Weg der Bekanntmachungen nur dann erfolgen, wenn das landesrechtlich vorgesehen ist. In Hessen war für eine Übergangszeit bis zum 29. Februar 2004 noch die Veröffentlichung im "Öffentlichen Anzeiger zum Staatsanzeiger für das Land Hessen" zugelassen (vgl. Runderlass des HMDJ Öffentliche Bekanntmachungen in Insolvenzverfahren im Internet vom 18. Dezember 2003, JMBl. 2004, S. 3 in Verbindung mit Runderlass des HMDJ Bekanntmachungen der Gerichte vom 21. Februar 1995, StAnz. S. 811). Zum Zeitpunkt der Veröffentlichung der Insolvenz der GmbH, deren Geschäftsführer der betroffene Bürger seinerzeit war, im Jahre 2003 im Öffentlichen Anzeiger des Staatsanzeigers, war diese Veröffentlichung noch zulässig. Allerdings kann ich - entgegen der mir mit Schreiben vom 15. September 2008 mitgeteilten Auffassung des HMDJ - die Zulässigkeit nur für das Printmedium feststellen. Durch die Einstellung als frei zugängliche Version ins Internet entsteht eine neue Qualität, die zusätzliche und zeitlich unbegrenzt fortwirkende Eingriffe in das Recht auf informationelle Selbstbestimmung bewirkt. Insbesondere durch die Such- und Auswertungsmöglichkeiten sind auf einfachem Weg Datenverarbeitungen möglich, die mit dem ursprünglichen Zweck der Veröffentlichung nicht mehr vereinbar sind. Werden die Inhalte als Texte ins Internet übernommen, kann z.B. entweder direkt oder durch Suchmaschinen nach Namen und Begriffen gesucht und es können auf diese Weise Informationen zusammengeführt werden bis hin zum Persönlichkeitsbild. Deshalb ist die Zulässigkeit der Bekanntmachung im Staatsanzeiger von der Zulässigkeit der Einstellung seiner frei auswertbaren Version ins Internet zu unterscheiden.

Zwar fallen nach § 3 Abs. 4 HDSG personenbezogene Daten, solange diese in allgemein zugänglichen Quellen gespeichert sind, nicht unter den Anwendungsbereich des HDSG.

§ 3 Abs. 4 HDSG

Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind sowie für Daten des Betroffenen, die von ihm zur Veröffentlichung bestimmt sind.

Printmedien zählen zu allgemein zugänglichen Quellen. Allerdings gilt das nicht zeitlich unbeschränkt (vgl. *Ronellenfitsch* Kommentar zum HDSG, § 3 Rdnr. 91, *Nungesser* Kommentar zum HDSG § 3 Rdnr. 47 mit Verweis auf die Lebach-Entscheidung BVerfGE 35, 203, 233). Die aus einer Grundrechtsabwägung zur Informationsfreiheit (Art. 5 Abs. 1 GG) resultierende Ausnahmeregelung des § 3 Abs. 4 findet gemäß Art. 5 Abs. 2 GG ihre Grenze in den Vorschriften der allgemeinen Gesetze.

Art. 5 Abs. 1 und 2 GG

(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

(2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.

Mit einer Veröffentlichung der kompletten Staatsanzeigerdaten im Internet werden die Einschränkungen umgangen, die durch die Regelungen der Insolvenzbekanntmachungen im Internet gesetzt wurden. Insbesondere werden die zum Schuldnerschutz vorgesehenen Löschfristen und Zugriffsbeschränkungen aufgehoben. Das Ziel, dem Schuldner nach Abwicklung und Abschluss des Insolvenzverfahrens einen unbelasteten Neustart zu ermöglichen, wird durch die einfachen und zeitlich unbegrenzten Auswertungsmöglichkeiten im Internet - wie der vorliegende Fall zeigt - konterkariert. Die frei zugängliche Bereitstellung solcher Daten im Internet ist deshalb unzulässig.

Dem HMDIS habe ich meine Rechtsauffassung mitgeteilt und um Stellungnahme gebeten. Mit einer Zwischennachricht teilte es mir umgehend mit, dass dort bereits zwei Eingaben zu gleichen Problemlagen vorlägen und in einem ersten Schritt die konkreten Bekanntmachungen aus dem Internetangebot des Staatsanzeigers herausgenommen würden. Dies geschah auch zeitnah für den betroffenen Bürger, nachdem dieser die Fundstelle im Staatanzeiger beigesteuert hatte. Mit dieser Lösung war zwar die unmittelbare Recherche im Internetangebot des Staatsanzeigers abgestellt. Da allerdings keine Möglichkeit besteht, die Trefferanzeige in den Suchmaschinen zu beeinflussen, ist der Index trotz der Löschung der Datenquelle noch über einen gewissen Zeitraum auffindbar. Das HMDIS informierte den Betroffenen über den Vollzug der Löschung und deren Auswirkungen.

Unabhängig von diesen Einzelfällen prüfte das HMDIS Lösungen zur Vermeidung solcher Datenschutzverletzungen für die Zukunft. Zunächst wurden die Suchmöglichkeiten auf den öffentlichen Anzeiger eingeschränkt. Bei der Recherche über Suchmaschinen sind jetzt nur noch Fundstellen auffindbar; diese sind mit der betreffenden Bekanntmachung nicht mehr verlinkt. Zudem wurde die Suchfunktion für Nicht-Abonnenten auf den Amtlichen Teil des Staatsanzeigers begrenzt.

Künftig sollen die Bekanntmachungen der Amtsgerichte im Staatsanzeiger abgetrennt und generell nicht mehr in der nach sechs Monaten für Nicht-Abonnenten zum Download eingestellten Version zur Verfügung gestellt werden. Die bereits im

Internet vorhandenen Ausgaben sollten "in einem angemessenen Zeitrahmen" um die Bekanntmachungen der Amtsgerichte bereinigt werden.

Für den registrierten eingeschränkten Nutzerkreis der derzeit rd. 380 Online-Abonnenten geht das HMDIS davon aus, dass ein Datenmissbrauch nachvollziehbar wäre. Für diesen Kreis soll deshalb der unbegrenzte Zugriff auf den Staatsanzeiger weiterhin erhalten bleiben. Auch hier ist jedoch zugesichert, dass bei Einwendungen gegen abgeschlossene Insolvenzveröffentlichungen die entsprechenden Einträge unverzüglich gelöscht werden.

Da Insolvenzveröffentlichungen nur noch für Altverfahren im Staatsanzeiger erfolgen dürfen und dies inzwischen die Ausnahme ist, habe ich mich mit dieser Lösung einverstanden erklärt.

4.1.2.2 Veröffentlichung des Staatsanzeigers der Jahrgänge bis 2002 im Internetangebot des Hessischen Landtags

Ein Betroffener hatte die Kanzlei des Hessischen Landtags aufgefordert, diejenige Seite des Staatsanzeigers aus dem Internet-Angebot zu entfernen, in der sein Name aufgeführt war. Es handelte sich um die Bekanntmachung einer Landesliste für eine weiter zurückliegende Landtagswahl. In der Frage, ob dies im Hinblick auf den Datenschutz erfolgen muss, habe ich die Kanzlei des Landtags beraten.

Die Bekanntmachung der Landeslisten im Staatsanzeiger ist nach §§ 36, 33 Abs. 1 i.V.m. § 73 LWO vorgeschrieben und inhaltlich festgelegt. Die Veröffentlichung ist damit zulässig. Dies umfasst auch die damit einhergehende langfristige Recherchierbarkeit der Landeslisten in Bibliotheken und Archiven. Die Bereitstellung des Staatsanzeigers als elektronisches Medium im Dokumentenarchiv des Hessischen Landtags im Internet wäre nur dann datenschutzrechtlich relevant, wenn sich dadurch die Qualität der Veröffentlichung im Hinblick auf den Eingriff in das informationelle Selbstbestimmungsrecht verändert. Das ist dann der Fall, wenn unmittelbar - oder weil die Informationen durch Suchmaschinen erschlossen werden - Such- und Auswertungsmöglichkeiten mit Personenbezug entstehen.

Das Internetangebot des Hessischen Landtags stellt den Staatsanzeiger nur als TIFF-Dokument zur Verfügung und bietet keine Suchfunktion auf Inhalte über Suchworte an. Mir sind keine Suchmaschinen bekannt, die heute schon TIFF-Dokumente auswerten. Nach derzeitigem Stand der Technik sind die Umwandlungsmethoden (OCR-Erkennung) noch zu fehlerbehaftet, sodass Suchmaschinen in solchen Formaten angebotene Inhalte nicht in Texte umsetzen und verarbeiten. Die Suche von Inhalten ist deshalb hier wie bei der Print-Version nur über Inhaltsverzeichnisse, 5-Jahres-Register oder bekannte Fundstellen möglich.

Da die Information selbst sowie die Auswertemöglichkeiten genau dem Papierexemplar entsprechen und lediglich zur Einsichtnahme der Gang in die Bibliothek entfällt, sehe ich das Vorhalten der Information in dieser Form als datenschutzrechtlich unproblematisch an.

4.2 Justiz und Strafvollzug

4.2.1 Netzkonzept in der Praxis bei kleinen Gerichten

Vor einigen Jahren hat das Hessische Ministerium der Justiz in einem Konzept Anforderungen an den Betrieb der IT in Gerichten formuliert. Ich habe nunmehr die Umsetzung in einem kleineren Gericht geprüft. Dabei hat sich die Annahme bestätigt, dass gerade kleinere Gerichte Probleme haben, die Vorgaben umzusetzen.

4.2.1.1 Ausgangslage

Vor einigen Jahren hat das HMDJ in der "Netzbeschreibung" die Struktur und wesentliche Rahmenbedingungen des Netzbetriebs für die Justiz festgelegt. Dies betraf insbesondere die Gegebenheiten in den Gerichten. In meinem 31. Tätigkeitsbericht (Ziff. 5.1) habe ich die Struktur und einige Details beschrieben. Mittlerweile wurde das Konzept fortgeschrieben und liegt in einer Fassung vor, die den aktuellen Stand der eingesetzten Technik berücksichtigt. Die organisatorischen Teile wurden dabei nur unwesentlich geändert. Da kleinere Gerichte nur beschränkte personelle Möglichkeiten haben, sind für sie die Anforderungen des Konzepts schwerer umzusetzen als durch Landgerichte oder das Oberlandesgericht. Ich habe daher in diesem Jahr geprüft, inwieweit sich Probleme bei der Umsetzung des Konzepts und des Datenschutzes in einem kleinen Gericht ergeben.

4.2.1.2 Feststellungen hinsichtlich der Umsetzung des HDSG

Der Direktor des Gerichts war gleichzeitig behördlicher Datenschutzbeauftragter. Trotz des vorhandenen Engagements in der Sache sind in diesem Fall Interessenkonflikte unvermeidbar. Ich habe daher gefordert, eine Person mit der Aufgabe zu betrauen, für die keine Interessenkonflikte vorliegen.

Es fehlten diverse Verfahrensverzeichnisse. Dies betraf insbesondere Altverfahren. Gerade vor dem Hintergrund, dass es sich in den meisten Fällen um einheitliche, vom Ministerium vorgeschriebene, Verfahren handelt, sollte es Muster der Verfahrensverzeichnisse geben, die dann durch das Gericht an die eigenen Gegebenheiten angepasst werden können. Das Justizministerium hat zugesagt, dass für alle einheitlichen Verfahren Muster bereitgestellt werden.

Verbesserungsbedürftig war der Umgang mit den Abteilungsablagen. So befanden sich teilweise Dokumente darin, die mehrere Jahre alt waren. Die Zugriffsrechte waren bis auf eine Abteilung so vergeben, dass alle Mitarbeiter des Gerichts uneingeschränkten Zugriff auf die Verzeichnisse hatten. Ich habe gefordert, organisatorische Maßnahmen zu ergreifen, um

nicht mehr benötigte Dokumente zu löschen. Die Zugriffsmöglichkeiten auf Abteilungsablagen sollten in Anlehnung an die Fachverfahren umgesetzt werden, für die differenzierte Zugriffsrechte vorhanden waren.

4.2.1.3 Feststellungen zur Umsetzung des Netzkonzepts

In der "Netzbeschreibung" waren eine Reihe von Maßnahmen explizit dafür vorgesehen, dass Dokumente auch gegen unbefugte Zugriffe durch Systemadministratoren geschützt sind. Dadurch sollte zusammen mit anderen Maßnahmen der richterlichen Unabhängigkeit Genüge getan werden.

- Es war die Rolle eines Systemrevisors vorgesehen.
- Es gab die Möglichkeit, das Verschlüsselungsprogramm Chiasmus zu nutzen.
- Es konnte ein Safeordner im persönlichen Verzeichnis des Richters eingerichtet werden, in dem Dokumente verschlüsselt abgelegt werden. Ergänzend musste sichergestellt werden, dass kein Systemadministrator unter der Kennung des Recovery-Agents arbeiten kann.

Seitens der Richter in dem Amtsgericht wurde kein Bedarf gesehen, Dokumente zur Wahrung der richterlichen Unabhängigkeit besonders vor unbefugten Zugriffen zu schützen. Die Möglichkeiten wurden nicht genutzt. Ich habe gefordert, trotzdem die Rolle des Systemrevisors zu vergeben, da sie ganz allgemein zur Kontrolle der Sicherheitsprotokolle durch das Gericht benötigt wird. Außerdem sollten die organisatorischen Maßnahmen für den Einsatz eines Recovery-Agents getroffen werden, damit die Safeordner bei Bedarf problemlos genutzt werden können.

Einschränkungen, die USB-Schnittstellen zu nutzen, gab es nicht. Hier sind Restriktionen nötig, die durch technische und organisatorische Maßnahmen umgesetzt werden.

4.2.1.4 Ergebnis

Es hat sich bestätigt, dass gerade kleine Gerichte Probleme haben, alle verschiedenen Funktionen durch dafür qualifizierte Mitarbeiter auszufüllen, die keinen Interessenkonflikten ausgesetzt sind. Dies betrifft den behördlichen Datenschutzbeauftragten, den Systemrevisor und den Recovery-Agent.

Die weitgehenden Zugriffsrechte über die Abteilungsablagen wurden u.a. damit begründet, dass die Mitarbeiter sich gegenseitig vertreten können müssen. Auch wenn ich der Begründung teilweise folgen kann, sind doch Einschränkungen analog den Zugriffsrechten in den Fachverfahren nötig.

4.2.2 Überwachung des Besuchs in einer Justizvollzugsanstalt durch Videokamera

Wird der Besuch in einer Haftanstalt videoüberwacht, so ist die Übertragung und Beobachtung der Aufnahme in Echtzeit zulässig. Für die Anfertigung und Aufbewahrung von Aufzeichnungen fehlt es an einer Rechtsgrundlage. Die Justizvollzugsanstalt Schwalmstadt tat sich schwer, dies anzuerkennen.

Die Ehefrau eines Insassen der Justizvollzugsanstalt Schwalmstadt machte mich darauf aufmerksam, dass im Besuchsraum der Anstalt neuerdings Videokameras installiert sind. Sie fragte mich, wie lange die Bänder, auf denen ihr Besuch aufgenommen ist, aufbewahrt werden und ob sie es überhaupt hinnehmen muss, dass ihr Besuch ihres Ehemannes videoüberwacht wird.

Auf entsprechende Nachfrage beschrieb mir die Haftanstalt den Videoeinsatz. Nach besonderen Vorkommnissen in der Vergangenheit, wie das Einbringen und die Übergabe von unerlaubten Gegenständen, wie z.B. Betäubungsmittel, Tabletten, Bargeld und Handys, sei nach Rücksprache mit dem Justizministerium eine Kameraüberwachungsanlage im großen Besuchsraum der Anstalt installiert worden. Die Überwachung erfolge mit zwei Kameras, die sichtbar an der Decke befestigt sind. An der Eingangstür werde darauf hingewiesen, dass der Raum kameraüberwacht wird. Die Bilder würden im Büro der Besuchsoberaufsicht angezeigt. Bei Bedarf könnten die Bilder mit einem Festplattenrekorder aufgenommen werden. Aufnahmen würden von der Sicherheitsabteilung angeordnet. Die gespeicherten Daten würden nach Erreichen der Festplattenkapazität automatisch überschrieben. Die Aufnahmekapazität betrage ca. fünf Monate. Die Installation der Kameraanlage diene der Sicherheit und Ordnung in der Justizvollzugsanstalt. Verteidigerbesuche würden nicht überwacht.

Gegen die Aufnahme von Besuchen habe ich grundsätzliche datenschutzrechtliche Bedenken. Das gilt nicht nur für die Justizvollzugsanstalt Schwalmstadt, sondern für alle hessischen Justizvollzugsanstalten. Die Videoüberwachung von Gefangenen und Besuchern stellt, insbesondere wegen der Aufzeichnung des Verhaltens der Betroffenen, einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Es bedarf nach der Rechtsprechung des Bundesverfassungsgerichtes einer hinreichend bestimmten gesetzlichen Grundlage, aus der sich die Voraussetzungen, ein hinreichend konkretisierter Zweck und der Umfang der Beschränkung klar und für die Betroffenen erkennbar ergeben (so auch in der Begründung zum Änderungsantrag der Fraktion der CDU zu dem Gesetzentwurf der Landesregierung für ein Hessisches Jugendstrafvollzugsgesetz - LTDrucks. 16/7798 zutreffend ausgeführt). Ich habe daher das Justizministerium bezüglich der Rechtmäßigkeit der Maßnahme um eine Stellungnahme gebeten.

Aus meiner Sicht stellt sich die Rechtslage wie folgt dar:
Eine bloße Echtzeitüberwachung **ohne Aufzeichnung** kann der Überwachung durch einen anwesenden Aufsichtsbeamten gleichgestellt und damit auf § 27 Abs. 1 StVollzG gestützt werden. Eine Rechtsgrundlage für die **Fertigung von Aufzeichnungen** ist hingegen nicht ersichtlich. § 27 Abs. 1 StVollzG regelt die Überwachung der Besuche.

§ 27 StVollzG

(1) Die Besuche dürfen aus Gründen der Behandlung oder Sicherheit oder Ordnung der Anstalt überwacht werden, es sei denn, es liegen im Einzelfall Erkenntnisse dafür vor, dass es der Überwachung nicht bedarf. Die Unterhaltung darf nur überwacht werden, soweit dies im Einzelfall aus diesen Gründen erforderlich ist.

(2) Ein Besuch darf abgebrochen werden, wenn Besucher oder Gefangene gegen die Vorschriften dieses Gesetzes oder die aufgrund dieses Gesetzes getroffenen Anordnungen trotz Abmahnung verstoßen. Die Abmahnung unterbleibt, wenn es unerlässlich ist, den Besuch sofort abzubrechen.

(3) Besuche von Verteidigern werden nicht überwacht.

(4) Gegenstände dürfen beim Besuch nur mit Erlaubnis übergeben werden. …

Der typische Fall der Überwachung in diesem Sinne ist die Überwachung durch einen anwesenden Aufsichtsbeamten. Soweit die Bilder nur im Büro der Besucheraufsicht angezeigt und nicht auch aufgezeichnet werden, steht die Videoüberwachung als "verlängertes Auge" der Überwachung durch persönliche Präsens im Besuchsraum gleich. Auch wenn die Art und Weise der Überwachung der Anstalt überlassen ist, kann auf § 27 Abs. 1 StVollzG aber nicht die **Aufzeichnung** des Besuches gestützt werden. Diese stellt im Vergleich zur bloßen Überwachung einen zusätzlichen Eingriff von erhöhter Intensität dar. § 81 Abs. 2 StVollzG kann ebenfalls nicht als Rechtsgrundlage der Aufzeichnung herangezogen werden.

§ 81 Abs. 2 StVollzG

Die Pflichten und Beschränkungen, die dem Gefangenen zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt auferlegt werden, sind so zu wählen, da sie in einem angemessenen Verhältnis zu ihrem Zweck stehen und den Gefangenen nicht mehr und nicht länger als notwendig beeinträchtigen.

Unabhängig von der Frage, ob die Regelung überhaupt eine Rechtsgrundlage für Eingriffe darstellt oder lediglich die aufgrund anderer Vorschriften erfolgenden Eingriffe im Hinblick auf den Verhältnismäßigkeitsgrundsatz beschränkt, kann eine eingriffsintensive Maßnahme wie die Videoaufzeichnung eines Besuchs nicht auf eine derart allgemein gefasste Regelung gestützt werden, zumal mit § 27 StVollzG eine spezielle Regelung zur Besuchsüberwachung existiert. Auch auf das Hausrecht können Videoaufzeichnungen nicht gestützt werden, da auch hier das Strafvollzugsgesetz eine abschließende Regelung der zulässigen Eingriffe durch Bedienstete von Justizvollzugsanstalten in die Rechte Strafgefangener vorsieht.

Das hessische Justizministerium bestätigte die Installation der Kameraanlage. Es bestätigte aber nicht die Aufzeichnung der Besuche. Es führte im Gegenteil ausdrücklich aus, eine Aufzeichnung der Aufnahmen erfolge weder in der Justizvollzugsanstalt Schwalmstadt noch in den anderen hessischen Justizvollzugsanstalten.

Ich fragte also bei der Justizvollzugsanstalt Schwalmstadt noch einmal nach, ob sie denn ihre mir gegenüber beschriebene anderslautende Praktik, bei Bedarf und auf Anordnung der Sicherheitsabteilung die Aufnahmen auch aufzuzeichnen und bis zu fünf Monate aufzubewahren, geändert und evtl. vorhanden gewesene Aufzeichnungen gelöscht habe. Die Gefängnisleitung teilte mir mit, bis dato sei noch keine entsprechende Anordnung getroffen und daher auch keine Aufzeichnungen vorgenommen worden. Dennoch hielt sie sich offen, entgegen der Versicherung des Ministeriums, auf Anordnung ihrer Sicherheitsabteilung jederzeit Aufzeichnungen herzustellen und aufzubewahren.

Deshalb habe ich erneut das hessische Justizministerium eingeschaltet und es gebeten, sicherzustellen, dass die Justizvollzugsanstalt Schwalmstadt es auch künftig unterlässt, den Besuch von Gefangenen aufzuzeichnen. Dabei halte ich es für geboten, die technische Vorkehrung so zu gestalten, dass Aufnahmen nicht jederzeit, sozusagen "auf Knopfdruck" aufgezeichnet werden können.

Kurz vor der Schlussredaktion dieses Berichtes hat die Justizvollzugsanstalt Schwalmstadt mitgeteilt, der Festplattenrecorder sei abgebaut, weitere Aufzeichnungsmöglichkeiten seien nicht vorhanden und es sei in der Zwischenzeit auch nicht zu Aufzeichnungen gekommen.

4.3 Polizei und Ordnungsbehörden

4.3.1 Novellierung des HSOG

Es besteht weiterhin dringender Bedarf zur Überarbeitung des HSOG vor allem zur Umsetzung der Rechtsprechung des Bundesverfassungsgerichts.

Ich hatte wiederholt darüber berichtet, dass der Hessische Gesetzgeber nicht alle Anforderungen zur Überarbeitung des HSOG, die sich insbesondere aus der Rechtsprechung des BVerfG ergeben, umgesetzt hat.

Schon im Jahre 2006 hatte die FDP - im Anschluss an die Entscheidung des BVerfG zur Rasterfahndung einen Gesetzentwurf zur Änderung des HSOG vorgelegt - ich hatte darüber berichtet (35. Tätigkeitsbericht, Ziff. 4.2.2). Allerdings war der Entwurf von der damaligen Mehrheit des Parlaments schließlich abgelehnt worden.

In der 17. Legislaturperiode wurde dieser Antrag wortgleich wieder eingebracht (LTDrucks. 17/133). Neu aufgenommen wurde eine Befugnisnorm zum Einsatz von Kennzeichenlesegeräten.

4.3.1.1 Umsetzung des Kernbereichsschutzes

Schon im Gesetzgebungsverfahren aus dem Jahre 2004 hatte ich kritisiert, dass Regelungen zum Schutz des Kernbereichs privater Lebensführung für den Einsatz der akustischen Wohnraumüberwachung und der präventiven Telekommunikationsüberwachung nicht bzw. nicht ausreichend vorgesehen waren. Hier sah der FDP-Gesetzentwurf eine Nachbesserung vor.

§ 15 Abs. 4 Satz 2 sowie § 15a Abs. 4 (neu) S. 2 FDP-Entwurf

Wird erkennbar, dass durch die Maßnahmen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, sind diese sofort abzubrechen. Bereits erlangte Informationen unterliegen einem Verwertungsverbot.

Die vorgeschlagenen Ergänzungen im Gesetz sind zwingend notwendig. Die Forderung, ggf. die Maßnahme abzubrechen bzw. zu unterbrechen, wenn der Kernbereich privater Lebensgestaltung betroffen wird, konkretisiert die Verhaltensmaßregeln für die betroffenen Beamten. Auch im präventiven Bereich sind den Kernbereich schützende Regelungen erforderlich. Maßnahmen, die zum Schutz von Leib, Leben oder Gesundheit einer Person getroffen werden und damit zum Schutz hochrangiger Rechtsgüter, verdrängen nicht den Schutz aus Art. 2 i.V.m. Art. 1 Abs. 1 GG der von der Maßnahme Betroffenen, zumal nicht auszuschließen ist, dass von solchen Maßnahmen auch Personen (mit)betroffen werden, die selbst für die drohende Gefahr nicht verantwortlich sind.

Auch mit einer solchen Ergänzung bleiben freilich noch Fragen der praktischen Umsetzung offen. Insbesondere dann, wenn nur teilweise die Überwachung nicht durch direktes Mithören, sondern durch eine Aufzeichnung erfolgt. Aber auch beim direkten Mithören ist oft nur schwer zu entscheiden - gerade wenn mehrere Personen zu hören sind -, ob alle wahrgenommenen Gespräche zum geschützten Kernbereich gehören, oder ob quasi zur Tarnung bewusst solche Inhalte vermischt werden.

4.3.1.2 Kennzeichenerkennung

Das BVerfG hatte im Rahmen eines Verfassungsbeschwerdeverfahrens entschieden, dass § 14 Abs. 5 HSOG nichtig ist (BVerfG 1BvR 2074/05 vom 11. März 2008).

§ 14 Abs. 5 HSOG in der bis zum 11. März 2008 geltenden Fassung

Die Polizeibehörden können auf öffentlichen Straßen und Plätzen Daten von Kraftfahrzeugkennzeichen zum Zwecke des Abgleichs mit dem Fahndungsbestand automatisiert erheben. Daten, die im Fahndungsbestand nicht enthalten sind, sind unverzüglich zu löschen.

Das BVerfG hatte seine Entscheidung im Wesentlichen damit begründet, dass diese Norm nicht dem Gebot der Normbestimmtheit und Normenklarheit genüge, da sie weder den Anlass noch den Ermittlungszweck benenne. Darüber hinaus genüge die Vorschrift in ihrer Unbestimmtheit auch nicht dem Gebot der Verhältnismäßigkeit.

Gleichzeitig hatte das BVerfG darauf hingewiesen, dass die Regelung zur Kennzeichenerkennung im Brandenburgischen Polizeirecht in weiten Teilen die verfassungsrechtlichen Anforderungen für einen Eingriff in das informationelle Selbstbestimmungsrecht erfülle.

Die von der FDP-Fraktion vorgeschlagene Neuregelung lehnte sich deshalb eng an die brandenburgische Regelung an.

§ 14 Abs. 5 HSOG i.d.F. der LTDrucks. 17/133

Die Polizeibehörden können die Kennzeichen von Fahrzeugen ohne Wissen der Person durch den offenen Einsatz technischer Mittel automatisiert erheben, wenn

1. dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person erforderlich ist,
2. dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung nach § 18 Abs. 2 Nr. 1, 3 oder 5 vorliegen oder
3. eine Person oder ein Fahrzeug nach § 17 ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht.

Die erhobenen Daten können mit zur Abwehr der Gefahr nach Satz 1 gespeicherten polizeilichen Daten automatisch abgeglichen werden. Bei Datenübereinstimmung sind unverzüglich Maßnahmen zur Klärung des Sachverhalts zu ergreifen. Die Erstellung von Bewegungsprofilen ist außer in Fällen des Satzes 1 Nr. 3 unzulässig. Bei Datenübereinstimmung können die Daten polizeilich verarbeitet und im Falle des Satzes 1 Nr. 3 zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. Anderenfalls sind sie unverzüglich zu löschen. Der flächendeckende stationäre Einsatz der technischen Mittel ist unzulässig.

Mit dieser vorgeschlagenen Neureglung wird der Anwendungsbereich dieser Maßnahme sehr eng gesteckt. Ob ein Einsatz solcher Geräte dann wirklich nützlich für einzelne polizeiliche Einsätze ist, kann nur durch die Polizei im Rahmen ihrer taktischen Einsatzplanung beurteilt werden. Allerdings hat im Rahmen der Verhältnismäßigkeitsprüfung schon im Gesetzgebungsverfahren eine Abwägung stattzufinden, die auch berücksichtigen muss, dass beim Einsatz dieser Geräte eine Vielzahl von gesetzestreuen Bürgerinnen und Bürgern tangiert wird, da auch ihre Kennzeichen gelesen und mit den Abgleichdateien verglichen werden, selbst wenn im Nicht-Treffer-Fall eine sofortige Löschung der Daten erfolgt.

Im Rahmen der Anhörung im Innenausschuss des Hessischen Landtages habe ich zudem erhebliche Bedenken zu § 14 Abs. 5 S. 4 des Entwurfes geltend gemacht. Ich bezweifele, dass diese Regelung mit den vom BVerfG formulierten Anforderungen an einen verfassungskonformen Einsatz der Kennzeichenerkennung im präventiven Bereich durch die Polizei übereinstimmt.

Zwar ist grundsätzlich das ausdrückliche Verbot der Erstellung von Bewegungsprofilen zu begrüßen. Allerdings formuliert die Vorschrift eine problematische Ausnahme im Zusammenhang mit Ausschreibungen zur polizeilichen Beobachtung. So wie die Ausnahme formuliert ist, könnte gezielt das Erstellen eines Bewegungsprofils im Rahmen einer polizeilichen Beobachtung Begründung für den Einsatz einer Kennzeichenerkennung sein. Bei einer derartigen Auslegung ergibt sich jedoch ein Widerspruch zwischen der verdeckten Maßnahme - polizeiliche Beobachtung - und dem offenen Einsatz technischer Mittel, als welches § 14 Abs. 5 S. 1 am Anfang des Entwurfes den Einsatz von Kennzeichenerkennung definiert. Das Erstellen eines Bewegungsprofils, das die zu beobachtende Person nicht bemerkt - i.S.d. § 17 HSOG ja auch nicht bemerken soll - entspricht in ihrer Auswirkung aber vollständig einer verdeckten Datenerhebung.

Aufgrund der Auflösung des Landtages am 19. November 2008 wurde über den Entwurf nicht mehr entschieden. In der nächsten Legislaturperiode sollte zeitnah mit der Überarbeitung des HSOG begonnen werden, um endlich die Vorgaben des BVerfG umzusetzen.

4.3.2 Datenspeicherungen über Teilnehmer an Demonstrationen gegen die Einführung von Studiengebühren

Die Polizei in Frankfurt speicherte über 224 Teilnehmer an einer Demonstration gegen die Einführung von Studiengebühren personenbezogene Daten wegen des Verdachtes, sie hätten Straftaten begangen. Sie bezeichnete sie als "gewalttätig" und als "politisch links motivierte Straftäter" auch wenn sie ihnen keine konkreten Tatbeteiligungen vorwerfen konnte. Nach meiner Intervention löschte sie zu den meisten Betroffenen ihre Datenspeicherungen und vernichtete ihre Akten.

Am 6. Juli 2006 demonstrierten in Frankfurt mehrere tausend Personen gegen die Einführung von Studiengebühren. Nach der zunächst friedlichen Protestaktion und einer Abschlusskundgebung im Stadtzentrum löste sich eine Gruppe von mehreren hundert Demonstranten und zog in Richtung Autobahn. Die Autobahn und mehrere Verkehrsknotenpunkte wurden blockiert. Lautsprecheraufforderungen, die Autobahn zu verlassen, halfen nichts. Nur unter Anwendung von Gewalt konnte die Polizei die Blockaden auflösen. Dabei kam es zu Widerstandshandlungen. Es flogen Steine und Flaschen durch die Luft und auf die Autobahn und es bildeten sich kilometerlange Staus. Über 200 Personen wurden festgenommen.

Etwa ein Jahr später stellte ein damals festgenommener Demonstrant beim Polizeipräsidium Frankfurt einen Antrag auf Löschung seiner Daten und bat mich, ihn bei seinem Anliegen zu unterstützen. Das Polizeipräsidium Frankfurt lehnte den Antrag ab. Das im Anschluss an die Demonstration durchgeführte Strafverfahren sei zwar gem. § 170 Abs. 2 StPO von der Staatsanwaltschaft eingestellt worden, allerdings sei in dem Einstellungsbescheid ausdrücklich davon die Rede, dass der Tatverdacht fortbestehe - so die Polizei in ihrem ablehnenden Bescheid. Darin bezog sie sich auf die Regelung in § 20 Abs. 4 HSOG.

§ 170 StPO

(1) Bieten die Ermittlungen genügend Anlass zur Erhebung der öffentlichen Klage, so erhebt die Staatsanwaltschaft sie durch Einreichung einer Anklageschrift bei dem zuständigen Gericht.

(2) Andernfalls stellt die Staatsanwaltschaft das Verfahren ein.

§ 20 Abs. 4 HSOG

Die Polizeibehörden können, soweit Bestimmungen der Strafprozessordnung oder andere gesetzliche Regelungen nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten speichern oder sonst verarbeiten. Die Speicherung oder sonstige Verarbeitung in automatisierten Verfahren ist nur zulässig, wenn es sich um Daten von Personen handelt, die verdächtig sind, eine Straftat begangen zu haben; entfällt der Verdacht, sind die Daten zu löschen.

In der Einstellungsverfügung der Staatsanwaltschaft, die mir der Betroffene vorlegte, war u.a. ausgeführt: "Dem Beschuldigten wird zur Last gelegt, an der Blockade der BAB 66 teilgenommen und sich dadurch einer Nötigung und eines Landfriedensbruchs schuldig gemacht zu haben. Er wurde im Bereich des genannten Autobahnabschnittes angetroffen und vorläufig festgenommen. Dies reicht jedoch zu einer konkreten Schuldfeststellung nicht aus." Es wird beschrieben, dass nicht festgehalten war, wer aktiv die Blockade tatsächlich vorgenommen hatte und wer, nachdem die Blockade bereits bestand, später hinzugetreten ist. Auch sind Personen - allein aus Gründen der Verkehrssicherheit - vorläufig festgenommen worden, die nur auf dem Standstreifen der Autobahn bzw. auf der Böschung am Fahrbahnrand standen. "Da eine zweifelsfreie Unterscheidung von Teilnehmern an der Blockade und ‚Nachzüglern' weder an Hand von Videomaterial noch an Hand von Festnahmeberichten vorgenommen werden kann, war das Ermittlungsverfahren trotz Fortbestehen eines Tatverdachts gegen den Beschuldigten einzustellen."

Ich stellte beim HLKA fest, dass auf Veranlassung des Polizeipräsidiums Frankfurt Daten zu dem Betroffenen unter Angabe des Deliktes "Landfriedensbruch" im polizeilichen Auskunftssystem POLAS gespeichert waren. Als Aufbewahrungsdauer waren zehn Jahre verfügt. Es war festgehalten, dass er am 6. Juli 2006 erkennungsdienstlich behandelt worden war. Der Datensatz enthielt außerdem die personenbezogenen Hinweise "gewalttätig" und "LIMO" (politisch links motivierter Straftäter).

Die Speicherung seiner Daten vollständig als unzulässig einzustufen und ihre Löschung zu verlangen, war nicht zu vertreten. Eine Löschpflicht nach § 20 Abs. 4 letzter Halbsatz HSOG bestand unzweifelhaft nicht. Zweifelhaft war allerdings, ob die gesamte Datenspeicherung sowie das festgesetzte Aussonderungsprüfdatum verhältnismäßig waren.

Um dies näher beurteilen zu können, sah ich die vom Polizeipräsidium Frankfurt zu dem Vorgang geführte Kriminalakte ein. Der Akte war eine konkrete, seiner Person zuzuordnende Tatbeteiligung nicht zu entnehmen. Der Vorwurf, dass er einer derjenigen war, die Flaschen oder Steine geworfen hatten, fand sich in der Akte nicht. Es war festgehalten, dass er sich seiner Festnahme um 15.50 Uhr nicht widersetzte. Nach der Aktenlage stand fest: Er war dabei, als Personen auf der Autobahn festgenommen wurden, nachdem Aufforderungen, sie zu verlassen, fruchtlos verlaufen waren. Er gehörte zu denjenigen Personen, die erst zu einer Gefangenensammelstelle und später ins Polizeipräsidium verbracht wurden. Dort wurden seine Personalien festgehalten, er wurde erkennungsdienstlich behandelt und kurz nach Mitternacht entlassen.

Bei der Beurteilung der Verhältnismäßigkeit ist zu berücksichtigen, dass von den erkennungsdienstlichen Unterlagen immer ein Duplikat dem BKA zur Verfügung gestellt wird und das BKA die Existenz der erkennungsdienstlichen Unterlagen in ihren Informationssystemen nachweist. Mit der Aufbewahrung dieser Unterlagen ist immer auch eine bundesweite Datenspeicherung verbunden. Aber auch die Zuordnung der personenbezogenen Hinweise "gewalttätig" und "LIMO" erschienen mir nicht angemessen, zumal die Datenspeicherung für die die Dauer von zehn Jahren im Zugriff aller Polizeidienststellen stehen sollte. Ich bat das Polizeipräsidium Frankfurt, seine ablehnende Haltung zu dem Löschungsantrag des Betroffenen noch einmal zu überprüfen. Eine förmliche Bescheidung stand ohnehin an, denn der Betroffene hatte in der Zwischenzeit gegen den ablehnenden Bescheid Widerspruch erhoben.

Die Feststellung in dem Einzelfall legte es nahe, der Frage nachzugehen, ob die personenbezogenen Hinweise "gewalttätig" und "LIMO" allen Personen zugeordnet worden waren, die im Zusammenhang mit der Demonstration festgenommenen worden waren. Auf mein Ersuchen wertete das PTLV die Datei POLAS aus und listete alle Personen auf, bei denen die beiden personenbezogenen Hinweise, als Tatzeit "6. Juli 2006" und als Tatort "Frankfurt" im Datensatz gespeichert waren. Die Liste umfasste 224 Personen.

Beim Polizeipräsidium Frankfurt nahm ich eine Stichprobe und sah mir die Kriminalakten von fünf Personen an. Der Akteninhalt war fast identisch. Bei keiner der fünf Personen war festzustellen, dass sie sich an der Autobahnblockade aktiv beteiligt und Gewalttaten oder Widerstandshandlungen begangen hatten. Nach den mir vorgelegten Einsatzberichten und internen Vermerken war dies nur bei wenigen einzelnen Personen der Fall. Dennoch waren bei allen 224 Personen die personenbezogenen Hinweise festgehalten. Die vorgesehene Aufbewahrungsdauer betrug bei Jugendlichen fünf, bei erwachsenen Beteiligten zehn Jahre. Nahezu alle waren erkennungsdienstlich behandelt worden. Ich forderte die Polizei in Frankfurt auf, auch in diesen Fällen die Verhältnismäßigkeit ihrer Datenspeicherungen zu überprüfen.

Diese Prüfung führte zu dem Ergebnis, dass bei 198 Personen beide personenbezogenen Hinweise gelöscht wurden. Bei 18 Personen kam man zu dem Ergebnis, beide Hinweise bestehen zu lassen, bei fünf Personen blieb der Hinweis "LIMO", bei drei Personen "gewalttätig" bestehen. Außerdem korrigierte die Polizei die Einstufung der Schwere der Fälle. Sie war zuvor von Standardfällen ausgegangen, die bei Jugendlichen zu der Speicherdauer von fünf und bei Erwachsenen von zehn Jahren führen. Nun stufte sie die Vorgänge als "Fälle geringer Bedeutung" ein. Dies führte zu Speicherfristen von zwei Jahren bei den Jugendlichen und drei Jahren bei den Erwachsenen. Bezüglich der Aufbewahrung der erkennungsdienstlichen Unterlagen erbat sich die Polizei noch etwas Bedenkzeit. Damit war die Streitmasse erheblich geschmolzen. Bezüglich der Einzelfallentscheidungen, in denen den Betroffenen konkrete Tatbeteiligungen zuzuordnen waren, habe ich gegen die Datenspeicherungen keine Einwände erhoben. Bezüglich der Jugendlichen war die Speicherdauer fast verstrichen, die Erwachsenen mussten evtl. noch ein Jahr warten. Doch die letzte Entscheidung war noch nicht getroffen.

In dem oben beschriebenen Einzelfall hob die Polizei ihren Bescheid auf, mit dem sie zuvor die Löschung der Daten des Betroffenen abgelehnt hatte. Sie löschte die Datenspeicherungen und vernichtete die dazugehörigen Unterlagen.

Zwar rechtfertigte sie die Rechtmäßigkeit der ursprünglichen Datenspeicherung, kam aber unter Betrachtung der mittlerweile verstrichenen knapp zwei Jahre seit dem Geschehen zu dem Ergebnis, dass die Datenspeicherung nun nicht mehr erforderlich sei. Zu der Frage der weiteren Erforderlichkeit bzw. Verhältnismäßigkeit führte das Polizeipräsidium Frankfurt in dem Widerspruchsbescheid sinngemäß aus:

Aus Anlass der Einzelfallbearbeitung sei zum jetzigen Zeitpunkt festzustellen, dass die Kenntnis der Daten für das Polizeipräsidium als speichernde Stelle zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben nicht mehr erforderlich sei.

Zur Beurteilung der Erforderlichkeit seien nach der Rechtsprechung des HessVGH mehrere Gesichtspunkte in den Blick zu nehmen und nach dem Grundsatz der Verhältnismäßigkeit abzuwägen. Der HessVGH führe in seinem Urteil vom 16. Dezember 2004 (Az. 11 UE 2982/02) aus: "Auf der einen Seite ist das prinzipielle Bedürfnis der Polizeipraxis zu berücksichtigen, in den polizeilichen Verbunddateien und Kriminalakten innerhalb der zeitlichen Grenzen der Aussonderungsprüffristen einen möglichst umfassenden Überblick über die kriminelle Aktivität und ‚Karriere' einer Person zu behalten. Nur durch die Auflistung und Aufbewahrung eines solchen ‚Werdeganges' kann den Intentionen der vorbeugenden Verbrechensbekämpfung wirksam entsprochen und auch die in den Polizeigesetzen verschiedentlich verlangte Prognose über einen Betroffenen gestellt werden. Auf der anderen Seite sind die Art und die Bedeutung der Daten in Rechnung zu stellen, deren Löschung in Streit steht. Je unbedeutender sich die Daten nach der Schwere der zugrunde liegenden Straftat und je uninteressanter sie sich unter kriminalistischen Aspekten darstellen, desto stärker schlagen die während der gesamten Aufbewahrungszeit andauernden und im Moment der Überprüfung aktuell werdenden Datenschutzbelange des Betroffenen zu Buche."

Danach müsse zugunsten des Betroffenen Berücksichtigung finden, dass das gegen ihn geführte Ermittlungsverfahren gemäß § 170 Abs. 2 StPO eingestellt worden sei. Unbeschadet des damit nicht ausgeschlossenen Restverdachtes, der die Speicherung nach § 20 Abs. 4 Satz 2 HSOG grundsätzlich rechtfertige, relativiere dies doch seine Bedeutung. Zudem falle ins Gewicht, dass der Betreffende erstmalig bei den Ereignissen am 6. Juli 2006 wegen des Verdachts auf Landfriedensbruch (§ 125 StGB), Nötigung (§ 240 StGB) und gefährlichem Eingriff in den Straßenverkehr (§ 315b StGB) strafrechtlich aufgefallen sei. Schließlich könne zu seinen Gunsten angeführt werden, dass es sich bei den in Rede stehenden Straftaten um Vergehen mit einer Strafandrohung im Höchstmaß von fünf Jahren handele und er seit dem der Speicherung zugrunde liegenden Ereignis nicht mehr strafrechtlich in Erscheinung getreten sei.

Diese Beurteilung trifft zu. Ich ersuchte die Polizei in Frankfurt, diese Beurteilung auch auf alle anderen am 6. Juli 2006 festgenommen Personen zu übertragen, soweit sie weder vorher noch nachher mit der Polizei zu tun hatten und ihnen bei der Demonstration keine konkrete Beteiligung an einer Gewalttat vorgeworfen werden kann. Dem kam die Polizei nach. Sie löschte bei 199 Personen die Datenspeicherungen und vernichtete die dazugehörigen Unterlagen. Bei 25 Personen führte die Einzelfallbeurteilung zu einem anderen Ergebnis.

4.3.3 Auskunft über eigene Daten aus der Vorgangsverwaltungsdatei ComVor der Polizei

Das Auskunftsrecht nach § 29 HSOG bezieht sich nicht nur auf das polizeiliche Auskunftssystem POLAS, sondern grundsätzlich auf alle polizeiliche Dateien, in denen personenbezogene Daten verarbeitet werden. Polizeiintern scheint es Unklarheiten zu geben, wer für eine Auskunft aus der Datei ComVor zuständig ist.

Eingaben von Betroffenen haben mich darauf aufmerksam gemacht, dass es offenbar Schwierigkeiten gibt, wenn sie Auskunft aus der Datei ComVor (**Com**putergestützte **Vor**gangsbearbeitung), dem Vorgangsverwaltungssystem der Hessischen Polizei, über ihre Daten möchten.

Bereits früher hatte sich ein Bürger an mich gewandt, nachdem sein Auskunftsverlangen aus ComVor vom HLKA ans Präsidium für Technik, Logistik und Verwaltung (PTLV) verwiesen wurde. Vom PTLV wurde er an das zuständige Polizeipräsidium weiter verwiesen. Das Polizeipräsidium verwies dann - jeweils nach mehrmonatiger Wartezeit - wieder ans HLKA zurück. Ich ging damals von einem Einzelfall aus, den ich nicht an das HLKA herangetragen hatte, sondern mit dem zuständigen Polizeipräsidium Wiesbaden lösen konnte.

Jetzt wollte sich ein Einwohner aus dem Schwalm-Eder-Kreis bei der Polizei darüber informieren, ob Daten zu seiner Person in der Datei ComVor gespeichert sind. Er wandte sich an das PTLV und fragte nach den zu seiner Person gespeicherten Daten, dem Zweck und der Rechtsgrundlage der Speicherung und Verarbeitung und der Herkunft der Daten, soweit dies gespeichert oder sonst bekannt ist. Seiner Anfrage, so begründete er sein Verlangen, liege ein generelles Informationsinteresse unter Wahrnehmung seines verfassungsrechtlich verbürgten Grundrechtes auf informationelle Selbstbestimmung zugrunde.

Seiner Anfrage an das PTLV war dieselbe Fragestellung an das HLKA vorausgegangen. An diese Behörde wandte er sich etwa vier Monaten zuvor und bezog seine Frage auf das polizeiliche Auskunftssystem POLAS und das Vorgangsverwaltungssystem ComVor. Das HLKA hat ihn mit der Mitteilung beschieden, dass keine Daten zu seiner Person in POLAS gespeichert sind. Bzgl. der Datei ComVor möge er sich aus Zuständigkeitsgründen an das PTLV wenden. Postwendend erhielt er vom PTLV die Antwort, es sei nicht zuständig. Das HLKA sei zuständig; sein Brief sei dorthin weitergeleitet worden. Nach weiteren drei Monaten erhielt er von dort die Mitteilung, ComVor sei kein Auskunfts- und Recherchesystem zur Informationsgewinnung, sondern ein polizeiinternes Vorgangsbearbeitungs- und -verwaltungssystem. Auskunft aus ComVor würde nicht erteilt.

Er monierte noch beim HLKA, er könne der gesetzlichen Regelung (§ 29 HSOG) keinen Hinweis darauf entnehmen, dass polizeiinterne Dateien von der Regelung über die Auskunftserteilung ausgenommen seien. Seine Frage blieb unbeantwortet. Gleichzeitig wandte er sich an mich.

Die Rechtsauffassung des Bürgers aus dem Schwalm-Eder-Kreis trifft zu. Die Auskunft nach § 29 HSOG bezieht sich nicht nur auf Auskunfts- und Recherchesysteme zur Informationsgewinnung, sondern auch auf polizeiinterne Vorgangsverwaltungssysteme wie ComVor.

§ 29 HSOG

(1) Der betroffenen Person ist auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. die Herkunft der Daten und die Empfängerinnen oder die Empfänger von Übermittlungen, soweit dies festgehalten ist,
3. den Zweck und die Rechtsgrundlage der Speicherung und sonstigen Verarbeitung.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Bei einem Antrag auf Auskunft aus Akten kann erforderlichenfalls verlangt werden, dass Angaben gemacht werden, die das Auffinden der Daten ohne einen Aufwand ermöglichen, der außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Kommt die betroffene Person dem Verlangen nicht nach, kann der Antrag abgelehnt werden. Statt einer Auskunft über Daten in Akten können die Gefahrenabwehr- und die Polizeibehörden der betroffenen Person Akteneinsicht gewähren.

(2) Abs. 1 gilt nicht für Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden.

(3) Abs. 1 gilt außerdem nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte der betroffenen Person hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung insoweit nicht, als durch die Mitteilung der Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

(5) Wird Auskunft nicht gewährt, ist die betroffene Person darauf hinzuweisen, dass sie sich an die Datenschutzbeauftragte oder den Datenschutzbeauftragten wenden kann. Dies gilt nicht in den Fällen des Abs. 1 Satz 4. Die Mitteilung der Datenschutzbeauftragten oder des Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern sie nicht einer weitergehenden Auskunft zustimmt.

Das Auskunftsrecht bezieht sich - von einigen Anwendungsausnahmen abgesehen - auf alle automatisiert und nicht automatisiert gespeicherten personenbezogenen Daten der Polizei (so auch Meixner/Fredrich, Rdnr. 6 und 5 zu § 29, und Hornmann, Rdnr. 7 zu § 29, in ihren Kommentaren zum HSOG). Das Verlangen des Bürgers aus dem Schwalm-Eder-Kreis war mit § 29 HSOG rechtlich begründet.

Nachdem sich bereits zum zweiten Mal keine der Polizeibehörden für die Auskunft aus dem System ComVor zuständig fühlte, musste ich annehmen, dass es ein organisatorisches Problem gibt.

Ich bat deshalb das HLKA, sich dieses Problems einmal anzunehmen und mich über die Zuständigkeiten und das ggf. Veranlasste zu informieren. Bezüglich der Rechtsfrage bat ich um Stellungnahme. Ferner bat ich, dem Betroffenen Auskunft zu erteilen.

Das HLKA informierte mich, dass es sich bzgl. der Zuständigkeiten um eine Klärung bemühe. Bzgl. des Auskunftsverhaltens sei man sich noch nicht ganz sicher, wie man künftig verfahren wolle; auch dazu werde an einer Lösung gearbeitet. Damit aber erst einmal die Interessen des Anfragers erfüllt sind, bat das HLKA mich, dem Betroffenen mitzuteilen, dass keine Daten zu seiner Person in der Datei ComVor gespeichert sind. Dieser Bitte kam ich nach. Auf diese Weise erhielt der Anfrager nach ca. einem Jahr hartnäckigen Nachfragens schließlich die Auskunft aus der Datei ComVor.

4.3.4 Zugriff auf das Passbild bei der Fahrerfeststellung

Ordnungswidrigkeitenbehörden dürfen zur Verfolgung von Verkehrsordnungswidrigkeiten das Radarfoto mit dem Lichtbild des Ausweisregisters vergleichen.

Das Hessische Ministerium des Innern hat mich von seiner Absicht in Kenntnis gesetzt, bei der Verfolgung von Verkehrsordnungswidrigkeiten einen schnelleren Abgleich des Beweisfotos mit dem Fotobestand des Pass- oder Personalausweisregisters zuzulassen. Es bat mich zu seinem Vorhaben um eine Stellungnahme.

Rechtsgrundlage des Verfahrens ist § 2b Abs. 2 Gesetz über Personalausweise (PAuswG).

§ 2b Abs. 2 PAuswG

Die Personalausweisbehörden dürfen anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln. Voraussetzung ist, dass

1. die ersuchende Behörde aufgrund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten,
2. die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und
3. die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss.

Das Passgesetz enthält in § 22 Abs. 2 eine sinngleiche Regelung.

Am Vorliegen der beiden ersten Voraussetzungen bestehen keine Zweifel. Die zu interpretierende Passage findet sich in Ziff. 3 der Norm: Der Zugriff auf das Lichtbild als eine Information der Ausweisregister ist u.a. nur zulässig, wenn die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können.

Eine Verwaltungsvorschrift des HMDIS führte bislang dazu aus:

Erlass HMDIS vom 6. Januar 2006 (StAnz. S. 286), Ziff. 3.2

Muss geprüft werden, ob die auf dem Lichtbild als Fahrzeugführerin oder Fahrzeugführer abgebildete Person diejenige ist, der die Verkehrsordnungswidrigkeit zur Last gelegt wird (betroffene Person), ist es grundsätzlich ausreichend, sie vorzuladen. Die betroffene Person ist mit der Vorladung auf mögliche Maßnahmen bei Nichtbeachtung der Vorladung hinzuweisen. Erscheint die betroffene Person nicht oder bringt die Inaugenscheinnahme der/des Betroffenen keine hinreichende Sicherheit hinsichtlich der Identität der/des Vorgeladenen mit der auf dem Foto abgebildeten Person, sind grundsätzlich die Personalausweisbehörden und lediglich hilfsweise, soweit die/der Betroffene nur einen Reisepass besitzt, die Passbehörden zu ersuchen, das Lichtbild aus dem Personalausweis- oder Passregister zu übermitteln und insoweit Einsicht in das Register zu gewähren. …

Das Ministerium argumentierte, in dem zuständigen Bund-Länder-Fachausschuss sei im Jahre 2006 der Beschluss gefasst worden, dass länderübergreifende Ermittlungsersuchen erst dann gestellt werden, wenn bürointerne Ermittlungshandlungen nicht weitergeholfen hätten oder keinen Erfolg versprächen. Als bürointerne Ermittlung werde auch der Abgleich des Passfotos im Rahmen der gesetzlichen Bestimmungen gesehen. Seit diesem Zeitpunkt würden Vorladungsersuchen der Zentralen Bußgeldstelle des Regierungspräsidenten Kassel an Polizeibehörden anderer Bundesländer zunehmend unter Berufung auf diesen Beschluss mit der Begründung zurückgesandt, man möge zunächst einen Abgleich mit dem Passfoto vornehmen. Die Verfahren müssten dann eingestellt werden, weil beide in Frage kommenden Ermittlungsmaßnahmen nicht möglich seien. Das länderübergreifende Vorladungsersuchen werde abgelehnt, weil noch kein Fotovergleich stattgefunden hat. Der Fotovergleich sei nicht möglich, weil der Erlass zur vorherigen Vorladung zwinge. Das Regierungspräsidium Kassel dränge daher darauf, dass das HMDIS einen Passbildvergleich ohne vorherige Vorladung zulasse. Die Polizeibehörden hätten sich diesem Verlangen angeschlossen. Das HMDIS hält es für vertretbar, eine Vorladung in einem Bußgeldverfahren wegen einer Verkehrsordnungswidrigkeit zum Zwecke der Feststellung, ob die Person des Halters mit der des Fahrers identisch ist, als "unverhältnismäßig hohen Aufwand" i.S.d. § 2b Abs. 2 Nr. 3 PAuswG zu bewerten, wenn der Halter bzw. die Halterin zuvor erfolglos nach § 55 OWiG angehört und auf die Möglichkeit des Passbildvergleiches hingewiesen worden ist.

Diese Argumentation ist plausibel. Ich habe dem Ministerium mitgeteilt, dass ich einer Änderung der Verwaltungsvorschrift nicht widerspreche.

Danach wurde die zitierte Passage in der Verwaltungsvorschrift wie folgt geändert:

Erlass HMDIS vom 9. Juli 2008 (StAnz. S. 1958), Ziff. 3.2

Muss geprüft werden, ob die auf dem Lichtbild als Fahrzeugführerin oder Fahrzeugführer abgebildete Person diejenige ist, der die Verkehrsordnungswidrigkeit zur Last gelegt wird (betroffene Person), kann die Personalausweisbehörde und hilfsweise, soweit die/der Betroffene nur einen Reisepass besitzt, die Passbehörde ersucht werden, das Lichtbild aus dem Personalausweis- oder Passregister zu übermitteln und insoweit Einsicht in das Register zu gewähren, wenn die betroffene Person zuvor erfolglos nach § 55 OWiG angehört und auf die Möglichkeit des Bildvergleichs hingewiesen worden ist. …

Damit ist die Pflicht, vor dem Zugriff auf das Lichtbild, Betroffene noch einmal vorzuladen, entfallen. Aus meiner Sicht ist dabei ausschlaggebend, dass Betroffene über die Möglichkeit des Zugriffs auf ihr Passfoto informiert werden und so die Möglichkeit haben, die Datenerhebung abzuwenden indem sie im Zuge der Anhörung nach § 55 OWiG an der Aufklärung der Ordnungswidrigkeit mitwirken.

4.4 Ausländerrecht

4.4.1 Prüfung von Ausländerbehörden

Entsprechend dem Beschluss der Gemeinsamen Kontrollinstanz Schengen habe ich überprüft, ob die bei der im Jahre 2004 in allen Schengenländern durchgeführten Prüfung von Ausschreibungen zum schengenweiten Wiedereinreiseverbot im SIS festgestellten Defizite weiterhin bestehen. Die Prüfung von Ausländerbehörden hat - regional unterschiedlich ausgeprägt - die Mängel bestätigt.

4.4.1.1 Follow-up-check der europaweit koordinierten Prüfung im Jahre 2004

Die GK (s. Ziff. 2.1.1.3) hat im März d.J. beschlossen, dass nationale Datenschutzkontrollstellen der Schengenstaaten prüfen sollen, ob die bei der europaweit koordinierten Prüfung im Jahre 2004 festgestellten Defizite weiterhin bestehen (sog. follow-up-check).

Die damals in Hessen festgestellten Defizite (s. 33. Tätigkeitsbericht, Ziff. 3.2) bezogen sich zum einen auf Ausschreibungen, die ohne ausreichenden Rechtsgrund stattfanden. Meist war den Ausländern mitgeteilt worden, sie seien ausreisepflichtig und hätten die Bundesrepublik Deutschland bis zu einem bestimmten Termin zu verlassen. Der Ausländerbehörde lagen keine Informationen vor, ob die Ausländer tatsächlich ausgereist waren. Sie nahm an, dass sie "untergetaucht" waren und möglicherweise ohne Aufenthaltsgenehmigung irgendwo in Deutschland lebten. Diese Annahme reicht aber nicht aus, um ein schengenweites Wiedereinreiseverbot zu verfügen. Art. 96 Abs. 3 SDÜ (Zitat s. Ziffer 2.1.1.3) verlangt ausdrücklich u.a., dass der Betroffene ausgewiesen, zurückgewiesen oder abgeschoben worden sein muss.

Zum anderen war festgestellt worden, dass das Gebot in Art. 112 Abs. 1 SDÜ, die Erforderlichkeit der Datenspeicherung spätestens nach drei Jahren zu überprüfen, nicht eingehalten worden war.

Art. 112 Abs. 1 SDÜ

Die zur Personenfahndung in dem Schengener Informationssystem aufgenommenen personenbezogenen Daten werden nicht länger als für den verfolgten Zweck erforderlich gespeichert. Spätestens drei Jahre nach ihrer Einspeicherung ist die Erforderlichkeit der weiteren Speicherung von der ausschreibenden Vertragspartei zu prüfen. Für die Ausschreibung gemäß Artikel 99 beträgt diese Frist ein Jahr.

In jedem Einzelfall wird die Ausländerbehörde durch ein Formschreiben des BKA auf den Ablauf der 3-Jahres-Frist hingewiesen. Aus Vereinfachungsgründen und zur Vermeidung von ungewollten Datenlöschungen braucht die Ausländerbehörde, falls sie die Fortdauer der Datenspeicherung verfügt, bezüglich deren technischer Umsetzung im SIS nichts zu unternehmen. Das BKA informiert in dem Formbrief, dass es die Dauer der Datenspeicherung vorläufig bereits um drei Jahre ver-

längert hat. Die Ausländerbehörde muss nun nur noch die Prüfung vornehmen und die Gründe für die Verlängerung dokumentieren. Andernfalls muss sie mittels des Vordruckes des BKA die Löschung im SIS verfügen. Ein entsprechender Text ist bereits vorgedruckt, sie muss dieses Blatt lediglich unterschreiben und an das LKA weiterreichen. Von dort wird die vorläufige Verlängerung rückgängig gemacht. Dies führt zur automatischen Löschung des Datensatzes.

Nach einer Speicherdauer von sechs Jahren wird die Ausländerbehörde vom BKA auf den erneuten Ablauf der 3-Jahres-Frist hingewiesen. Nun ist das Verfahren umgekehrt. Der Vordruck ist dementsprechend anders formuliert. Will die Ausländerbehörde die Datenspeicherung aufrechterhalten, so muss sie dies nun ausdrücklich verfügen **und** die – schon vorgedruckte – Verfügung dem LKA mitteilen. Das LKA kann dann die Verlängerung der Speicherdauer in das System eingeben. Die Verfügung muss, versehen mit einer Begründung, in der Akte dokumentiert sein. Will sie dagegen die Löschung der Speicherdauer hinnehmen, muss sie nichts tun. Das DV-System löscht die Daten automatisch zum Ablauf des sechsten Jahres nach der Ersteinspeicherung.

Bei der Kontrolle im Jahre 2004 habe ich festgestellt, dass die Prüfung nach 3-jähriger Speicherdauer zum überwiegenden Teil nicht stattfand. Soweit sie stattfand, führte sie nur selten zur Löschung im SIS. Gründe für die Fristverlängerung waren nur in Einzelfällen ersichtlich; meist nicht vorhanden.

Diesen Mangel hatte ich schon einmal nach einer im Jahre 2000 durchgeführten Prüfserie beschrieben (s. 29. Tätigkeitsbericht, Ziff. 12.1). Sie führte damals zu einem Erlass (nicht veröffentlicht) des Hessischen Ministeriums des Innern und für Sport, in dem alle Ausländerbehörden auf die Prüf- und Dokumentationspflicht hingewiesen wurden.

Auszug aus dem Erlass des HMDIS vom 5. Dezember 2000

2.2 Ausschreibungen im SIS nach Art. 96 Abs. 3 SDÜ

Wenn die Ausländerbehörde vor dem Ablauf der Ausschreibungspflicht nach spätestens drei Jahren die Mitteilung über den Fristablauf erhält, hat sie im Einzelfall zu überprüfen, ob die Verlängerung der Ausschreibung erforderlich ist (Art. 112 Abs. 4 SDÜ). Die Gründe für eine Verlängerung der Ausschreibung sind in der Akte zu vermerken.

Ich habe nun bei zwei Ausländerbehörden die Prüfserie aus den Jahren 2000 und 2004 fortgesetzt. Ausgewählt hatte ich die Ausländerbehörden des Landkreises Bergstraße und der Stadtverwaltung Darmstadt.

Um gezielt den damals festgestellten Defiziten nachgehen zu können, habe ich das LKA gebeten, mir zu diesen beiden Ausländerbehörden alle Datensätze von Betroffenen aufzulisten, deren Erstausschreibung länger als drei Jahre zurückliegt. Jeweils ca. ein Viertel des Gesamtbestandes habe ich der Prüfung unterzogen.

4.4.1.2 Ausländerbehörde des Landkreises Bergstraße

Beim Landkreis Bergstraße habe ich 25 Einzelfälle überprüft. Davon lagen in 5 Fällen die Ausschreibungsvoraussetzungen nicht vor. Die Betroffenen waren weder ausgewiesen noch zurückgewiesen noch abgeschoben worden.

Ebenso unbefriedigend war das Ergebnis bezüglich der Prüfung nach 3-jähriger Speicherdauer.

Von den 25 geprüften Fällen

- war in 13 Fällen nicht ersichtlich, dass diese Prüfung stattgefunden hat. Sie war jedenfalls nicht dokumentiert. Auch das Formschreiben des BKA befand sich nicht in den Akten. In nahezu allen dieser Fälle waren auch keine Gründe ersichtlich, die eine Fortdauer des Einreiseverbotes begründet hätten.

- In einem Fall befand sich das Formschreiben des BKA zwar in der Akte, war aber offensichtlich nur unbearbeitet abgeheftet worden.

- In neun Fällen hatte die Ausländerbehörde die Ausschreibungen von Anfang an auf drei Jahre befristet. Das ist aus meiner Sicht zu begrüßen. Diese Befristungen wurden aber vom BKA aufgrund des oben beschriebenen Verfahrens nicht beachtet. Ich werde der Frage noch nachgehen, weshalb das BKA solche Befristungen ignoriert. Dennoch war festzuhalten, dass die Ausländerbehörde trotz der Befristungen nicht gutgläubig von Löschungen ausgehen konnte, denn sie wurde durch die erwähnten, systemseitig hergestellten Vordrucke jeweils auf die Verlängerung der Datenspeicherungen aufmerksam gemacht. Die Hinweisschreiben des BKA waren in sieben dieser Fälle unbearbeitet abgeheftet. In den anderen beiden dieser neun Fälle waren sie nicht aufzufinden. Bei mehreren dieser neun Fälle lag die Ersteinspeicherung sogar länger als sechs Jahre zurück. Bei der nach sechs Jahren vorzunehmenden Prüfung erfolgt die Verlängerung der Speicherdauer nur, wenn die Ausländerbehörde aktiv wird. Entgegen ihrer ursprünglichen Befristung muss sie also nach der 6-jähriger Speicherdauer die Fortdauer des Einreiseverbots verfügt haben, denn sonst wäre die Datenspeicherung automatisch gelöscht worden.

- In zwei Fällen war die Prüfung ordnungsgemäß erfolgt und die Löschung verfügt worden.

4.4.1.3 Ausländerbehörde der Stadtverwaltung Darmstadt

Bei der Ausländerbehörde der Stadt Darmstadt habe ich 35 Einzelfälle überprüft. Bei allen lagen die Ausschreibungsvoraussetzungen vor.

Zu der Prüfung nach dreijähriger Speicherdauer konnte ich feststellen, dass die materiellen Voraussetzungen zur Verlängerung der Speicherdauer in nahezu allen Fällen gegeben waren. Die Prüfungen waren auch dokumentiert und begründet. Die Ausländerbehörde hatte sich selbst einen Vordruck geschaffen, den sie auf die Rückseite des BKA-Formschreibens aufdruckte. Darin werden optional Gründe für die Verlängerung der Speicherdauer aufgeführt und die Bearbeiter brauchten nur noch anzukreuzen, weshalb die Fortdauer der Datenspeicherung für erforderlich erachtet wurde. In den meisten Fällen war angegeben, dass der Betroffene Straftaten begangen hatte, die in §§ 53 oder 54 AufenthG genannt sind (z.B. Verstöße gegen das Betäubungsmittelgesetz oder Schleuserkriminalität) oder dass der Betroffene entgegen des Wiedereinreiseverbotes erneut eingereist ist. Dies sind Gründe, die eine Verlängerung rechtfertigen.

Zu bemängeln war der jeweilige Zeitpunkt der Prüfungen. Selten zeitnah, meist einige Quartale und oft auch über ein Jahr später als die Mitteilungen des BKA datiert sind, war die Bearbeitung erfolgt. Auch war ersichtlich, dass kurz vor meiner Datenschutzkontrolle ausstehende Prüfungen noch schnell nachgeholt worden sind. Soweit Gründe für die Verlängerungen vorlagen, handelte es sich "nur" um einen Formfehler. Doch nach den festgestellten zeitlichen Abläufen war damit zu rechnen, dass auch bei denjenigen Betroffenen, deren Wiedereinreiseverbot zu löschen war, die Löschungen immer erst entsprechend verspätet verfügt worden waren.

4.4.1.4 Ergebnis

Im Landkreis Bergstraße waren 25 v.H. der Ausschreibungen zum Wiedereinreiseverbot ins Schengengebiet rechtswidrig. Die Datenspeicherungen, die älter als drei Jahre waren, waren zu über 90 v.H. fehlerhaft. Aufgrund der hohen Fehlerquote habe ich den Landrat des Landkreises Bergstraße gebeten, den gesamten Bestand der von seiner Behörde veranlassten Ausschreibungen im SIS zu überprüfen. Dieser hat mir mitgeteilt, er habe alle unzulässigen Ausschreibungen zurückgenommen. Fehlende Prüfungen seien nachgeholt und dokumentiert worden. Sie hätten zu weiteren Löschungen geführt. Eine Prüfung des Gesamtbestandes aller restlichen Ausschreibungen sei veranlasst. Weiterhin habe er intern geregelt, wie künftig bei SIS-Ausschreibungen zu verfahren sei, insbesondere auch im Hinblick auf die Überwachung der Speicherdauer.

Die Stadtverwaltung Darmstadt hat eingeräumt, dass alle ausstehenden Prüfungen kurz vor meiner Kontrolle nachgeholt worden waren. Auch die Annahme, dass notwendige Löschungen regelmäßig verspätet erfolgt sind, wurde bestätigt. Die Bearbeitung der Formschreiben des BKA genieße nicht immer die notwendige Priorität. Die Behörde versprach Besserung. Jetzt, nachdem alle ausstehenden Prüfungen nachgeholt seien, sei man auf dem aktuellen Stand, der solle gehalten werden - so die Ausländerbehörde Darmstadt.

Nach Ablauf einer angemessenen Zeit werde ich bei beiden Ausländerbehörden die Einhaltung der getroffenen Zusagen überprüfen.

4.5 Schulen und Schulverwaltung

4.5.1 Ergebnisse der Prüfung beim Staatlichen Schulamt Hanau

Die Prüfung des Staatlichen Schulamtes Hanau erbrachte keine überraschenden Ergebnisse, bestätigte aber meine Erfahrung, dass vermeidbare datenschutzrechtliche Mängel in den Schulaufsichtsbehörden immer wieder anzutreffen sind.

Im Berichtsjahr stattete ich dem Staatlichen Schulamt für den Main-Kinzig-Kreis in Hanau einen Prüfbesuch ab. Schulaufsichtsämter gehören immer wieder zum jährlichen Prüfprogramm, weil sie auch eine Vorbildfunktion für die übrige Schulverwaltung haben sollten (s. auch 31. Tätigkeitsbericht, Ziff. 15.1). Nachfolgend sind die wichtigsten Prüfergebnisse dargestellt, in der Hoffnung, dass sie bei den übrigen Schulämtern künftig beachtet werden.

4.5.1.1 Bestellung eines stellvertretenden Datenschutzbeauftragten

Nach § 5 Abs. 1 S. 1 HDSG muss jede hessische Behörde neben dem hauptamtlichen auch einen stellvertretenden Datenschutzbeauftragten schriftlich bestellen.

§ 5 Abs. 1 Satz 1 HDSG

Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen.

Die Stellvertreterin war nur in mündlicher Form bestellt. Es wurde zugesagt, die schriftliche Bestellung umgehend nachzuholen.

Weiter verlangt die Vorschrift in Satz 3 schon bei der Bestellung das Vorliegen der "erforderlichen Sachkenntnis".

§ 5 Abs. 1 Satz 3 HDSG

Für die Wahrnehmung seiner Aufgaben nach Abs. 2 muss der behördliche Datenschutzbeauftragte die erforderliche Sachkenntnis und Zuverlässigkeit besitzen.

Diese Sachkenntnis verlangt vor allem ein vertieftes Fachwissen in den in der jeweiligen Verwaltung geltenden allgemeinen und besonderen Datenschutzvorschriften, das z.B. durch den Besuch von Fachseminaren erworben werden kann. Bei der Bestellung war die erforderliche Sachkenntnis nicht vorhanden. Maßnahmen zur Vermittlung dieser Kenntnisse waren weder im Zusammenhang mit der Bestellung noch danach geplant. Auf meinen Hinweis wurde der baldige Besuch eines Fachseminars zugesagt.

4.5.1.2 Verschlüsselung bei der Speicherung der Diagnosedaten des Schulpsychologen

Schulpsychologen nutzen der Einfachheit halber zunehmend die Verwaltungs-IT des Staatlichen Schulamts und speichern dabei u.a. auch ihre Gutachten über die körperlichen und psychischen Erkrankungen der von ihnen untersuchten Personen. Diese Daten sind naturgemäß von außerordentlich hoher Sensibilität. Um diese Daten auch vor der technisch möglichen Einsicht durch Wartungspersonal oder Systemadministratoren absolut zu schützen, sieht § 83 Abs. 6, letzter Satz HSchulG zwingend vor, dass diese Daten nur verschlüsselt gespeichert werden dürfen. Eine solche technische Möglichkeit fehlte jedoch auf den Rechnern der Psychologen.

§ 83 Abs. 6, letzter Satz HSchulG

Personenbezogene Daten des schulpsychologischen Dienstes dürfen nur automatisiert verarbeitet werden, wenn sie dabei nach dem jeweiligen Stand der Technik hinreichend sicher verschlüsselt werden.

Die Rechtsgrundlage ist eindeutig: Steht eine Verschlüsselung nicht zur Verfügung, darf eine automatisierte Verarbeitung nicht erfolgen. Gleichwohl verfügte bis Redaktionsschluss der schulpsychologische Dienst nicht über die Möglichkeit der Verschlüsselung. Das HKM wollte zukünftig auch für die Schulpsychologen das Dokumentenmanagementsystem DOMEA nutzen.

Auf die Dringlichkeit einer Lösung habe ich das HKM nachdrücklich hingewiesen. Den Bevollmächtigten für eGovernment und Informationstechnologie in der Landesverwaltung habe ich im Hinblick auf die Notwendigkeit, auch im DOMEA eine Verschlüsselung vorzusehen, auf diese Problematik angesprochen. Ich erhielt die Zusage, dass entweder kurzfristig eine Verschlüsselungslösung in DOMEA realisiert oder dem schulpsychologischen Dienst eine Möglichkeit geboten wird, seine Dokumente verschlüsselt abzulegen. Erfreulich rasch, d.h. noch im Dezember, hat das HKM mit einem Erlass die Schulämter angewiesen, eine verschlüsselte Ablage auf den Fileservern der staatlichen Schulämter bis Ende Januar einzurichten. Sobald DOMEA eine Verschlüsselungslösung anbietet, soll diese dann genutzt werden.

4.5.1.3 Vernichtung und Archivierung des Schriftgutes

Soweit die elektronischen und papierbezogenen Verwaltungsunterlagen nicht mehr im Verwaltungsalltag benötigt werden, wird es erforderlich sein, sie noch für einen bestimmten Zeitraum in der Daten verarbeitenden Stelle aufzubewahren, z.B. um Rückfragen beantworten zu können. Diesem Umstand wird durch die Festsetzung von an der Verwaltungserfahrung orientierten Aufbewahrungsfristen Rechnung getragen, innerhalb derer die Unterlagen - obwohl der zugrunde liegende Vorgang abgeschossen ist - noch aufzubewahren sind. Die für die unterschiedlichen Arten von Unterlagen differenziert ausgelegten Aufbewahrungsfristen sind im Erlass des HMDIS vom 16. Mai 2007 (StAnz. 2007, S. 1125) für die gesamte Landesverwaltung festgelegt. Nach Ablauf der Frist sind die dann auszusondernden Unterlagen dem örtlich zuständigen Staatsarchiv anzubieten, wie es § 10 HAchivG vorschreibt.

§ 10 HArchivG

(1) Die in § 6 genannten Stellen sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind, unverzüglich auszusondern und dem zuständigen Archiv zur Übernahme anzubieten. Dies soll spätestens dreißig Jahre nach Entstehung der Unterlagen erfolgen. Diejenigen elektronischen Unterlagen, die einer laufenden Aktualisierung unterliegen, werden in Absprache dem zuständigen Archiv angeboten. Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterworfen sind. Unberührt bleiben gesetzliche Vorschriften über die Löschung oder Vernichtung unzulässig erhobener oder verarbeiteter Daten oder Unterlagen.

(2) Die in § 6 genannten Stellen dürfen Unterlagen nur vernichten oder Daten nur löschen, wenn das zuständige öffentliche Archiv die Übernahme abgelehnt oder nicht binnen eines Jahres über die Archivwürdigkeit angebotener Unterlagen entschieden hat. Von dem Anbieten und Vorhalten von Unterlagen von offensichtlich geringer Bedeutung kann im Einvernehmen mit dem zuständigen öffentlichen Archiv abgesehen werden. Ausgesonderte Unterlagen, deren Übernahme von den öffentlichen Archiven abgelehnt wird, sind im Regelfall zu vernichten, sofern kein Grund zu der Annahme besteht, dass durch die Vernichtung schutzwürdige Belange von Betroffenen beeinträchtigt werden.

Eine Überprüfung des "Archivs" des Staatlichen Schulamtes ergab, dass bei zahlreichen Unterlagen die Aufbewahrungsfrist abgelaufen war. Diese Unterlagen hätten ausgesondert und dem Staatsarchiv angeboten werden müssen. Die Verwaltung des Staatlichen Schulamtes sagte zu, diese Schritte unverzüglich einzuleiten.

4.5.1.4 Das Schlüsselsystem

Eine Kontrolle des im Erdgeschoss in der Nähe des Haupteinganges befindlichen Postraums ergab, dass dieser im Kontrollzeitpunkt offen stand und nicht besetzt war. Der unkontrollierte Zugriff auf alle dort befindlichen Postfächer war damit möglich. Noch erheblich problematischer war jedoch, dass in diesem Raum der zentrale Schlüsselkasten an der Wand hing, der zahlreiche Sicherheitsschlüssel enthielt für die meisten Räume des Amtes. Dieser Schlüsselkasten selbst war unverschlossen, der Schlüssel steckte im Schloss. Es bedarf keiner weiteren Darlegungen, dass dieser Zustand auf keinen Fall tolerabel war, auch wenn eingewendet wurde, dies sei ein seltener, unglücklicher Einzelfall. Er verstößt deutlich gegen die gesetzlich nach § 10 Abs. 3 HDSG geforderte Pflicht, den Aktenzugriff Unbefugter zu verhindern.

§ 10 Abs. 3 HDSG

Werden personenbezogene Daten nicht automatisiert verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Ein Raum-Schlüsselsystem dient dieser Pflicht, wenn die Schlüsselzuweisung deutlich ausdifferenziert an die Personen erfolgt, die die jeweiligen Räume zu unterschiedlichen dienstlichen Zwecken betreten dürfen. Der unkontrollierte Zugriff auf alle Schlüssel des Amtes konterkarierte das an sich sinnvoll angelegte Schließsystem. Es wurde mir zugesagt, künftig den zentralen Schlüsselkasten im Amtszimmer des Leiters der Verwaltung zu montieren und ihn permanent verschlossen zu halten. Nur wenige Bedienstete sollten künftig Zutritt zu diesem Zimmer und diesem Schlüsselkasten erhalten.

4.5.2 Panne bei der Datenübermittlung nach § 17 Meldedatenübermittlungsverordnung an Wiesbadener Schulen

Die Unkenntnis der einschlägigen Vorschriften führte dazu, dass in dem Schülerdatensatz, den die Schulen jährlich einmal zur Prüfung der eintretenden Schulpflicht vom Meldeamt vor Beginn des neuen Schuljahres erhalten, ein sensibles Schülerdatum enthalten war, das alle Wiesbadener Schulen vom Meldeamt der Stadt erhielten.

Rechtzeitig vor Beginn eines jeweiligen neuen Schuljahres muss die örtlich zuständige Grundschulleiterin oder der örtlich zuständige Grundschulleiter überprüfen, ob die Eltern die für ihr Kind eintretende Grundschulpflicht einhalten und es einschulen lassen (s. auch 36. Tätigkeitsbericht, Ziff. 5.6.1). Zwar sind die Eltern für die Einhaltung der Schulpflicht nach § 67 Abs. 1 HSchulG verantwortlich. Die Kontrolle obliegt nach § 88 Abs. 3 Nr. 2 aber der örtlich zuständigen Schulleitung.

§ 67 Abs. 1 HSchulG

Die Eltern sind dafür verantwortlich, dass die Schulpflichtigen am Unterricht und an den Unterrichtsveranstaltungen der Schule regelmäßig teilnehmen. Sie sind verpflichtet, die Schulpflichtigen bei der zuständigen Schule an- und abzumelden und sie für den Schulbesuch angemessen auszustatten.

§ 88 Abs. 3 HSchulG

Die Schulleiterin oder der Schulleiter ist für den ordnungsgemäßen Verwaltungsablauf in der Schule verantwortlich. Ihr oder ihm obliegen insbesondere die

1. Aufnahme und Entlassung der Schülerinnen und Schüler,
2. Sorge für die Erfüllung der Schulpflicht,
3. …

Um diese Kontroll-Pflicht einhalten zu können, sieht § 17 Abs. 1 der MeldedatenübermittlungsVO vor, dass das örtlich für die jeweilige Schule zuständige Meldeamt der Schule in Papierform einen Datenauszug zukommen lässt, der den exakt vorgeschriebenen Schülerdatensatz enthält.

§ 17 Abs. 1 MeldedatenübermittlungsVO

Die Meldebehörde übermittelt zur Überwachung der Erfüllung der Schulpflicht der jeweils zuständigen Grundschule nach § 143 Abs. 1 des Schulgesetzes in der Fassung vom 14. Juni 2005 (GVBl. I S. 442), zuletzt geändert durch Gesetz vom 11. Dezember 2007 (GVBl. I S. 921), automatisiert folgende personenbezogenen Daten der in § 58 Abs. 1 Satz 1 des Schulgesetzes genannten Kinder:

1. Familiennamen (jetziger Name mit Namensbestandteilen)
2. Vornamen
3. Tag und Ort der Geburt
4. Geschlecht
5. gesetzliche Vertreterin/gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt)
6. Staatsangehörigkeiten
7. gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch die letzte frühere Anschrift im Inland

Durch ein Gespräch mit der Leiterin einer Wiesbadener Grundschule erfuhr ich im Berichtsjahr zufällig, dass in der entsprechenden Schülerdatenliste des Jahres 2007 auch die Religionszugehörigkeit aller benannten Kinder enthalten war. Dieses Datum ist nicht nur nicht in der o.g. Datenliste aufgeführt, weil es für die Prüfung der Schulpflicht irrelevant ist, es stellt zudem auch ein sog. sensibles Datum nach § 7 Abs. 4 HDSG dar, dessen Verarbeitung an besonders strenge Voraussetzungen geknüpft ist.

§ 7 Abs. 4 HDSG

Soweit nicht eine Rechtsvorschrift die Verarbeitung personenbezogener Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben vorsieht oder zwingend voraussetzt, darf eine Verarbeitung nur nach §§ 33 bis 35 und 39 erfolgen. Im Übrigen ist eine Verarbeitung aufgrund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt und der Hessische Datenschutzbeauftragte vorab gehört worden ist.

In einem sofortigen Anruf beim Meldeamt der Stadt Wiesbaden forderte ich dieses auf, die Ursache dieser unzulässigen Datenübermittlung und auch die Frage zu klären, ob diese Panne in dem Zeitraum auch alle anderen Wiesbadener Grundschulen betraf. Dieser Verdacht bewahrheitete sich dann auch. Das Meldeamt hatte eine Fachfirma beauftragt, das entsprechende Datenauswertungsprogramm für diese Übermittlung zu erstellen. Diese Firma hatte dem Schülerdatensatz die Religionszugehörigkeit hinzugefügt. Eine Überprüfung durch das ebenfalls eingeschaltete Innenministerium in anderen hessischen Gemeinden ergab, dass dieser Fehler sich auf den Bereich des Wiesbadener Meldeamtes beschränkte.

Eine datenschutzrechtliche Prüfung des Programms und der daraus entstehenden Datensätze durch das Meldeamt hatte offensichtlich nicht stattgefunden. Anderenfalls wäre diese Panne verhindert worden.

Als datenschutzrechtliche Konsequenz der unzulässigen Datenübermittlung und der daraus entstandenen unzulässigen Datenspeicherung bei den Grundschulen sind die Religionsdaten nach § 19 Abs. 4 HDSG zu löschen.

§ 19 Abs. 4 HDSG

Personenbezogene Daten sind zu löschen, wenn ihre Verarbeitung unzulässig ist.

Von einer generellen Forderung der Löschung der unzulässig gespeicherten Daten habe ich aufgrund der folgenden Besonderheit abgesehen:

Wenn die Eltern ihr Kind zur Einschulung anmelden, sind sie nach § 83 Abs. 3 HSchulG verpflichtet, die für die Schulverwaltung erforderlichen Angaben zum Schüler zu machen.

§ 83 Abs. 3 HSchulG

Schülerinnen und Schüler, deren Eltern und Lehrerinnen und Lehrer sind verpflichtet, die erforderlichen Angaben zu machen.

Zu diesen Angaben gehören alle Schülerdaten, die in Anlage 1, Nr. 1.1 - 1.9 der "Verordnung über die Verarbeitung personenbezogener Daten in Schulen" erwähnt sind. Nach Nr. 1.9 der Anlage gehört dazu auch die Konfession bzw. Religionszugehörigkeit, sofern keine Befreiung vom Religionsunterricht vorliegt.

Zwar hätten die Daten der Religionszugehörigkeit nicht vom Meldeamt übermittelt werden dürfen. Sie hätten aber für alle Kinder, für die keine Befreiung vom Religionsunterricht vorliegt, von den Eltern erhoben werden müssen und wären dann im Datensatz der Schule vorhanden. Der zum Prüfungszeitpunkt relevante Datenbestand hätte nur die Religionszugehörigkeit von Kindern, die vom Religionsunterricht befreit sind, nicht enthalten dürfen.

Ich habe aus Praktikabilitätsgründen mit dem HKM deshalb vereinbart, dass dieses über das zuständige Staatliche Schulamt die Wiesbadener Grundschulen auffordert, die Schülerstammdaten des betroffenen Jahrganges auf diese Frage hin zu überprüfen und in allen den Fällen das Datum der Religionszugehörigkeit zu löschen, in denen eine Befreiung vom Religionsunterricht vorlag.

4.6 Landwirtschaft

4.6.1 Unzulässige Datenerhebung der Hessischen Tierseuchenkasse bei Tierpensionen

Die Tierseuchenkasse darf bei Tierpensionen keine Daten über die in Pension genommenen Tiere und ihre Halter erheben, es sei denn, die Halter haben darin eingewilligt.

4.6.1.1 Rechtswidrige Datenerhebung

Durch eine Beschwerde wurde ich darauf aufmerksam, dass die Hessische Tierseuchenkasse im Rahmen der Tierbestandserhebung bei Tierpensionen Daten über die in Pension genommenen Tiere und ihre Halter erhob. Die Kasse berief sich dabei auf eine Satzungsregelung. Nach § 1 Abs. 6 Satz 3 der Satzung der Hessischen Tierseuchenkasse über die Erhebung von Tierseuchenbeiträgen für das Wirtschaftsjahr 2008 konnten Personen, denen Tiere in Pension übergeben worden waren, die Tiere selbst der Tierseuchenkasse melden und hatten dann mit der Meldung eine Liste mit den Tierhaltern der bei ihnen aufgenommenen Tiere vorzulegen.

Die Vorschrift verstieß gegen § 12 Abs. 5 HAGTierSG. Die Tierbestandserhebung ist dort weitgehend geregelt. § 12 Abs. 5 HAGTierSG schreibt die Erhebungsmerkmale und das Erhebungsverfahren vor: Die Tierseuchenkasse gibt amtliche Erhebungskarten an die einzelnen Tierbesitzer aus (Satz 3). Erhoben werden Name und Anschrift der Tierbesitzer, landwirtschaftliche Betriebsnummer, Art und Zahl aller beim Tierbesitzer vorhandenen Tiere einer Gattung (Satz 4). Sonstige Angaben darf die Tierseuchenkasse nur verlangen, wenn sie Aufgaben der Tierseuchenbekämpfung dienen und wenn sie in der amtlichen Erhebungskarte als freiwillig bezeichnet werden (Satz 8). Die Tierbesitzer haben der Tierseuchenkasse die ausgefüllten Erhebungsbögen spätestens zwei Wochen nach dem Stichtag abzugeben (Satz 9).

§ 12 Abs. 5 HAGTierSG

Zur Beitragsberechnung führt die Tierseuchenkasse jährlich eine amtliche Erhebung an einem von ihr durch Satzung bestimmten Stichtag durch. Sofern sich bei einer Tierart die Zahl der Tiere um mehr als zehn vom Hundert - mindestens fünf Tiere -, bezogen auf den Stichtag, erhöht oder ein Tierbestand nach dem Stichtag neu begründet wird oder Tiere einer am

Stichtag nicht vorhandenen Tierart in einem Bestand neu aufgenommen werden, so sind die Tierbesitzer verpflichtet, die Änderung der Tierseuchenkasse unverzüglich zwecks Veranlagung mitzuteilen. Für die amtliche Erhebung gibt die Tierseuchenkasse amtliche Erhebungskarten an die einzelnen Tierbesitzer aus. Die Erhebungskarten sehen Angaben über Name und Anschrift der Tierbesitzer sowie die landwirtschaftliche Betriebsnummer und über die Art und die Zahl aller bei ihr oder ihm am Stichtag vorhandenen Tiere einer Gattung unabhängig vom Alter, Geschlecht, Gewicht oder von der Nutzungsart, in den Fällen von Satz 5 und 6 Angaben über den entsprechenden Umsatz, vor. Bei Viehhändlern sind abweichend von Satz 1 und 2 vier vom Hundert der Anzahl der im Vorjahr umgesetzten Tiere als der für die Berechnung der Beiträge maßgebende Viehbestand anzusetzen. Die Beitragsberechnung für Forellen und Karpfen richtet sich abweichend von Satz 1 und 2 bei Satzfischen nach der Anzahl der im Vorjahr umgesetzten Tiere, bei anderen Fischen nach dem im Vorjahr umgesetzten Gewicht. Näheres über die Beitragsberechnung regelt, auch unter Berücksichtigung von § 71 Abs. 1 Satz 4 des Tierseuchengesetzes, die Beitragssatzung. Sonstige Angaben dürfen nur verlangt werden, wenn sie Aufgaben der Tierseuchenbekämpfung dienen und wenn sie die amtliche Erhebungskarte als freiwillig bezeichnet. Die Tierbesitzer haben der Tierseuchenkasse die ausgefüllten Erhebungsbögen spätestens zwei Wochen nach dem Stichtag abzugeben. Die Angaben der Tierbesitzer dienen zugleich der Durchführung von Maßnahmen der Tierseuchenbekämpfung, zu denen die Tierseuchenkasse oder das Land Hessen Leistungen erbringt. Die Satzung der Tierseuchenkasse kann vorsehen, dass für die Beitragserhebung die Zahl der Tiere oder in den Fällen von Satz 5 und 6 der Umsatz des Vorjahres maßgeblich ist.

Nach dem HAGTierSG trifft allein den Tierbesitzer eine Meldepflicht. Personen, die Tiere in Pension nehmen, wären zwar, soweit sie die tatsächliche Gewalt über die Tiere haben, zivilrechtlich gesehen Tierbesitzer (§ 854 BGB). Die Satzung der Tierseuchenkasse stellte jedoch in § 1 Abs. 6 Satz 1 zu Recht klar, dass mit dem Begriff Tierbesitzer im Hessischen Ausführungsgesetz der Tierhalter i.S.v. § 833 BGB gemeint ist. Dafür spricht auch, dass im bundesrechtlichen Tierseuchengesetz nicht der Begriff Tierbesitzer, sondern Tierhalter als Anknüpfungspunkt für Mitwirkungs- und Duldungspflichten verwendet wird (vgl. § 23 Abs. 2 TierSG). Tierhalter ist nach der Rechtsprechung des BGH derjenige, der die Bestimmungsmacht über das Tier hat, aus eigenem Interesse für die Kosten des Tieres aufkommt, den allgemeinen Wert und Nutzen des Tiers für sich in Anspruch nimmt und das Risiko seines Verlustes trägt (BGH VI ZR 188/87, NJW-RR 1988, 655). Jemand, der Tiere in Pension nimmt, ist nicht Tierhalter und damit nicht Tierbesitzer im Sinne des Hessischen Ausführungsgesetzes, obwohl er möglicherweise die tatsächliche Gewalt über das Tier hat und damit zivilrechtlich Tierbesitzer ist.

Durch die Datenerhebung bei den Betreibern von Tierpensionen erhob die Tierseuchenkasse auch Angaben darüber, wem der Tierhalter seine Tiere zur Aufsicht übergeben hatte. Dieses Erhebungsmerkmal ging über den Katalog des § 12 Abs. 5 Satz 4 HAGTierSG hinaus. Solche Angaben darf die Tierseuchenkasse gemäß § 12 Abs. 5 Satz 8 HAGTierSG allenfalls auf freiwilliger Basis bei den Tierhaltern erheben.

Schließlich verstieß die Datenerhebung bei den Tierpensionen gegen § 12 Abs. 3 HDSG. Danach dürfen öffentliche Stellen wie die Tierseuchenkasse personenbezogene Daten bei Dritten außerhalb des öffentlichen Bereichs nur erheben, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt. Keine dieser Anforderungen war hier erfüllt.

Die Tierseuchenkasse musste deshalb ihre Satzung ändern. Ich habe ihr empfohlen, falls es triftige Gründe für eine Datenhebung bei den Tierpensionen geben sollte, auf eine entsprechende Änderung des HAGTierSG hinzuwirken.

4.6.1.2 Reaktion der Tierseuchenkasse

Die Tierseuchenkasse teilte mir mit, dass die Datenerhebung bei den Tierpensionen zwar unverzichtbar sei, aber wegen der entgegenstehenden Regelung im HAGTierSG die Satzung geändert und eine landesgesetzliche Regelung angestrebt werde. Im September 2008 hat mir das HMULV einen Entwurf eines Hessischen Ausführungsgesetzes zum Tierischen Nebenprodukte-Beseitigungsgesetz zur Stellungnahme vorgelegt. Da in dem Artikelgesetz auch Änderungen des HAGTierSG vorgesehen sind, habe ich das Ministerium in meiner Stellungnahme auch auf den Regelungsbedarf im Zusammenhang mit der Tierbestandserhebung durch die Tierseuchenkasse hingewiesen.

4.7 Gesundheitswesen

4.7.1 Aufbau einrichtungsübergreifender elektronischer Fallakten im Gesundheitsbereich

In zunehmendem Umfang wird auch in Hessen der Aufbau einrichtungsübergreifender Fallakten realisiert. Meine Dienststelle hat 2008 mehrere Projekte hinsichtlich der datenschutzrechtlichen Anforderungen beratend begleitet.

Seit einigen Jahren werden im Gesundheitsbereich in zunehmendem Umfang einrichtungsübergreifende elektronische Fallakten (eFA) geplant bzw. realisiert. Der Aufbau einer eFA wird von mehreren Behandlungseinrichtungen vereinbart, die einen bestimmten Patienten gemeinsam bezüglich einer spezifischen Diagnose oder eines spezifischen Behandlungskomplexes behandeln. Zweck der eFA ist es grundsätzlich, dass alle berechtigten Behandler in der eFA Behandlungsdaten speichern und auf die in der eFA gespeicherten Behandlungsdaten zugreifen können. Im Einzelnen unterscheiden sich die Projekte allerdings zum Teil erheblich hinsichtlich des Inhalts und der Zweckbestimmung der Fallakte sowie des vorgesehenen Kreises der Nutzer.

Meine Dienststelle hat 2008 insbesondere die folgenden Projekte beratend begleitet:

- das von der Universität Gießen in Kooperation mit weiteren Stellen betriebene Projekt CIMECS, eine internetbasierte Kommunikationsplattform zum Austausch von Patientendaten zwischen Haus- und Fachärzten sowie Kliniken (s. 36. Tätigkeitsbericht, Ziff. 5.8.3),

- das Projekt einer zentralen Datenbank für HIV-Patienten, an der ein Universitätsklinikum und mehrere Arztpraxen (Schwerpunktpraxen) beteiligt sind, und
- das Projekt der AOK Hessen "AOK aktiv und vital"; ein Projekt zur integrierten Versorgung i.S.v. §§ 140 ff. SGB V; ein wesentlicher Bestandteil dieses Vorhabens ist die gemeinsame Dokumentation der Behandlung eines Patienten durch die an der Behandlung beteiligten Ärzte und Kliniken.

Darüber hinaus wurde das Thema im Arbeitskreis "Datenschutz im Gesundheitswesen Hessen", an dem interne Datenschutzbeauftragte aus dem Gesundheitsbereich teilnehmen, besprochen.

Da einrichtungsübergreifende Fallakten betreffende Projekte im Detail unterschiedlich ausgestaltet sind, können die Anforderungen an Datenschutz und Datensicherheit nicht in allgemeiner Form abschließend konkretisiert werden. Wichtig ist in jedem Fall, dass **vor** der Einrichtung einer eFA aus datenschutzrechtlichen (und auch aus arztrechtlichen) Gründen eine Reihe von Aspekten geklärt und in einem Datenschutz- und Sicherheitskonzept festgelegt ist. Hierzu zählen insbesondere die folgenden Aspekte:

4.7.1.1 Zweck/Umfang/Beteiligte Ärzte bzw. Institutionen

Von zentraler Bedeutung ist zunächst die Festlegung des Inhalts und der konkreten Zweckbestimmung der eFA, da dies auch entscheidend ist für den Inhalt und Umfang der Datenschutz- und Datensicherheitsanforderungen. Aus der Zweckbestimmung ergibt sich auch die Dauer der Speicherung der Daten in der eFA, die ebenfalls festgelegt werden muss. Die Zweckbestimmung kann sehr verschieden sein. Es kann sich z.B. um eine Fallakte handeln, die speziell die Kommunikation zwischen entlassendem Krankenhaus und weiterbehandelndem niedergelassenen Arzt ermöglichen soll, oder auch um eine Fallakte, die eine längerfristige Kommunikation zwischen Hausarzt, Fachärzten und Klinik bezüglich einer Diagnose oder eines Behandlungskomplexes ermöglichen soll. Auch die ärztliche Betreuung von Schwangerschaften wird z.B. als Inhalt einer eFA diskutiert.

Ein Anwendungsfall für eine einrichtungsübergreifende eFA ist die integrierte Versorgung i.S.d. §§ 140 ff. SGB V. Gemäß § 140a SGB V können die Krankenkassen Verträge über eine verschiedene Leistungssektoren übergreifende Versorgung der Versicherten oder eine interdisziplinär-fachübergreifende Versorgung mit den in § 140b SGB V genannten Vertragspartnern abschließen. Gemäß § 140b Abs. 3 SGB V müssen die Vertragspartner eine an dem Versorgungsbedarf der Versicherten orientierte Zusammenarbeit zwischen allen an der Versorgung Beteiligten einschließlich der Koordination zwischen den verschiedenen Versorgungsbereichen und **eine ausreichende Dokumentation, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss**, sicherstellen. Eine Möglichkeit der Realisierung dieser Vorgaben ist die Einrichtung einer gemeinsamen eFA. Der Gesetzgeber hat in § 140a Abs. 2 SGB V festgelegt, dass die Teilnahme an der integrierten Versorgung für den Patienten freiwillig ist (s. dazu noch unten); nähere Einzelheiten zur rechtlichen, organisatorischen und technischen Ausgestaltung der gemeinsamen Dokumentation sind im Sozialgesetzbuch allerdings nicht geregelt, sodass auch hier dieser Fragenkatalog zu beachten ist.

4.7.1.2 Ärztliche Dokumentation im Sinne der Berufsordnung oder zusätzliche zentrale (Teil-)Datenspeicherung?

Der Arzt ist zur Dokumentation seiner Behandlung verpflichtet (vertragliche Nebenpflicht, ärztliche Berufsordnung). Klärungsbedürftig ist bei dem Aufbau einer eFA, ob diese Dokumentation weiterhin (ausschließlich?) bei den jeweiligen Leistungserbringern selbst oder (auch) in der eFA erfolgt. Derzeit wird bei vielen Projekten davon ausgegangen, dass die ärztliche Dokumentation i.S.d. Berufsordnung bei jedem der beteiligten Leistungserbringer selbst verbleibt, d.h. bei dem Inhalt der eFA handelt es sich um eine inhaltlich und zeitlich begrenzte zusätzliche Datenspeicherung, die eine Kommunikation **im konkreten Behandlungskontext** ermöglichen soll. Deshalb sollte für alle Dokumente in der eFA und beim jeweiligen Leistungserbringer einheitlich verfahren werden, da sonst verschiedene Rechtsfolgen z.B. bezüglich des Löschungszeitpunkts für die in der eFA gespeicherten Dokumente die Konsequenz wären. Soweit es sich um eine Zweitdokumentation handelt, ist klärungsbedürftig, ob lediglich Verweise (Links) gespeichert werden sollen oder Volltextdokumente. Zumindest die Dokumente von niedergelassenen Ärzten werden i.d.R. im Volltext in der eFA gespeichert, damit sie 24 Stunden am Tag für die Mitbehandler zur Verfügung stehen.

4.7.1.3 Wer ist verantwortliche Stelle für die zentral in der elektronischen Fallakte gespeicherten Daten?

Soweit Behandlungsdaten in Arztpraxen oder in Krankenhäusern gespeichert und weiterverarbeitet werden, gibt es für die betroffenen Patientinnen und Patienten eine klar erkennbare **verantwortliche Daten verarbeitende Stelle**. Die datenschutzrechtlichen Regelungen legen die Rechte und Pflichten dieser verantwortlichen Stelle fest (vgl. z.B. § 3 Abs. 7 BDSG; § 2 Abs. 3 HDSG) und es können sich z.B. die betroffenen Patientinnen oder Patienten an die jeweilige Stelle wenden zur Wahrnehmung ihrer Rechte auf Auskunft, Einsicht, Berichtigung, Sperrung und Löschung ihrer Daten. Bei der Einrichtung einer eFA sind die Verantwortlichkeiten geteilt. Es muss die Frage geklärt werden, wer für welche rechtlichen und/oder technisch-organisatorischen Entscheidungen/Verfahrensweisen/Maßnahmen verantwortlich ist und dies muss verbindlich in vertraglichen Vereinbarungen festgelegt werden.

Eine mögliche rechtliche Konstruktion ist z.B., dass zwischen den Beteiligten eine sog. **Verbunddatei** vereinbart wird, d.h. dass eine gemeinsame Datei eingerichtet wird, in der die beteiligten Stellen ihre für die eFA vorgesehenen Daten (im Regelfall Teildatensätze ihrer eigenen Dokumentation im Primärsystem) speichern, und in der die beteiligten Stellen die für ihre Behandlung erforderlichen Patientendaten der Mitbehandelnden lesen bzw. diese auch herunterladen können. Je nach den beteiligten Behandlungseinrichtungen sind unterschiedliche datenschutzrechtliche Regelungen für die Errichtung einer Verbunddatei bzw. eines Abrufverfahrens zu beachten. Für hessische Krankenhäuser gilt gemäß § 12 HKHG die Regelung des § 15 HDSG zu gemeinsamen Verfahren.

Erforderlich ist in jedem Fall die Klärung und vertragliche Festlegung der Inhalte der eFA, der Dauer der Speicherung der Volltextdokumente bzw. Links in der eFA und insbesondere der Verteilung der Verantwortlichkeiten zwischen den beteiligten Behandlungseinrichtungen, ferner auch die Maßnahmen zur Herstellung von Transparenz für die Patienten. Jede der beteiligten Stellen bleibt jeweils für ihre Daten verantwortliche Stelle, d.h. insbesondere verbleibt bei ihr die Verantwortlichkeit für die inhaltliche Richtigkeit ihrer Daten und dafür, dass nur die für die Speicherung in der eFA vorgesehenen Daten an die eFA übertragen werden und dass hierfür die Einwilligung des betroffenen Patienten vorliegt. Alle beteiligten Stellen müssen gemeinsam vereinbaren, welche der beteiligten Stellen als federführende Stelle mit der technischen Durchführung des gemeinsamen Verfahrens nach den vereinbarten Vorgaben beauftragt wird. Soweit für die Datenverarbeitung in der zentralen eFA durch die federführende Stelle ein externer Provider (Datenverarbeitung im Auftrag der federführenden Stelle) eingeschaltet werden soll, sind Fragen der Verschlüsselung der Patientendaten und des Beschlagnahmeschutzes zu klären. Es muss grundsätzlich sichergestellt werden, dass der Provider keine personenbezogenen Patientendaten zur Kenntnis nehmen kann.

Die federführende Stelle ist i.d.R. dafür verantwortlich, dass eine Stelle nur die Daten von Patienten bzw. Behandlungsfällen zur Kenntnis nehmen kann, an deren Behandlung sie auch beteiligt ist. Der federführenden Stelle obliegt die Verantwortung für die Zuordnung von Behandlungsteams zu Patienten und innerhalb der Teams für die korrekte Definition von Rollen und Berechtigungen als organisatorische Maßnahme.

Es muss darüber hinaus klar vereinbart werden, welche Stelle unter welchen Voraussetzungen welche Daten zu welchem Zweck in der eFA speichern und aus der eFA abrufen darf. Auch das Verfahren einer evtl. späteren Einräumung einer Speicherungs- und Zugriffsberechtigung an weitere (mit-)behandelnde Ärzte/Institutionen bedarf der Klärung; ferner, wie die Betroffenen ihre Rechte angemessen wahrnehmen können: Die betroffenen Patientinnen und Patienten müssen informiert werden, an wen sie sich zur Wahrnehmung ihrer Datenschutzrechte wenden können, und die ihnen genannten Adressaten müssen rechtlich und technisch in der Lage sein, die Datenschutzrechte der Patienten umzusetzen.

4.7.1.4 Wie wird die Integrität und die Authentizität der in der Akte gespeicherten Daten gewährleistet?

Wenn Daten zwischen zwei Behandlern lediglich durch Datenübertragung ausgetauscht werden, kann die Vertraulichkeit sowie die Integrität und Authentizität der Daten relativ einfach durch Verschlüsselung und elektronische Signatur sichergestellt werden (derzeit noch oft mit einer auf Softwarezertifikaten basierenden Signatur, demnächst mit dem elektronischen Heilberufsausweis). Wenn einrichtungsübergreifende Krankenakten für alle Mitbehandler zentral gespeichert werden sollen, sind darüber hinausgehende datenschutzrechtliche Aspekte zu beachten:

- Wie wird sichergestellt, dass die Daten während des gesamten Zeitraums der Verarbeitung unversehrt und vollständig sind, d.h. nicht während der Speicherung auf dem zentralen Rechner (durch Programmfehler oder durch Unbefugte) verändert werden?
- Wie wird sichergestellt, dass der Urheber der Daten jederzeit eindeutig feststellbar ist?
- Wie wird sichergestellt, dass der Auslöser eines Verarbeitungsvorgangs bzw. der Verantwortliche für einen Verarbeitungsvorgang jederzeit eindeutig feststellbar ist?

4.7.1.5 Wie werden die Abrufsberechtigungen ausgestaltet?

Benutzern bzw**.** Benutzergruppen sind Rollen zuzuweisen, die mit bestimmten Berechtigungen zum Zugriff auf Datenarten und/oder auf bestimmte Programmfunktionen verbunden sind (z.B. niedergelassener Arzt, berechtigter Arzt im Krankenhaus, Administrator der federführenden Stelle, interner Datenschutzbeauftragter). Der Zugriff auf Auswertungen sollte auf bestimmte Benutzer mit bestimmten Aufgaben begrenzt werden können. Bei Bedarf (z.B. wenn die Patientendaten auch zur Qualitätssicherung/Forschung verwendet werden sollen) sollten Funktionen zur Anonymisierung bzw. Pseudonymisierung von Patientendaten zur Verfügung stehen.

Da der Zweck einer eFA die Behandlung des Patienten bezüglich einer spezifischen Diagnose bzw. eines spezifischen Behandlungskomplexes ist, kann das Zugriffskonzept grundsätzlich so ausgestaltet werden, dass **alle** beteiligten **Behandler** bei Bedarf auf **alle** darin gespeicherten Patientendaten zugreifen können, also inhaltlich differenzierte Zugriffsberechtigungen bezüglich der medizinischen Details technisch nicht eingerichtet werden. Je umfangreicher der Kreis der beteiligten Stellen bzw. Rollen und die in der eFA gespeicherten Datensätze sind, desto eher wird jedoch ein differenziertes Zugriffskonzept gefordert werden müssen (z.B. wenn detaillierte psychiatrische Behandlungsdaten gespeichert werden). Werden zu einem Patienten gleichzeitig mehrere eFA angelegt, so dürfen nur die jeweils für die konkrete Fallakte Berechtigten auf **diese** Fallakte zugreifen.

4.7.1.6 Wie sind Patienteninformation und Patienteneinwilligung ausgestaltet?

Da die bei jeder beteiligten Stelle im Primärsystem gespeicherten Patientendaten der ärztlichen Schweigepflicht i.S.v. § 203 StGB und der Ärztlichen Berufsordnung unterliegen, bedarf die Einrichtung einer eFA mit Abrufmöglichkeit für alle beteiligten Behandler der Einwilligung des Patienten, die zugleich auch die Funktion einer Entbindung des jeweiligen Behandlers von der ärztlichen Schweigepflicht zum Zwecke der Einrichtung und Führung der eFA erfüllt. Die Einwilligung muss schriftlich erteilt werden. Vor der Einwilligung muss der Patient darüber informiert werden, welcher Behandler federführende Stelle ist, welche Daten durch wen in die Fallakte eingestellt werden sollen und wer unter welchen Voraussetzungen Zugriff auf die Fallakte haben soll (sog. informierte Einwilligung, vgl. § 7 Abs. 2 HDSG). Auf die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung muss hingewiesen werden. Eine pauschale Einwilligung in die künftige Übermittlung von bisher nicht bekannten Behandlungsdaten an eine unbestimmte Vielzahl von Behandlungseinrichtungen könnte nicht als informierte Einwilligung qualifiziert werden und wäre daher nicht rechtswirksam.

Wenn die Einwilligung zurückgenommen wird, muss die Fallakte sofort gesperrt werden. Die Behandlungsdaten und die Protokolldaten müssen gelöscht werden, sobald dies möglich ist. Hier gibt es noch offene Fragen.

Für die integrierte Versorgung i.S.v. §§ 140 ff. SGB V ist in § 140a Abs. 2 ausdrücklich festgelegt, dass die Teilnahme der Versicherten freiwillig ist. Ferner ist in § 140a Abs. 2 SGB V festgelegt, dass ein behandelnder Leistungserbringer aus der gemeinsamen Dokumentation Daten nur abrufen darf, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat und die Information für den konkret anstehenden Behandlungsfall genutzt werden soll.

Sofern die Einwilligung zwar alle beteiligten Behandler inhaltlich einbezieht, die Einwilligung aber einmal zu Beginn erteilt wird und nicht direkt gegenüber jedem Behandler, müssen alle beteiligten Behandler technisch auf die Einwilligung selbst als Bestandteil der eFA zugreifen können. Wenn sie lediglich auf die Angabe zugreifen können, wann und wo die Einwilligung erteilt wurde und wo sie als Papierdokument abgelegt ist, wird im Regelfall der Umfang der Einwilligung nicht für den Behandler klar sein.

4.7.1.7 Wie werden die Betroffenenrechte gewährleistet?

Die Patienten können sich bezüglich ihrer Rechte auf Auskunft, Einsicht, Berichtigung, Sperrung oder Löschung **von Daten in der eFA** an jede beteiligte Behandlungseinrichtung wenden. Soweit erforderlich leitet diese das Anliegen an die zuständige Stelle weiter. Zur Unterstützung der für die eFA verantwortlichen federführenden Stelle sollte das technische Verfahren geeignete Funktionen bieten, um die Rechte des Patienten auf Auskunft bzw. Einsicht zeitnah zu gewährleisten. Es sollte eine Übersichtsfunktion über die zu einem Patienten in der eFA vorliegenden Daten und Dokumente vorhanden sein, aus der auch hervorgeht, welche der beteiligten Stellen die Daten bzw. Dokumente eingegeben hat und bei welcher Stelle sie gespeichert werden. Diese Übersicht sollte in einer für den Patienten verständlichen Form ausgedruckt werden können.

Die Nutzung der Auskunftsfunktion sollte revisionssicher protokolliert werden, damit die Zulässigkeit der Nutzung überprüfbar ist.

4.7.1.8 Technisch-organisatorische Datensicherheitsmaßnahmen

Die **technisch-organisatorischen Datensicherheitsmaßnahmen** zur Sicherstellung von Integrität, Authentizität, Verfügbarkeit, Vertraulichkeit und Revisionsfähigkeit müssen zwischen den beteiligten Behandlungseinrichtungen in einem Datensicherheitskonzept vereinbart werden einschließlich der Festlegung, für welche Aspekte die federführende Stelle und für welche Aspekte welche anderen beteiligten Einrichtungen verantwortlich sind.

Im Datensicherheitskonzept ist insbesondere auch darzulegen, wie die differenzierten Zugriffsberechtigungen technisch umgesetzt werden sollen. Die Modalitäten einer Berichtigung, Sperrung und Löschung von Daten müssen geklärt werden. Eine Software zur Realisierung der gemeinsamen eFA sollte über eine komfortable Löschfunktion verfügen. Diese sollte in geeigneter Form die Löschung aller Daten eines Patienten auf Anforderung ebenso wie die Löschung von Patientendaten nach Fristablauf unterstützen.

Das Datensicherheitskonzept muss erläutern wie die Verfügbarkeit der Daten sichergestellt wird. Die Daten müssen während des gesamten Zeitraums der Verarbeitung zeitnah zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.
Der Sicherstellung der Vertraulichkeit der Daten während aller Phasen der Datenverarbeitung kommt zentrale Bedeutung zu. Auch hierzu sind Festlegungen im Datensicherheitskonzept zu dokumentieren.

Auf der Grundlage des Datenschutz- und -sicherheitskonzepts müssen die verantwortlichen Daten verarbeitenden Stellen eine Vorabkontrolle (vgl. z.B. § 7 Abs 6 HDSG) durchführen, d.h. sie müssen bewerten, ob mit dem Einsatz der einrichtungsübergreifenden eFA unter Berücksichtigung der vorgesehenen technischen und organisatorischen Maßnahmen Gefahren für die Rechte der Betroffenen verbunden sind. Nur wenn keine Gefahren vorhanden sind und höchstens ein tolerierbares Restrisiko verbleibt, darf das Verfahren eingeführt werden.

4.7.1.9 Wie wird nachvollzogen, wer welche Daten wann zur Verfügung gestellt, weiterverarbeitet und/oder abgerufen hat (Revisionsfähigkeit)?

Die Verarbeitungsprozesse müssen lückenlos nachvollzogen werden können und es muss feststellbar sein, wer wann welche Patientendaten auf welche Weise verarbeitet hat. Es muss gewährleistet werden, dass der Sender einer personenbezogenen Patienteninformation sicher sein kann, dass die Information ihren Empfänger erreicht hat, und er darf auch nicht abstreiten können, dass er diese Information an den Empfänger gesendet hat. Ebenfalls muss der Empfänger einer personenbezogenen Patienteninformation sicher sein können, genau diese Information von einem bestimmten Sender empfangen zu haben, und er darf nicht abstreiten können, genau diese Information von einem bestimmten Sender empfangen zu haben. Die erfolgten Speicherungen, Veränderungen, Nutzungen, Übermittlungen, Sperrungen und Löschungen der personenbezogenen Patientendaten müssen transparent und nachvollziehbar sein.

Aus den protokollierten Daten sollten sich zumindest die folgenden Fragen beantworten lassen [s. auch Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder, Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme, www.datenschutz.hessen.de/tf007,htm)]:

- Wer hat wann mit welchen Mitteln auf welche Daten zugegriffen?
- Wer hat wann welche Änderungen am Zustand des IT-Systems herbeigeführt, dabei besonders: Wer hatte von wann bis wann welche Zugriffsrechte und durch wem wurden sie vergeben?

Folgende Angaben sollten vollständig oder zumindest stichprobenartig protokolliert werden:

1. Protokollierung der Systemadministration:
   Einstellung und Veränderung von Systemparametern
   Ändern der Systemkonfiguration
   Einrichten, Löschen und Sperren von Benutzern
   Verwaltung von Zugriffsrechten
   Einspielen und Ändern von Software
   Durchführung von Datensicherungen
   Zurücksetzen von Passwörtern

2. Protokollierung der Verarbeitung und Nutzung von Patientendaten:
   Alle Eingaben von Patientendaten (Ersteingabe und Änderungen, mit Volltext)
   Alle Übermittlungen von Patientendaten (hier insbesondere an bzw. von allen beteiligten Stellen der IV)
   Lesende Zugriffe auf Patientendaten (Abfragen, Auswertungen) stichprobenhaft oder bestimmte besonders sensitive Daten (ohne Volltext)
   Löschung von Patientendaten

3. Protokollierung von auffälligen Vorgängen:
   Anmeldeversuche mit ungültigen oder abgelaufenen Benutzerkennungen
   evtl. alle Anmeldeversuche (bei eFA jedenfalls kein Problem der Arbeitnehmerkontrolle)
   Wiederholte Anmeldeversuche mit ungültigen Passwörtern
   Anmeldungen zu unüblichen Zeiten
   Anmeldungen unter Systemadministratorkennungen
   Verstöße gegen Zugriffsregelungen
   Zurückgewiesene Programm- und Funktionsaufrufe

Jeder aufgezeichnete Vorgang sollte mit Art des Zugriffs, Datum und Uhrzeit, ausführende Person, Datensatz und Programm(-funktion) festgehalten werden. Wegen der großen Menge an protokollierten Daten sind zusätzlich geeignete Auswertungstools zur Verfügung zu stellen, die das gezielte und effiziente Durchsuchen der Daten nach bestimmten Ereignissen, Benutzern, Zeiträumen oder anderen sicherheitsrelevanten Fragestellungen ermöglichen.

Die Protokolldaten sind gegen unbefugte Änderungen/Löschungen durch den Administrator zu schützen, z.B. durch ein Vier-Augen-Prinzip. Entsprechendes gilt für die Abschaltung der Protokollierung oder andere sicherheitskritische Funktionen.

Die Verarbeitungsprozesse müssen lückenlos nachvollzogen werden können. Aus den Protokolldaten muss erkennbar sein, wer von wann bis wann welche Zugriffsrechte hatte, wer wann mit welchen Mitteln auf welche Daten zugegriffen hat und wer wann welche Änderungen am Zustand des IT-Systems herbeigeführt hat.

4.7.2 Ein Netzwerk für Ärzte und Krankenhäuser

In Osthessen wurde in den letzten Jahren ein Kommunikationsnetz im Gesundheitsbereich aufgebaut, das hinsichtlich der Vertraulichkeit der übertragenen Daten erhebliche Vorteile gegenüber dem Telefax und der üblichen E-Mail aufweist.

4.7.2.1 Ein Kommunikationsnetz für Ärzte und Krankenhäuser

Im Jahr 2003 bat mich die KV Hessen um eine Stellungnahme zu einem Kommunikationsnetz, mit dem Ärzte und Krankenhäuser Patientendaten elektronisch übertragen wollten. Trotz aller Fragen, die sich an die Rechtsverbindlichkeit der übermittelten Daten und Dokumente knüpften und knüpfen, wurde eine Reihe von Sicherheitsvorkehrungen getroffen, um einen akzeptablen Stand bei der Datensicherheit zu erreichen. Das System wurde über die Jahre weiterentwickelt und wird von den Ärzten mittlerweile auch zur Übertragung von Daten an die KV genutzt.

4.7.2.2 Das Konzept und seine Umsetzung

Das Verfahren dient ausschließlich der Übertragung von Daten zwischen zwei Kommunikationspartnern, die Teilnehmer in diesem "privaten" Netzwerk sind. Es setzt auf eine PKI (Public-Key-Infrastructure) auf. Da der Heilberufeausweis (HBA) noch nicht zur Verfügung steht, wurde eine softwarebasierte PKI aufgebaut. Die Generierung der Schlüsselpaare geschieht bei der Installation der Software auf den Rechnern in den Arztpraxen resp. den Krankenhäusern, sodass die geheimen Schlüssel die Stellen nicht verlassen. Sie werden besonders gesichert auf den Clientrechnern gespeichert. Die Verzeichnisse mit den Namen der Teilnehmenden und den zugehörigen öffentlichen Schlüsseln werden durch den Dienstleister gespeichert und stehen nur den Teilnehmenden zur Verfügung.

Die Daten werden vor der Übertragung signiert und dann verschlüsselt. Da die Signatur mit einem Softwareschlüssel gemacht wird, erfüllt sie weder die Anforderungen einer qualifizierten noch einer fortgeschrittenen Signatur. Sollte ein Arzt aber einen HBA oder eine Signaturkarte besitzen, kann er auch damit die Daten signieren. Die Verschlüsselung erfolgt mit dem öffentlichen Schlüssel des Empfängers, sodass nur er die Daten entschlüsseln und lesen kann.

In der ursprünglichen Konzeption und Umsetzung wurden die Daten nur bei der Übertragung zum und vom Server verschlüsselt. Es gab deshalb als wesentliche Schwachstelle die unverschlüsselte Speicherung der Daten auf dem Kommunikationsserver beim Dienstleister. Dieser hätte sie also zur Kenntnis nehmen können. Der Schwachpunkt wurde schnell beseitigt.

Es gibt zwei Unterschiede zu einigen anderen Konzepten aus der letzten Zeit, auf die ich hinweisen möchte:

- Sobald eine Nachricht auf dem Kommunikationsserver eingeht, wird sie mit Zeitstempel qualifiziert signiert.
  Für diese Funktion gibt es eine Schnittstelle zu einem Dienstanbieter, der die qualifizierte Signatur vornimmt. Der Empfänger kann somit prüfen, dass die Nachricht auf dem Server und bei der anschließenden Übertragung nicht mehr geändert wurde.
- Es werden nicht nur die Nachricht selbst oder eine Anlage verschlüsselt, sondern auch der Betreff. Anhand der auf dem Kommunikationsserver gespeicherten Daten kann nur noch auf den Sender und den Empfänger geschlossen werden. Es gibt keinen Anhaltspunkt auf den Patienten, zu dem Informationen ausgetauscht werden.

Als weitere Anforderung bleibt sicherzustellen, dass nur berechtigte Stellen und Personen miteinander kommunizieren können. Dies wird durch einen zweistufigen Ansatz erreicht. In einer ersten Stufe werden der Client-Rechner und der Server dahingehend geprüft, ob es sich um für das "private" Netz zugelassene Geräte handelt. Dies geschieht durch entsprechende Einstellungen auf den Routern und ergänzende Prüfungen. Danach muss sich der Teilnehmer auf dem Server mit seiner Benutzerkennung und Passwort anmelden.
Die Absicherung des eigenen Netzes bleibt in der Verantwortung des jeweiligen Teilnehmers.

4.7.2.3 Fazit

Das Kommunikationsnetz ist derzeit auf einem Stand, der die unbefugte Kenntnisnahme der übertragenen Daten weitgehend ausschließt. Es sind auch Maßnahmen ergriffen, die für den Empfänger Rückschlüsse auf den Absender zulassen und die Inhalte vor Veränderungen während der Übertragung schützen. Es muss allerdings spätestens dann konzeptionell und in der Umsetzung überarbeitet werden, wenn die Telematikinfrastrukur, die im Zuge der elektronischen Gesundheitskarte eingeführt wird, zur Verfügung steht.

4.7.3 Datenschutzkonzept für das europäische IPF-Register

Im Berichtszeitraum wurde an der Universität Gießen mit dem Aufbau des europäischen IPF-Registers begonnen. Das Projekt wurde von meiner Dienststelle hinsichtlich des Datenschutzkonzepts für die Daten und Proben der Patientinnen und Patienten sowie der Gestaltung der Patienteninformation und Patienteneinwilligung beratend begleitet.

4.7.3.1 Zweck und organisatorischer Rahmen des IPF-Netzwerks und des IPF-Registers

Seit dem 1. Januar 2008 fördert die Europäische Kommission den Aufbau des europäischen IPF-(Idiopathische Pulmonale Fibrose-)Netzwerks (eurIPFnet). Bei der idiopathischen Lungenfibrose kommt es zu einem fortschreitenden Funktionsverlust der Lunge. Die Ursachen der Erkrankung sind bislang weitgehend unbekannt. Mit dem Forschungsverbund sollen Ursachen, Verlauf und neue Behandlungsmöglichkeiten der Krankheit erforscht werden (www.pulmonary-fibrosis.net). An dem Netzwerk nehmen derzeit zehn universitäre und ein industrieller Partner in fünf europäischen Staaten teil. Im Grant Agreement mit der EU und im Konsortialvertrag sind u.a. grundsätzliche Aspekte zur Struktur, Organisation, Haftung und zum Datenschutz geregelt. Organisatorisch wird das Netzwerk geleitet von einem Koordinator, der in Zusammenarbeit mit dem Steering Committee wesentliche Aspekte der Umsetzung des Konzepts regelt. Grundlegende Entscheidungen werden von der Generalversammlung getroffen. Ein Ethikkomitee begleitet beratend das Forschungsvorhaben.

Ein zentraler Bestandteil des Netzwerks ist das europäische Register der IPF (eurIPFreg). Auf der Grundlage von Einwilligungen der Patientinnen und Patienten sollen in dem Register Angaben zum Beschwerdebild und klinische Daten sowie den Betroffenen entnommene Biomaterialien zentral gespeichert und analysiert werden.

4.7.3.2 Ausgangspunkt der datenschutzrechtlichen Beratung

In dem Grant Agreement mit der EU sind einige aus Datenschutzsicht wesentliche Punkte bereits verbindlich festgelegt:

- Die Patientendaten sollen in dem IPFRegister pseudonymisiert gespeichert werden.
- Die Speicherung von Patientendaten und die Sammlung und Verwendung von Biomaterial bedarf der schriftlichen Einwilligung der Patientinnen und Patienten.
- Die Einhaltung der Bestimmungen der EU-Datenschutzrichtlinie muss durch die zuständigen Gremien sichergestellt werden.
- Das zu erstellende Datenschutzkonzept bedarf der Zustimmung des Ethikkomitees und des Hessischen Datenschutzbeauftragten.

Nicht geregelt sind in dem Grant Agreement und den vertraglichen Vereinbarungen die Details des Pseudonymisierungsverfahrens (Verfahren der Pseudonymbildung, Stelle, die die personenbezogene Patientenliste führt, etc.), die technisch-organisatorischen Datensicherheitsmaßnahmen sowie der Text von Patienteninformation und -einwilligung.

4.7.3.3 Das Datenschutzkonzept für das IPF-Register

In mehreren Besprechungen mit dem Koordinator des Netzwerks und weiteren Projektbeteiligten wurde ein Konsens über die Details des Datenschutzkonzepts erzielt. Das Datenschutzkonzept orientiert sich in wesentlichen Punkten an den mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmten Datenschutzmodellen der Telematikplattform für Medizinische Forschungsnetze e. V. (TMF e.V., www.tmf-ev.de; Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin, Medizinische Wissenschaftliche Verlagsgesellschaft 2006; Wellbrock, Generische Datenschutzmodelle für Biomaterialbanken, DuD 31/2007, S. 17 ff.). Ein zentraler Punkt der Modelle ist die verteilte Speicherung und Ver-

arbeitung von Informationen (sog. informationelle Gewaltenteilung); damit ist nicht lediglich eine rein technisch verteilte Speicherung und Verarbeitung gemeint, die den Datenschutz nicht wesentlich verstärken würde, sondern auch eine damit einhergehende **rechtlich klar differenzierte Verteilung von Verantwortlichkeit** auf verschiedene Personen und Stellen, die voneinander unabhängig sind. Ein zentraler Punkt ist dabei die Trennung von Identitätsdaten (Name, Geburtsdatum, Adresse etc.) von den medizinischen Daten (Diagnosen, Befunde, Probenanalysedaten etc.). Die Patientendaten werden durch die **Universität Gießen pseudonymisiert** gespeichert. Die Identitätsdaten der Patienten mit den zugeordneten Pseudonymen werden in der IT-Abteilung der **Universität München verschlüsselt** gespeichert. Die den Patientinnen und Patienten (mit Einwilligung) entnommenen Biomaterialien werden ebenfalls in pseudonymisierter Form (d.h. mit Proben-ID) zentral in der Universität Gießen aufbewahrt.

Die Rechte und Pflichten der (mit Einwilligung der Betroffenen) zugriffsberechtigten behandelnden Ärztinnen und Ärzte werden in einer schriftlichen Vereinbarung zwischen dem jeweiligen Arzt bzw. der Ärztin und der Universität Gießen geregelt. Forschende können aufgrund eines Antrags an das eurIPFnet die zu ihrem spezifischen Forschungsvorhaben erforderlichen Daten als Datenextrakt und/oder Biomaterialien erhalten. Voraussetzung hierfür ist die Freigabe durch das Leitungsgremium des eurIPFnet nach Beratung durch das Ethikgremium, insbesondere ist ein Reidentifizierungsrisiko für die betroffenen Patientinnen und Patienten auszuschließen. Der Datenextrakt wird ausschließlich **pseudonymisierte** medizinische Daten enthalten, keine Identitätsdaten. Forschende dürfen die Daten und Biomaterialien nur entsprechend der erteilten Genehmigung analysieren, eine vollständige oder teilweise Weitergabe an Dritte ist untersagt. Die Rechte und Pflichten der Forschenden werden diesen mit der Genehmigung zum Datenextrakt mitgeteilt.

Für den Fall eines evtl. für die Behandlung eines Patienten oder einer Patientin relevanten Forschungsergebnisses wird im eurIPFnet ein Verfahren für deren Information über Forschungsergebnisse etabliert.

Wie schon geschildert, sind die Verantwortlichkeiten für die Verarbeitung der Identitätsdaten (IDAT) und der medizinischen Daten (MDAT) klar getrennt. Sie werden jeweils auf dedizierten Rechnern in unterschiedlichen Rechenzentren gespeichert. Die Datenspeicherung erfolgt verschlüsselt. Die Rechenzentren müssen die Anforderungen an die Verarbeitung medizinischer Daten erfüllen, wovon ich nach dem jetzigen Stand des Projekts ausgehe. Insbesondere sind die Netze durch Firewalls und andere Maßnahmen gegen unbefugte Zugriffe aus dem Internet geschützt. Ferner gibt es Protokolle, die es erlauben, unzulässige Datenzugriffe zu erkennen. Hinsichtlich der Sicherheitsmaßnahmen bei den Clientrechnern gibt es im Vertrag Vorgaben, deren Umsetzung von den teilnehmenden Ärztinnen und Ärzten zugesagt wird.

Vertraglich ist auch sichergestellt, dass die Systembetreuer der Rechner nur auf die Daten in ihrem Zuständigkeitsbereich entsprechend den Vorgaben des Datenschutzkonzepts zugreifen. So muss die Systemadministration der MDAT für Forschungszwecke einem Wissenschaftler bzw. einer Wissenschaftlerin die Daten in genau dem Umfang zur Verfügung stellen, wie es vom Leitungsgremium des eurIPFnet vorgegeben ist. Für die Information von Patientinnen und Patienten gibt es auch ein detailliert beschriebenes Verfahren, in dem die Systemadministration der IDAT Auswertungen machen darf. Es gibt aber keinen Fall, in dem beide gemeinsame Auswertungen machen und medizinische Daten und die Identitätsdaten zusammengeführt werden können.

Einen direkten Zugriff auf die medizinischen Daten zu einem Betroffenen erhalten nur die diesen behandelnden Ärztinnen bzw. Ärzte. Um auf die Daten zugreifen zu können, richtet der oder die Behandelnde eine Anfrage mit Name, Vorname, Geburtsort und Geburtsdatum an die Datenbank mit den IDAT. Es werden keine Auswahllisten von Betroffenen angeboten und bei Schreibfehlern werden keine Daten angezeigt. Wenn die Anfrage erfolgreich ist, wird das dort zu der Patientin bzw. zu dem Patienten gespeicherte Pseudonym (PID) zusammen mit der Arztkennung an die MDAT übertragen. Dort wird geprüft, ob die anfragende Person als Behandler bzw. Behandlerin eingetragen ist. Wenn ja, wird Zugriff auf die Daten gewährt. Die Zugriffsrechte der Nutzenden sind mit vordefinierten Benutzerrollen beschrieben.

Technisch ist sichergestellt, dass Daten nur verschlüsselt übertragen werden. Dies gilt sowohl für die Kommunikation zwischen Ärztin bzw. Arzt und IDAT, zwischen IDAT und MDAT sowie MDAT und Ärztin bzw. Arzt. Es handelt sich jeweils um eine Ende-zu-Ende-Verschlüsselung.

Um sich am System anmelden zu können, war ursprünglich eine tokenbasierte Anmeldeprozedur mit Einmalpasswörtern vorgesehen. An diesem Punkt kam es zu einer Abweichung, da das eingesetzte Programm diese Option nicht unterstützt. Derzeit erfolgt die Anmeldung mit Benutzerkennung und Passwort. Es wird jedoch versucht, schnellstmöglich die ursprünglich geplante Lösung umzusetzen.

Insgesamt sind die vorgesehenen Maßnahmen nach meiner Einschätzung geeignet, die Rechte der Patientinnen und Patienten zu wahren.

4.7.3.4 Text der Patienteninformation und Patienteneinwilligung

In den Besprechungen wurde ebenfalls Konsens erzielt über die Patienteninformation und die Patienteneinwilligungen. Zentrales Anliegen aus Datenschutzsicht war es dabei, dass für die Patientinnen und Patienten transparent ist, welches Ziel mit dem Register verfolgt wird, welche Stellen beteiligt sind und für welche Aspekte des Projekts sie jeweils verantwortlich sind, wer unter welchen Voraussetzungen personenbezogene bzw. pseudonymisierte Daten und/oder Proben erhält und welche Rechte die Patientinnen und Patienten haben. Es ist vorgesehen, dass in allen beteiligten Ländern derselbe (jeweils übersetzte) Text verwendet wird.

4.7.4 Prüfung der Datenübermittlungen zwischen Kliniken und Medizinischen Versorgungszentren

Bei der Kommunikation zwischen einer Klinik und einem Medizinischen Versorgungszentrum muss beachtet werden, dass es sich um zwei zu unterscheidende Daten verarbeitende Stellen handelt, die Übermittlung von personenbezogenen Patientendaten auf die jeweils erforderlichen Daten zu beschränken ist und die Einwilligung der Patientinnen und Patienten vorliegen muss. Stichprobenhafte Überprüfungen haben ergeben, dass diese Vorgaben nicht immer eingehalten werden.

4.7.4.1 Anlass der Prüfungen

Im Gesundheitsbereich gewinnt die strukturierte, interdisziplinäre Zusammenarbeit von Vertragsärztinnen und -ärzten untereinander sowie von Vertragsärztinnen und -ärzten und Angehörigen anderer Heilberufe sowie weiterer Versorgungseinrichtungen zunehmend an Bedeutung. Seit dem Inkrafttreten des Gesundheitsmodernisierungsgesetzes (GMG) am 1. Januar 2004 ist die Gründung eines Medizinischen Versorgungszentrums (MVZ) als eine neue fachübergreifende Versorgungsform möglich. Derartige Zentren sind fachübergreifende ärztlich geleitete Einrichtungen, in denen Ärztinnen und Ärzte als Angestellte oder als Vertragsärztinnen und -ärzte tätig sind. Der Behandlungsvertrag wird zwischen Patientin und Patient (bzw. Krankenkasse) und dem MVZ geschlossen, nicht zwischen Patient und einzelnem im MVZ tätigen Arzt oder Ärztin. Die Vorschriften des SGB V finden entsprechende Anwendung. MVZ haben die gleichen Rechte und Pflichten wie Vertragsärzte im System der gesetzlichen Krankenversicherung. Eigentümer eines MVZ kann eine natürliche oder eine juristische Person sein, z.B. eine Vertragsärztin oder ein Vertragsarzt, eine Apothekerin oder ein Apotheker, eine Klinik oder eine Kapitalgesellschaft. Vielfältige verschiedene Ausgestaltungen und Rechtsformen der MVZ sind möglich (siehe z.B. www.kbv.de). Mitte 2008 gab es bereits ca. 1.100 MVZ bundesweit.

In vielen Fällen wird eine enge Kooperation zwischen MVZ und Klinikum angestrebt. Ziel ist es dabei u.a., dass die Patientin bzw. der Patient gemeinsam umfassend ärztlich betreut wird und sowohl MVZ wie auch Klinik die jeweils erforderlichen Behandlungsdaten rechtzeitig und vollständig zur Verfügung stehen. Dieses Ziel kann auch auf der Grundlage des geltenden Datenschutzrechts realisiert werden. Ebenso wie bei der Kommunikation zwischen Kliniken und Ärztinnen bzw. Ärzten, die als Freiberufler in eigener Praxis tätig sind, muss bei der Kommunikation zwischen Klinik und MVZ jedoch beachtet werden, dass es sich bei dem Klinikum und dem MVZ aus datenschutzrechtlicher Sicht um zwei zu unterscheidende Daten verarbeitende Stellen handelt und die Übermittlung von Patientendaten auf die jeweils erforderlichen Daten beschränkt sein muss und der Einwilligung der Patientinnen und Patienten bedarf.

Zur Klärung der gegenwärtigen Praxis habe ich stichprobenhaft die Kommunikation zwischen MVZ und Krankenhaus geprüft. Da ein MVZ in öffentlich-rechtlicher Rechtsform (d.h. Zuständigkeit des Hessischen Datenschutzbeauftragten) oder auch in privatrechtlicher Rechtsform (d.h. Zuständigkeit des RP Darmstadt, Dezernat Datenschutz) betrieben werden kann, habe ich meine Tätigkeit und die wesentlichen datenschutzrechtlichen Forderungen mit dem RP Darmstadt, Dezernat Datenschutz koordiniert.

4.7.4.2 Prüfungsergebnisse

4.7.4.2.1 Übermittlungsumfang und Rechtsgrundlage

Meine stichprobenhaften Feststellungen ergaben:
Teilweise wird zwischen MVZ und Klinik klar unterschieden. Die Übermittlung von Patientendaten erfolgt im Einzelfall im jeweils erforderlichen Umfang, soweit dies für die Mitbehandlung der anderen Stelle erforderlich ist.

Teilweise waren die Strukturen nicht klar:

- Es erfolgte eine pauschale Übermittlung der Daten von Patientinnen und Patienten des MVZ an das Klinikum, d.h. auch von Personen, die nicht im Klinikum mitbehandelt wurden.

- Umgekehrt bestand die Möglichkeit der Kenntnisnahme der Daten von Patientinnen und Patienten des Klinikums, ohne dass diese (auch) im MVZ behandelt wurden. Im Krankenhausinformationssystem wurden die Ärztinnen bzw. Ärzte des MVZ teilweise als Angehörige des Klinikums, Fachbereich MVZ qualifiziert.

Soweit Daten übermittelt wurden, die zur Mitbehandlung durch die andere Stelle nicht erforderlich waren, war teilweise zuvor eine Einwilligung der Patientin bzw. des Patienten eingeholt worden. Der Wortlaut dieser Einwilligungserklärung bezog sich jedoch auf die Behandlungsdaten, die zur weiteren Mitbehandlung erforderlich sind, und konnte daher keine Rechtsgrundlage sein für die Übermittlung der Daten von Personen, die gar nicht Patientinnen bzw. Patienten der anderen Stelle waren.

Grundsätzlich ist hinsichtlich der Patienteneinwilligung in eine Datenübermittlung noch auf Folgendes hinzuweisen:
Eine **schriftliche** Einwilligung ist für die Übersendung eines Befundes an den Mitbehandler in der Regel nicht zwingend erforderlich. Allerdings kann es von Vorteil für alle Beteiligten sein, wenn die vorgesehenen Datenübermittlungen auf diese Weise klar vereinbart sind. Unabhängig davon kann sich eine Einwilligung stets nur auf den aktuellen Behandlungsfall beziehen, nicht auf sämtliche künftigen Behandlungsfälle im MVZ bzw. in der Klinik. Gemäß § 12 HKHG i.V.m. § 7 Abs. 2 HDSG ist eine **informierte Einwilligung** einzuholen: der oder die Betroffene ist vor der Einwilligung über die Bedeutung der Einwilligung, insbesondere auch über den Verwendungszweck der Daten, aufzuklären. Eine pauschale Einwilligung in Datenübermittlungen in allen künftigen Behandlungsfällen erfüllt diese Voraussetzungen nicht.

4.7.4.3 Technischer Ablauf der Datenübermittlungen

Gegenstand der Prüfung war auch der technische Ablauf der Datenübermittlungen: Erfolgt die Übermittlung der Patientendaten per Post, per E-Mail, per Fax oder durch Abruf?

Nach meinen Feststellungen kann zwischen zwei Konstellationen unterschieden werden. Entweder agierte das MVZ autonom wie eine übliche Arztpraxis, oder es kooperierte so eng mit einer Klinik, dass aus dem MVZ auf das Kliniknetz zugegriffen werden konnte.

Im ersten Fall gibt es die üblichen Wege der Übermittlung von Patientendaten. Der Versand per Post ist die Regel, die Übermittlung per Fax erfolgt, wenn es schnell gehen soll, die Kommunikation per E-Mail ist die Ausnahme. Mit den verschiedenen Versandformen verbundene Datensicherheitsprobleme habe ich bei meinen Prüfungen nicht vertieft, da sie nicht spezifisch für ein MVZ waren (zur Kommunikation per Fax s. 20. Tätigkeitsbericht, Ziff. 9.1, zur Kommunikation per E-Mail s. 28. Tätigkeitsbericht, Ziff. 10.1).

Hinsichtlich der Zugriffsmöglichkeiten aus dem MVZ in ein Kliniknetz stellte sich die Situation so dar, dass man sich über eine gesicherte Verbindung vom Arbeitsplatz im MVZ aus, wie von einem klinikinternen Arbeitsplatz, im Klinikinformationssystem (KIS) anmelden konnte. Die vergebene Benutzerkennung war im KIS mit den gewünschten Zugriffsrechten eingerichtet. In diesem Zusammenhang konnten auch Daten vom KIS in die Verwaltungssoftware des MVZ übernommen werden.

Außerdem wurden standardmäßig von der Verwaltungssoftware des MVZ die Stammdaten neuer Patientinnen und Patienten an die Klinik übertragen und dort in das KIS übernommen. Dort wurden sie dann wie Daten neuer Klinikpatientinnen und -patienten behandelt. Die Datenübertragung war technisch ausreichend gegen Zugriffe Dritter abgesichert. Hinsichtlich der eingeräumten Zugriffsrechte ergaben sich aber die oben geschilderten Probleme.

Außer den Datenübermittlungen gab es noch die Zugriffe auf Daten im Zusammenhang mit Fernwartungen. Die Fernwartungen waren nicht in allen Fällen nachvollziehbar. Hierbei handelte es sich ebenfalls um keine MVZ-Problematik, sondern um ein generelles Problem, das seit vielen Jahren den Datenschutz beschäftigt.

"Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (Deutsches Ärzteblatt, A 1026, Heft 19. Mai 2008; www.bundesaerztekammer.de)

10 Fernwartung

Beim Einsatz der Fernwartung müssen grundlegende Sicherheitsvorkehrungen getroffen werden, um der Datensicherheit Genüge zu tun. Bei der Einwahl in die Fernwartungsaktivitäten muss eine Autorisierung mittels einem aktuell gültigen Passwort erfolgen. Grundsätzlich gilt, dass der Techniker ohne ein gültiges Passwort nicht auf den Praxisrechner zugreifen kann. Nach Beendigung einer Fernwartungssitzung sollte daher eine Änderung des Passwortes erfolgen, somit kann zu einem späteren Zeitpunkt der Techniker nicht ohne Autorisierung auf das System zugreifen.

Die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers dürfen nur verschlüsselt über eine geschützte Verbindung (s. Kapitel 3.3.2) übermittelt werden. Im Rahmen der Fernwartung sollte darauf geachtet werden, dass die Fernwartung ausdrücklich von der Arztpraxis freigegeben wird. Die Zugriffsrechte des Technikers müssen auf ein Minimum beschränkt werden.

In begründeten Notfällen (z.B. Systemstillstand) kann eine Wartung auf Basis der Echtdaten erfolgen. Grundsätzlich sollten jedoch Testdaten (Testpatienten) dem Fernwartungspersonal zur Verfügung gestellt werden.

Die Fernwartung muss protokolliert werden und vor Ort am Bildschirm durch den Praxisinhaber oder autorisiertes Personal überwacht werden. Weiterhin wird empfohlen, dass der Arzt oder das Praxispersonal Mindestkenntnisse über die Praxis-EDV erwerben, um die Arbeit des Wartungstechnikers qualifiziert begleiten zu können. Anhand des Protokolls sollte jederzeit nachvollzogen werden, welche Veränderungen vorgenommen und auf welche Dateien zugegriffen wurde.

4.7.4.4 Zugriffsausgestaltung innerhalb eines MVZ

Diskutiert wurde bei den Prüfungen auch die Frage, ob **innerhalb eines MVZ** hinsichtlich der Zugriffsberechtigungen der einzelnen Ärztinnen bzw. Ärzte differenziert wird. Nach meinen bisherigen Feststellungen werden in MVZ nur teilweise verschiedene Rollen wie z.B. Administrator, Arzt, Arztgehilfin etc. unterschieden, und Differenzierungen hinsichtlich des Zugriffs durch die Ärztinnen bzw. Ärzte werden vielfach nicht getroffen.

Die verschiedenen Rollen und die damit verbundenen differenzierten Berechtigungen müssen auf jeden Fall eingerichtet werden. Was Differenzierungen hinsichtlich des Zugriffs durch die Ärztinnen bzw. Ärzte anbelangt, so ist zumindest in den Fällen, in denen diese sich nicht wechselseitig vertreten, kein Grund dafür ersichtlich, dass **jeder von ihnen** auf die Daten **aller** Patientinnen und Patienten zugreifen kann. Je höher die Anzahl der Ärztinnen bzw. Ärzte und Fachrichtungen in einem MVZ ist, desto wichtiger wird die Frage nach einer Zugriffsdifferenzierung, d.h. nach einer internen technischen Beschränkung der Zugriffsmöglichkeiten auf die Patientendaten auf den jeweiligen behandelnden Arzt bzw. die Ärztin und die evtl. Vertretung. Dies gilt umso mehr, als nach Information der MVZ rechtlich vorgegeben ist, dass höchstens 30 v.H. der Patientinnen und Patienten fachfremd und höchstens 20 v.H. fachintern von mehr als einer Ärztin oder einem Arzt eines MVZ behandelt werden dürfen.

Teilweise wird von den Patientinnen oder Patienten vor Beginn der Behandlung in einem MVZ eine Einwilligung eingeholt in die Möglichkeit der Kenntnisnahme ihrer Daten durch **alle** Ärztinnen bzw. Ärzte in dem MVZ; teilweise wird dann auch die Behandlung außer in Notfällen dann abgelehnt, wenn die Patientin oder der Patient die Einwilligungserklärung nicht unterschreibt. Offensichtlich wird hier zumindest erkannt, dass ein Zugriff durch alle Ärztinnen bzw. Ärzte keineswegs selbstverständlich ist. Das Einholen einer Einwilligung in nicht erforderliche Zugriffsmöglichkeiten ist jedoch eine rechtlich problematische und nicht im Interesse der Patientinnen und Patienten liegende Verfahrensweise.

Auch die aktualisierten "Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung" der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (Deutsches Ärzteblatt, A 1026, Heft 19. Mai 2008; www.bundesaerztekammer.de) sehen in der Technischen Anlage zu diesem Thema Folgendes vor:

Deutsches Ärzteblatt, A 1026, Heft 19. Mai 2008

2.4 Mindestmaß der Datenzugriffsmöglichkeiten

Betreffend der Datenzugriffsrechte sollte darauf geachtet werden, dass jeder Benutzer des Computersystems (einschließlich Administrator) ausschließlich Zugriffe bzw. Ausführrechte auf die seinem Tätigkeitsfeld entsprechenden Datenbestände und Programme hat. Insbesondere Programme, welche Verwendung bei der Systemadministration finden, sollten auf die jeweiligen Mitarbeiter beschränkt sein, welche diese für ihre Arbeit benötigen. Die vergebenen Zugriffsrechte sollten in regelmäßigen Abständen auf Aktualität bezüglich der jeweiligen Tätigkeitsfelder überprüft werden.

2.5 Beschränkung der Arbeit mit Administratorrechten

… Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zu diesem Zweck sollten die berechtigten Personen über Zugriffskontrollmechanismen (z.B. Passwörter) legitimiert werden …

Diese Empfehlungen finden zwar auf MVZ nicht direkt Anwendung. Entsprechende Maßnahmen sind aber im MVZ mindestens ebenso wichtig: Von den Mitte 2008 in Deutschland bereits vorhandenen ca. 1.100 MVZ hatten zu diesem Zeitpunkt einige bis zu 70 Ärztinnen und Ärzte beschäftigt.

Bei unseren Prüfungen wurden wir teilweise darauf hingewiesen, dass nicht jede auf dem Markt erhältliche Arztpraxissoftware die differenzierte Ausgestaltung der Zugriffsrechte und die Benutzerverwaltung so unterstützt, dass die Differenzierungen im Alltag eines MVZ umgesetzt werden können, jedenfalls nicht mit vertretbarem Aufwand. In den o.a. Empfehlungen wird allerdings Folgendes ausgeführt:

Viele der heute in Arztpraxen eingesetzten Programme verfügen über eine Vielzahl hervorragender Schutzmechanismen. …

Soweit aufgrund der beschränkten Größe eines MVZ und/oder technischer Probleme eine technische Zugriffsdifferenzierung derzeit nicht in vollem Umfang realisiert werden kann bzw. muss, ist zu beachten, dass ein tatsächlicher Zugriff im Einzelfall nur zulässig ist, wenn er erforderlich ist. Es sollte auf jeden Fall ein Zugriff auf die Patientendaten im Streitfall mittels ausreichender Protokollierung nachvollziehbar sein, d.h. schreibende Zugriffe sollten immer nachvollziehbar sein, während lesende Zugriffe jenseits eines Behandlungszusammenhangs protokolliert werden müssen (s.a. Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder, Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme, www.datenschutz.hessen.de/tf007.htm). Als eine Konsequenz müssen alle Nutzenden eigene Benutzerkennungen samt persönlichem Passwort erhalten, damit Protokolleinträge den richtigen Personen zugeordnet werden können. Für evtl. Notfälle können besondere Verfahrensweisen getroffen werden. Eine wesentliche Anforderung betrifft die Dokumentation. Es muss nachträglich möglich sein festzustellen, wer wann welche Zugriffsrechte besessen hat und von wem die Zugriffsrechte vergeben sowie eingetragen wurden. Für die Kontrolle der Protokolle muss ein schriftliches Konzept (Organisationsanweisung o.Ä.) vorliegen, aus dem hervorgeht, wer in welchen Zeitabständen was kontrolliert und welche Maßnahmen bei Anhaltspunkten für einen evtl. Datenschutzverstoß von wem ergriffen werden. Alle Ärztinnen, Ärzte und weitere Beteiligte müssen über die Rechtslage, die Zugriffsprotokollierungen und Protokollauswertungen schriftlich informiert werden.

Zur weiteren Konkretisierung der künftigen Verfahrensweisen sind für das nächste Jahr gemeinsame Besprechungen mit dem RP Darmstadt und der LÄK vorgesehen.

4.7.5 Sozialmedizinische Fallberatung des MDK Hessen

Im Rahmen von Sozialmedizinischen Fallberatungen durch den Medizinischen Dienst der Krankenversicherung werden nach der Begutachtungsrichtlinie "Vorsorge und Rehabilitation" von Versicherten beantragte medizinische Rehabilitationsmaßnahmen auf ihre Notwendigkeit hin überprüft. Dabei kann der MDK den von der Krankenkasse erteilten Prüfauftrag bei Bedarf erweitern.

4.7.5.1 Die Beschwerde eines Versicherten

Ein Versicherter der Techniker Krankenkasse mit Wohnsitz in Berlin beschwerte sich darüber, dass ein von ihm bei der Krankenkasse eingereichter Antrag auf medizinische Rehabilitation nicht nur abgelehnt, sondern der Untersuchungsauftrag

vom Medizinischen Dienst der Krankenversicherung (MDK) in Hessen erweitert worden war. Der Betroffene hatte wegen gelegentlicher Schulter- und Armbeschwerden den Rehabilitationsantrag gestellt, der einen Kuraufenthalt zur Folge haben sollte. Die Geschäftsstelle des MDK Hessen in Darmstadt erhielt den Antrag von der Techniker-Kasse im Zusammenhang mit einer Sozialmedizinischen Fallberatung, bei der die Krankenkasse u.a. die Frage geklärt wissen wollte, ob die Erwerbsfähigkeit des Versicherten gefährdet sei.

In seiner Stellungnahme an den Versicherungsträger stellte der MDK fest, dass die beantragte Maßnahme medizinisch nicht notwendig, die Erwerbsfähigkeit jedoch aufgrund neuer Aspekte gefährdet sei. Der MDK erklärte, dass eine Langzeitentwöhnung von Alkohol beim Betroffenen vorgenommen werden müsse. Hiergegen verwahrte sich der Beschwerdeführer. Er sah u.a. seine Rechte auf den Schutz seiner personenbezogenen Daten beeinträchtigt, da der MDK nicht befugt sei, den Untersuchungsauftrag aus eigenen Stücken zu erweitern bzw. abzuändern.

4.7.5.2 Verfahrensablauf bei der Beantragung von medizinischer Rehabilitation

Wenn gesetzlich Versicherte erkrankt sind und zur Wiederherstellung ihrer Gesundheit einen Kuraufenthalt benötigen, müssen sie einen Kurantrag stellen. Zusammen mit dem Hausarzt muss ein Formular zur "Verordnung von medizinischer Rehabilitation" ausgefüllt werden. Unter anderem wird eine Sozialanamnese erstellt, die Rehabilitationsfähigkeit beurteilt und eine Prognose zum Heilungsverlauf gestellt. Schließlich gibt der Hausarzt eine zusammenfassende Wertung ab. Diese Unterlage wird zusammen mit ggf. vorhandenen Befunden an die Krankenkasse übermittelt. Zur Beurteilung, ob die gewünschte Maßnahme erforderlich ist, wird gem. § 275 Abs. 1 Nr. 3 Buchst. a SGB V der MDK eingeschaltet.

Im vorliegenden Fall hat die Techniker-Krankenkasse die Bearbeitung von Anträgen für Kuraufenthalte zur Wiederherstellung der Erwerbsfähigkeit für das gesamte Bundesgebiet in Darmstadt zentralisiert. Dort ist auch eine Geschäftsstelle des MDK Hessen angesiedelt, welche die Anträge unter medizinischen Gesichtspunkten prüft. Hierzu werden die vorhanden Unterlagen, die dem MDK von der Kasse zur Verfügung gestellt werden, herangezogen. In diesem Zusammenhang kommt es nicht selten vor, dass der MDK zusätzliche Unterlagen benötigt, die z.B. über die Krankenkasse bei den Versicherten angefordert werden. Gemäß § 276 Abs. 2 SGB V kann der MDK auch bei den Leistungserbringern selbst, also den behandelnden Ärztinnen bzw. Ärzten, Sozialdaten erheben, soweit dies erforderlich ist.

§ 275 Abs. 1 Nr. 3 Buchst. a SGB V

Die Krankenkassen sind in den gesetzlich bestimmten Fällen oder wenn es nach Art, Schwere, Dauer und Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, verpflichtet…bei Arbeitsunfähigkeit zur Sicherung des Behandlungserfolgs, insbesondere zur Einleitung von Maßnahmen der Leistungsträger zu Wiederherstellung der Arbeitsfähigkeit … eine gutachtliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung einzuholen.

§ 276 Abs. 2 SGB V

Der Medizinische Dienst der Krankenversicherung darf Sozialdaten nur erheben und speichern, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen … erforderlich ist. Haben die Krankenkassen … eine gutachtliche Stellungnahme oder Prüfung durch den Medizinischen Dienst veranlasst, sind die Leistungserbringer verpflichtet, Sozialdaten auf Anforderung des Medizinischen Dienstes zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist.

4.7.5.3 Verfahrensweise des MDK Hessen

In dem mir vorliegenden Fall hatte der MDK den vom Hausarzt und dem Versicherten ausgefüllten Antrag von der Krankenkasse des Versicherten übermittelt bekommen. Zunächst konnte jedoch keine sozialmedizinische Fallberatung durchgeführt werden, weil der zuständigen Gutachterin eine Entscheidung auf Basis der ihr vorliegenden Unterlagen nicht möglich war. Über die Krankenkasse forderte der MDK weitere Unterlagen vom Versicherten an, die dieser bereitstellte. Die von der Krankenkasse gestellte Frage, ob die beantragte medizinische Maßnahme notwendig sei, verneinte die Gutachterin aufgrund der Aktenlage. Allerdings teilte sie der Krankenkasse mit, dass eine Langzeitentwöhnung von Alkohol notwendig sei. Die Information über vorhandenen und übermäßigen Alkoholkonsum hatte die Gutachterin den Unterlagen entnommen, die der Versicherte auf Nachfrage der Kasse im Zusammenhang mit dem Antrag zur Verfügung gestellt hatte.

Die Krankenkasse informierte den Versicherten über die vom MDK Hessen abgegebene Empfehlung.

4.7.5.4 Rechtliche Bewertung

Die Gutachterin des MDK Hessen war befugt, den ihr gestellten Untersuchungsauftrag zu erweitern. Bei Anträgen auf Vorsorge- oder Rehabilitationsleistungen sind die Krankenkassen nach § 275 SGB V verpflichtet, zur Prüfung der medizinischen Notwendigkeit, Zweckmäßigkeit und Wirtschaftlichkeit dieser Leistungen vor Bewilligung und bei beantragter Verlängerung, den MDK mit einer gutachtlichen Stellungnahme zu beauftragen. Hierzu hat der Medizinische Dienst der Spitzenverbände der Krankenkassen eine "Begutachtungs-Richtlinie Vorsorge und Rehabilitation" erlassen. Beurteilungsgrundlagen für die gutachtliche Stellungnahme sind der Antrag des Versicherten und der ärztliche Befundbericht bzw. die ärztliche Verordnung von medizinischer Rehabilitation sowie ggf. weitere vorliegende Unterlagen.

Die Krankenkassen formulieren konkrete Fragen, zu denen der MDK aus sozialmedizinischer Sicht Stellung zu nehmen hat. Die sozialmedizinische Fallberatung (SFB) stellt das Regelbegutachtungsverfahren in den Leistungsbereichen Vorsorge und Rehabilitation dar. Das Ergebnis der SFB soll für die Krankenkasse verständlich sowie schlüssig und somit als sozialmedi-

zinische Grundlage eines Leistungsentscheides geeignet sein. In der SFB wird durch den/die Gutachter/in entschieden, ob der Antrag abschließend beurteilt werden kann und ob eine Begutachtung nach Aktenlage oder mit Befunderhebung (nach körperlicher Untersuchung) erfolgen soll. In sozialmedizinisch eindeutigen Fällen reicht eine zusammenfassende Stellungnahme zu den Vorsorge-/Rehabilitationskriterien (z.B. Ziele, Prognose, Bedürftigkeit, Fähigkeit) auf dem Antrag mit nachvollziehbarer Begründung aus. In den übrigen Fällen ist ein (Formular-)Gutachten zu erstellen, in dem die Empfehlungen zu begründen sind. Ggf. sind realistische Alternativen zur beantragten Leistung aufzuzeigen. Werden eine erhebliche Gefährdung oder Minderung des Leistungsvermögens im Erwerbsleben festgestellt, sind diese im Gutachten schlüssig darzulegen.

In dem mir zur Prüfung vorliegenden Fall hatte der Versicherte einen Kuraufenthalt u.a. zur Linderung einer psychovegetativen Erschöpfung und Behandlung eines Schulter- und Armsyndroms beantragt. Einen Kuraufenthalt zur Behandlung dieser Symptome beurteilte die Gutachterin des MDK als medizinisch nicht notwendig. Die weiteren ihr vorliegenden Unterlagen legten den Verdacht auf Alkoholismus nahe. Daraus schlussfolgerte die Gutachterin eine erhebliche Gefährdung des Leistungsvermögens im Erwerbsleben und dokumentierte dies im Rahmen der SFB gegenüber der Krankenkasse. Hierzu war eine Befugnis gegeben, weil die vom Medizinischen Dienst der Spitzenverbände (MDS) hierzu herausgegebenen Richtlinien dies ausdrücklich vorsehen. Gerade die Frage, ob eine Gefährdung der Erwerbsfähigkeit eventuell vorliegt, worin diese begründet ist und welche Maßnahmen zur Beseitigung der Gefährdung vorgeschlagen werden, sind essenzielle Aufgaben, die im Rahmen einer SFB zu beantworten sind.

4.7.6 Weiterleitung von Verdachtsdiagnosen an Dritte gegen den Willen des Betroffenen

Ergibt eine medizinische Behandlung Zufallsbefunde, die weder der die Untersuchung in Auftrag gegebene Arzt noch der die Untersuchung durchführende Arzt noch der Patient selbst erwartet haben, so muss der Arzt das Einverständnis in die Weitergabe einholen. Überdies gilt der Grundsatz, dass der Patientenwille die Behandlungsgrenze für alle den Patienten behandelnden Ärzte bildet. Der Patient kann daher entscheiden, welcher Arzt welche Information über ihn befugt erheben und weitergeben darf.

4.7.6.1 Beschwerde des Patienten

Ein Patient, der sich in die urologische Abteilung eines Frankfurter Krankenhauses begeben hatte, beklagte sich über die ärztliche Leitung. Diese habe in einem an seinen Facharzt gerichteten Arztbrief, in dem über den Behandlungsverlauf berichtet wurde, entgegen seinem Willen eine kompromittierende Diagnose beigefügt. Dabei handelte es sich um den Verdacht auf eine schizophrene Psychose. Diese Verdachtsdiagnose wurde in einem Konsiliar durch die Neurologische Abteilung der Klinik festgestellt. Der Patient war zuvor aus Sicht der Klinik verhaltensauffällig gewesen und deshalb untersucht worden. Der Patient kritisierte nun, dass diese Diagnose in einem Arztbrief an einen von ihm angegebenen Facharzt übermittelt wurde. Zuvor hatte man dem Betroffenen einen "vorläufigen Arztbrief" ausgehändigt, in dem die besagte Verdachtsdiagnose nicht enthalten war. Er sah die bei ihm durchgeführte urologische Behandlung und die in dem endgültigen Arztbrief formulierte Verdachtsdiagnose einer schizophrenen Psychose in keinerlei Zusammenhang, der dazu hätte führen müssen, den Facharzt im Rahmen der Nachbehandlung hierüber zu informieren.

4.7.6.2 Bewertung eines solchen Sachverhaltes durch die von mir eingeschaltete Landesärztekammer

Auch meinen Mitarbeitern erschloss sich die Notwendigkeit nicht, eine solche nur im Rahmen eines nicht weiter abgeklärten Verdachts dokumentierte Diagnose an einen Facharzt für Urologie weiterzuleiten, der die Nachbehandlung vornehmen sollte. Die Klinik erachtete diese Information als durchaus notwendig und für den nachbehandelnden Arzt erforderlich. Deshalb wurde die Landesärztekammer zum Sachverhalt befragt und um eine Stellungnahme gebeten.

Die Kammer stellte zunächst fest, dass die ärztliche Schweigepflicht auch unter den Ärzten gilt. Eine Nachbehandlung konnte in dem vorliegenden Fall angenommen werden, da der Patient wegen aufkommender Beschwerden die Klinik aufgesucht hatte und eine weitere (Nach-)Behandlung durch den Facharzt erfolgen sollte, den der Patient der Klinik angegeben hatte. Nach Auffassung der Kammer informierte der behandelnde Arzt im Rahmen des mit dem Patienten geschlossenen Behandlungsvertrages den danach behandelnden Arzt. Weiter führt die Kammer aus: "Ergibt die Behandlung jedoch Zufallsbefunde, die weder der die Untersuchung in Auftrag gegebene Arzt noch der die Untersuchung führende Arzt noch der Patient selbst erwartet hat, etwa eine weitere, völlig andersartige Erkrankung, so soll der Arzt beim Patienten das Einverständnis in die Weitergabe einholen." Außerdem gelte der Grundsatz, "dass der Patientenwille die Behandlungsgrenze für alle den Patienten behandelnden Ärzte bildet. Der Patient kann daher entscheiden, welcher Arzt welche Information und Daten über ihn befugt erheben und weitergeben darf." Weiterhin zog die Standesvertretung der Ärzte in Hessen in Zweifel, dass der Arztbrief an den Facharzt die beanstandete Diagnose (Verdacht auf schizophrene Psychose) enthalten durfte, obwohl der Patient dem widersprochen hatte. Aus Sicht der Kammer hätte der Arzt zunächst den Patienten um sein Einverständnis bitten müssen, bevor diese Verdachtsdiagnose übermittelt wurde. Dieses Erfordernis erschien der Kammer umso größer, als es sich bei dem nachbehandelnden Arzt um einen Urologen gehandelt hatte, "für den die Diagnose Schizophrenie wahrscheinlich nicht von essenzieller Bedeutung für die Weiterbehandlung war".

4.7.6.3 Bewertung des Hessischen Datenschutzbeauftragten

Die rechtlichen Ausführungen der Landesärztekammer zu dem von mir geschilderten Sachverhalt teile ich in vollem Umfang. Dies habe ich dem Betroffenen ebenso zur Kenntnis gegeben wie dem Datenschutzbeauftragten der Klinik.

4.8 Sozialwesen

4.8.1 Hartz IV - Bekämpfung von Leistungsmissbrauch

Bei der Bekämpfung von Leistungsmissbrauch durch den Außendienst ist der Grundsatz der Verhältnismäßigkeit zu beachten.

Ein Vizepräsident des Hessischen Landtags hat mich gebeten, die Überprüfung einer Bezieherin von Arbeitslosengeld II durch den Außendienst zur Bekämpfung von Leistungsmissbrauch (Hochtaunuskreis) datenschutzrechtlich zu bewerten. Konkret ging es bei der in Rede stehenden Exploration darum, dass über ein halbes Jahr an 89 Beobachtungstagen 58-mal ein PKW vor der Wohnung der Hilfeempfängerin registriert wurde, um persönliche Lebensumstände (eheähnliche Gemeinschaft, finanzielle Verhältnisse) der Hilfeempfängerin aufzuklären. Die sehr hohe Zahl der Beobachtungstage kam entscheidend dadurch zustande, weil der Außendienstmitarbeiter bei seinen Fahrten zwischen Wohnung und Dienststelle bzw. Dienststelle und Wohnung nur einen kurzen Umweg nehmen musste.

Gesetzlicher Hintergrund solcher Überprüfungen ist § 6 Abs. 1 Satz 2 SGB II (Grundsicherung für Arbeitsuchende), der einen Außendienst zur Bekämpfung von Leistungsmissbrauch vorsieht.

§ 6 Abs. 1 Satz 2 SGB II

Die Träger der Grundsicherung sollen einen Außendienst zur Bekämpfung von Leistungsmissbrauch errichten.

Auf der Grundlage dieser seit 2006 geltenden Regelung soll der Außendienst insbesondere überprüfen, ob die Anspruchsvoraussetzungen von Personen, die Leistungen der Grundsicherung für Arbeitsuchende beziehen oder bezogen haben, vorliegen bzw. vorlagen. Dabei soll der Außendienst Sachverhalte überprüfen, die nicht allein aufgrund der Aktenlage beurteilt werden können (näher hierzu etwa Hauck/Noftz, SGB II, § 6 Rdnr. 14a). Hierzu zählen gerade auch Fragestellungen wie eheähnliche Gemeinschaft und finanzielle Verhältnisse (vgl. etwa Oestreicher, SGB II, § 6 Anmerkung V 3). Bei der Vollziehung dieser Norm, die typischerweise einen gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung bedeutet, ist allerdings der Grundsatz der Verhältnismäßigkeit zu beachten.

Der Erste Beigeordnete und Sozialdezernent des Hochtaunuskreises hat darauf hingewiesen, die Sozialverwaltung des Hochtaunuskreises sei bestrebt, insbesondere bei langjährigen und konfliktgeneigten Sozialverwaltungsrechtsverhältnissen "wasserdichte" Entscheidungen zu treffen, die wiederum eine solide und gerichtsverwertbare Sachverhaltsaufklärung voraussetzten. Diese Position steht mit dem Verfahrensrecht der Sozialverwaltung durchaus im Einklang; danach ermittelt die Behörde den Sachverhalt von Amts wegen, und sie bestimmt Art und Umfang der Ermittlungen (§ 20 Abs. 1 SGB X). Bei der Sachverhaltsaufklärung sind jedoch, soweit es um personenbezogene Daten geht, datenschutzrechtliche Vorgaben vorrangig zu beachten (§ 37 Satz 3 SGB I, § 3 Abs. 2 HDSG), und das bedeutet insbesondere, unnötige, nicht erforderliche Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) zu unterlassen (§ 67a SGB X, § 11 HDSG).

§ 67a Abs. 1 SGB X

Das Erheben von Sozialdaten … ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist.

Offenbar war sich die Sozialverwaltung des Hochtaunuskreises der datenschutzrechtlichen Facette bei der Überprüfung der Leistungsempfängerin nur unzureichend bewusst, weil "nur ein PKW vor ihrer Wohnung" Gegenstand der monatelangen Beobachtungen war. Ein PKW ist datenschutzrechtlich aber von Relevanz, wenn dieser Beobachtungsgegenstand gerade dazu dient, persönliche Lebensumstände wie finanzielle Verhältnisse, eheähnliche Gemeinschaft etc. aufzuklären und zu belegen. Deshalb ist die besagte Exploration über ein halbes Jahr, um an 89 Beobachtungstagen 58-mal den PKW vor der Wohnung zu registrieren, datenschutzrechtlich bewertet eine überdosierte Datenerhebung gewesen. Damit steht zugleich ein Verstoß gegen die Verhältnismäßigkeit fest. Eigentlich sich selbst relativierend hat der Sozialdezernent des Hochtaunuskreises auch eingeräumt, die Überprüfung wäre sicher früher beendet worden, wenn sie sich aufwändiger gestaltet hätte; konkret: wenn der Außendienstmitarbeiter bei seinen Fahrten zwischen Wohnung und Dienststelle bzw. Dienststelle und Wohnung einen größeren Umweg hätte fahren müssen. Mit anderen Worten: Die Überprüfung war in ihrem Ausmaß nicht wirklich nötig.

Ich gehe davon aus, dass die Sozialverwaltung des Hochtaunuskreises infolge meiner datenschutzrechtlichen Kritik künftig sensibler vorgehen wird, zumal der Landrat des Hochtaunuskreises in Übereinstimmung mit dem kommunalen Datenschutzbeauftragten mir gegenüber bekräftigt hat, dass die Dauer der Überprüfungsmaßnahme durch den Außendienstmitarbeiter erheblich überzogen wurde und, um dies künftig auszuschließen, beim Hochtaunuskreis über entsprechende Maßnahmen nachgedacht wird. Vor diesem Hintergrund habe ich von einer förmlichen Beanstandung nach § 27 HDSG abgesehen, obwohl der Sozialdezernent des Hochtaunuskreises weiterhin auf der Rechtmäßigkeit der Überprüfungsaktion beharrt.

Den anfragenden Vizepräsidenten des Landtages habe ich über meine datenschutzrechtliche Bewertung informiert.

4.8.2 Hartz IV - Auskunftspflichten von Trägern der freien Wohlfahrtspflege gegenüber Arbeitsagenturen

Träger der freien Wohlfahrtspflege, die Leistungen zur Eingliederung in Arbeit erbringen, müssen mit den Agenturen für Arbeit eng zusammenarbeiten.

Ich habe mehrfach Anfragen erhalten (z.B. vom Fachbereich Soziales einer Hochschule, von einem Verband von Trägern der freien Wohlfahrtspflege), welcher datenschutzrechtliche Rahmen für die Zusammenarbeit von Trägern der freien Wohlfahrtspflege mit den Arbeitsagenturen gilt. Die Anfragen haben ihren Hintergrund vor allem darin, dass solche Träger insbesondere Schuldnerberatung, psychosoziale Betreuung und Suchtberatung durchführen.

Im Rahmen des SGB II (Grundsicherung für Arbeitsuchende) handelt es sich um Leistungen zur Eingliederung in Arbeit, die das SGB II zwecks Beseitigung von möglichen Vermittlungshemmnissen ausdrücklich vorsieht (§ 16 Abs. 2 SGB II).

§ 16 Abs. 2 SGB II

Über die in Abs. 1 genannten Leistungen hinaus können weitere Leistungen erbracht werden, die für die Eingliederung des erwerbsfähigen Hilfebedürftigen in das Erwerbsleben erforderlich sind. Dazu gehören insbesondere

…

2. die Schuldnerberatung
3. die psychosoziale Betreuung
4. die Suchtberatung …

Von daher stellt sich auch die Frage, inwieweit bei solchen Leistungen, die Hilfebedürftige erhalten, Auskunftspflichten der Träger sowie der Hilfebedürftigen gegenüber den Agenturen für Arbeit bestehen. Diese Frage stellt sich gerade auch deshalb, weil das SGB II Hilfebedürftige verpflichten, an allen Maßnahmen zu ihrer Eingliederung in Arbeit mitzuwirken (§ 2 Abs. 1 SGB II), und vor diesem Hintergrund ein gesetzlicher Informationsanspruch der Arbeitsagenturen über den Verlauf und Erfolg solcher Eingliederungsmaßnahmen besteht. Die Einzelheiten hinsichtlich der Auskunftspflichten bei Leistungen zur Eingliederung in Arbeit sind in § 61 SGB II geregelt.

§ 61 SGB II

(1) Träger, die eine Leistung zur Eingliederung in Arbeit erbracht haben oder erbringen, haben der Agentur für Arbeit unverzüglich Auskünfte über Tatsachen zu erteilen, die Aufschluss darüber geben, ob und inwieweit Leistungen zu Recht erbracht worden sind oder werden. Sie haben Änderungen, die für die Leistungen erheblich sind, unverzüglich der Agentur für Arbeit mitzuteilen.

(2) Die Teilnehmer an Maßnahmen zur Eingliederung sind verpflichtet,

1. der Agentur für Arbeit auf Verlangen Auskunft über den Eingliederungserfolg der Maßnahme sowie alle weiteren Auskünfte zu erteilen, die zur Qualitätsprüfung benötigt werden, und
2. eine Beurteilung ihrer Leistung und ihres Verhaltens durch den Maßnahmeträger zuzulassen.

Die Maßnahmeträger sind verpflichtet, ihre Beurteilungen des Teilnehmers unverzüglich der Agentur für Arbeit zu übermitteln.

Die Vorschrift bedeutet insbesondere auch, dass die Arbeitsagenturen bei Schuldner- oder Suchtberatungsstellen Auskünfte über die Teilnehmer an solchen Maßnahmen zur Eingliederung in Arbeit einholen können, ohne dass es hierfür der Einwilligung der betroffenen Hilfebedürftigen bedarf (ausführlich zu dem Dreiecksverhältnis Arbeitsagentur, Maßnahmeträger und Hilfebedürftiger die Kommentierung von Hauck/Noftz, SGB II, § 61). Allerdings ist zu beachten, dass eine Sucht- oder Schuldnerberatung ein gewisses Vertrauensverhältnis zwischen Hilfebedürftigen und der Beratungsstelle voraussetzt und Hilfebedürftige insoweit eine gewisse Diskretion erwarten und verlangen können. Erfährt aber die Beratungsstelle beispielsweise, dass Hilfebedürftige gegenüber der Arbeitsagentur ihre finanziellen Verhältnisse verschleiern oder der "Schwarzarbeit" nachgehen, oder erscheint der oder die Hilfebedürftige nicht zu den Beratungsterminen, so hat sie das der Arbeitsagentur mitzuteilen. In einem solchen Fall kommt nämlich die Absenkung bzw. der Wegfall des Arbeitslosengeldes II in Betracht (§ 31 SGB II).

Die anfragenden Stellen habe ich über die in § 61 SGB II geregelten Auskunftspflichten informiert.

4.8.3 Zusammenarbeit zwischen Arbeitsschutzbehörden und Unfallversicherungsträgern

Es ist datenschutzrechtlich zulässig, wenn Arbeitsschutzbehörden und Berufsgenossenschaften Daten anlassbezogen austauschen, um die in der Zeitarbeit erhöhten Unfallzahlen zu senken.

Das Sozialministerium hat angefragt, ob im Rahmen eines Pilotprojekts zur Erarbeitung einer gemeinsamen Aufsichtsstrategie in der Zeitarbeit Daten ausgetauscht werden dürfen, um die gesetzlichen Aufgaben sowohl der Arbeitsschutzverwaltung als auch der Berufsgenossenschaften besser erfüllen zu können. Die Beratung und Überwachung des Arbeitsschutzes in der Zeitarbeit sind dadurch geprägt, dass die Verleiher des Personals Mitglied in der Verwaltungsberufgenossenschaft, die Entleiher des Personals jeweils Mitglied in einer zur Branche gehörenden gewerblichen Berufsgenossenschaft sind und dass die staatlichen Arbeitsschutzbehörden sowohl für die Verleiher als auch die Entleiher zuständig sind. Konkret geht es bei dem Vorhaben darum, sich gegenseitig über durchgeführte Betriebsbesichtigungen und deren wesentliche Ergebnisse zu unterrichten; vorrangiges Ziel ist die Reduzierung von Arbeitsunfällen durch ein arbeitsteiliges Zusammenwirken der zuständigen Verwaltungsbehörden.

Datenschutzrechtlich kommt es darauf an, ob Daten anlassunabhängig, losgelöst vom Einzelfall verarbeitet werden oder ob anlassbezogen, im Einzelfall Daten übermittelt und verwendet werden sollen. Nur die zweite Konstellation ist grundsätzlich datenschutzrechtlich zulässig: Soweit nämlich nicht spezielle gesetzliche, etwa einen anlassunabhängigen Datenabgleich

vorsehende Vorschriften existieren, muss die Datenverarbeitung grundsätzlich auf den Einzelfall, also anlassbezogen fokussiert sein. Dementsprechend lassen das Arbeitsschutzrecht (§ 23 ArbSchG) sowie das Sozialgesetzbuch (§§ 199 SGB VII, 70 SGB X) auch nur am Einzelfall orientierte gegenseitige Datenübermittlungen zwischen Arbeitsschutzbehörden und Unfallversicherungsträgern zu.

§ 23 Abs. 2 Satz 1 ArbSchG

Die mit der Überwachung beauftragten Personen dürfen die ihnen bei ihrer Überwachungstätigkeit zur Kenntnis gelangten Geschäfts- und Betriebsgeheimnisse nur in den gesetzlich geregelten Fällen oder zur Verfolgung von Gesetzwidrigkeiten oder zur Erfüllung von gesetzlich geregelten Aufgaben zum Schutz der Versicherten dem Träger der gesetzlichen Unfallversicherung oder zum Schutz der Umwelt den dafür zuständigen Behörden offenbaren.

§ 199 Abs. 1 und 2 SGB VII

(1) Die Unfallversicherungsträger dürfen Sozialdaten nur erheben und speichern, soweit dies zur Erfüllung ihrer gesetzlich vorgeschriebenen oder zugelassenen Aufgaben erforderlich ist. Ihre Aufgaben sind

…

5. die Verhütung von Versicherungsfällen, die Abwendung von arbeitsbedingten Gesundheitsgefahren sowie die Vorsorge für eine wirksame Erste Hilfe nach dem Zweiten Kapitel,
6. die Erforschung von Risiken und Gesundheitsgefahren für die Versicherten.

(2) Die Sozialdaten dürfen nur für Aufgaben nach Abs. 1 in dem jeweils erforderlichen Umfang verarbeitet oder genutzt werden.

§ 70 SGB X

Die Übermittlung von Sozialdaten ist zulässig, soweit sie zur Erfüllung der gesetzlichen Aufgaben der für den Arbeitsschutz zuständigen staatlichen Behörden oder der Bergbehörden bei der Durchführung des Arbeitsschutzes erforderlich ist und schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Arbeitsschutzes das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt.

Weil die einzelfallbezogene Datenverarbeitung ein prägendes Strukturelement des Modellprojekts ist, ist es auch datenschutzrechtlich vertretbar, dass im Rahmen des Projekts die anfallenden Daten zentral gespeichert werden. Es handelt sich hierbei um Daten, die sich auf ein im Einzelfall aufgetretenes Problem beziehen (z.B. Unfalluntersuchungsberichte, Gefährdungsbeurteilungen). Insofern ist freilich sehr bedeutsam, dass nach Angabe des Sozialministeriums die anvisierte Datenspeicherung nicht in einer zentralen Datenbank erfolgt, die mit der latenten Gefahr unzulässiger Auswertungen verbunden ist, sondern ein "digitaler Briefkasten" eingerichtet wird, in den E-Mails mit PDF-Anhängen gelangen, um dann für die gesetzliche Aufgabenwahrnehmung den Beteiligten zur Verfügung zu stehen.

Ich habe dem Sozialministerium mitgeteilt, dass das Modellprojekt aus datenschutzrechtlicher Sicht durchgeführt werden kann. Wie für Modellprojekte typisch, wird eine anschließende Evaluation neue verwaltungsfachliche Erkenntnisse zutage fördern, und womöglich wird dann auch aus datenschutzrechtlicher Perspektive nachzubessern sein.

4.9 Personalwesen

4.9.1 Informationsrecht des Personalrats

Ein regelmäßiger, halbjährlicher Bericht über Qualifizierungsmaßnahmen mit namentlicher Auflistung der Bediensteten ist ebenso wie ein dauerhaftes Leserecht des Personalrats für die Daten der elektronischen Zeiterfassung der Bediensteten aus datenschutzrechtlicher Sicht unzulässig.

Ein Personalrat einer Anstalt des öffentlichen Rechts hat mich mit zwei Fragestellungen im Zusammenhang mit der Erarbeitung einer Rahmendienstvereinbarung zur Gestaltung der Arbeitszeit in der dortigen Dienststelle um datenschutzrechtliche Würdigung gebeten. Gefragt wurde, ob die Aushändigung von namentlichen Aufstellungen über Qualifizierungsmaßnahmen in einem halbjährlichen Bericht durch die Geschäftsführung an den Personalrat und ein dauerhaftes Leserecht für den Personalrat in der elektronischen Zeiterfassung datenschutzrechtlich zulässig sind.

Für die Fragestellungen sind, da es sich hierbei um personenbezogene Daten von Beamten und Tarifbeschäftigten handelt, die §§ 107 ff. HBG i.V.m. § 34 Abs. 1 HDSG einschlägig.

§ 34 Abs. 1 HDSG

Der Dienstherr oder Arbeitgeber darf Daten seiner Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher, planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden.

Zur Personalakte gehören nach § 107 Abs. 1 Satz 2 HBG alle Unterlagen einschließlich der in Dateien gespeicherten, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Nach § 107g Abs. 1 Satz 1 HBG, der die automatisierte Verarbeitung regelt, dürfen Personalaktendaten nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein.

Nach dem Hessischen Personalvertretungsgesetz (HPVG) sollen Dienststelle und Personalrat vertrauensvoll zusammenarbeiten "zur Erfüllung der dienstlichen Aufgaben und zum Wohle der Beschäftigten" (§ 60 Abs. 1 HPVG). Dazu und zur Durchführung seiner Aufgaben, beispielsweise die in § 62 Abs. 1 HPVG aufgezählten allgemeinen Aufgaben sowie die in § 74 Abs. 1 HPVG aufgezählten Gegenstände der Mitbestimmung, ist der Personalrat allgemein auf Informationen durch die Dienststelle angewiesen. Eine gesetzliche Regelung in Form einer Befugnis, die der Personalvertretung die hier gewünschten anlassfreien Aufstellungen und Leserechte gewähren würde, findet sich in den Vorschriften des Hessischen Personalvertretungsgesetzes explizit jedoch nicht, § 62 Abs. 2 Satz 4 HPVG stellt die Einsichtnahme in Personalaktendaten vielmehr unter den Vorbehalt der Einwilligung durch den Betroffenen: Personalaktendaten dürfen nur mit Zustimmung des Beschäftigten und nur von den von ihm bestimmten Mitgliedern des Personalrats bekanntgegeben werden.

§ 62 Abs. 2 HPVG

Der Personalrat ist zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten. Ihm sind die hierfür erforderlichen Unterlagen vorzulegen. Dazu gehören in Personalangelegenheiten Bewerbungsunterlagen aller Bewerber. Personalakten dürfen nur mit Zustimmung des Beschäftigten und nur von den von ihm bestimmten Mitgliedern des Personalrats eingesehen werden. Dienstliche Beurteilungen sind auf Verlangen des Beschäftigten dem Personalrat zur Kenntnis zu bringen.

Diese Vorschrift ist im Sinne eines gestuften Verfahrens zu verstehen, d.h. auf einen konkreten Sachverhalt und Einzelfall bezogen kann in diesem Sachzusammenhang die Erteilung einer Information, die personenbezogene Daten enthält, erforderlich sein und ggf. auch ohne vorherige Einwilligung des Betroffenen gegeben werden. Nach den grundlegenden datenschutzrechtlichen Prinzipien der Erforderlichkeit und Zweckgebundenheit bei der Verarbeitung von Daten kann dies aber bei Personalaktendaten und somit sensiblen Daten nur abgestuft und vor dem Hintergrund der beide Prinzipien beachtenden Würdigung eines konkreten Einzelfalls geschehen.

Ich habe den Personalrat über diese Rechtslage informiert.

4.9.2 Amtsbezeichnungen im Intranet der Finanzverwaltung

Von Bediensteten dürfen nur die Personaldaten im Landesintranet veröffentlicht werden, die für den verfolgten Zweck erforderlich sind.

Ein Bediensteter der hessischen Finanzverwaltung hat mich um Prüfung gebeten, ob die Angabe seiner Amtsbezeichnung im Intranet der Hessischen Finanzverwaltung datenschutzrechtlich zulässig ist.

Nach der datenschutzrechtlichen Vorschrift § 34 Abs. 1 HDSG darf der Dienstherr oder Arbeitgeber Daten seiner Beschäftigten u.a. nur verarbeiten, wenn dies zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist.

§ 34 Abs. 1 HDSG

Der Dienstherr oder Arbeitgeber darf Daten seiner Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden.

Im vorliegenden Fall hatte die zuständige OFD den einzelnen Finanzämtern freigestellt, die Amtsbezeichnungen der dortigen Bediensteten im Intranet der Hessischen Finanzverwaltung zu veröffentlichen. Exakt dieser Aspekt, dass die Veröffentlichung dieser Personaldaten in das freie Ermessen der Finanzämter gestellt wurde, hat bei mir erhebliche Zweifel an der Erforderlichkeit geweckt. Daher bat ich die OFD um Stellungnahme, ob die Angabe der Amtsbezeichnung im Intranet der Hessischen Finanzverwaltung für erforderlich gehalten wird.

Nach Prüfung durch die OFD wurden die Amtsbezeichnungen aus dem Intranet der Hessischen Finanzverwaltung entfernt. Der Vorgang zeigt exemplarisch, dass eine kritische Frage nach der Notwendigkeit der Veröffentlichung von Personaldaten einen Beitrag zur Datensparsamkeit liefern kann. Ich habe den anfragenden Bediensteten über diese Entwicklung informiert.

4.10 Finanzwesen

4.10.1 Auskunftspflicht der Finanzämter gegenüber Sozialleistungsbehörden für die Bearbeitung von Arbeitslosengeld II-Anträgen

Das Steuergeheimnis kann aufgrund § 21 Abs. 4 SGB X i.V.m. den Vorschriften des SGB II gegenüber den Sozialbehörden, die Leistungen nach dem SGB II erbringen, durchbrochen werden. Auskünfte sind aber nur zulässig, wenn keine ernsthaften Zweifel

bestehen, dass die Datenübermittlung im Einzelfall erforderlich ist, sich auf die dem Finanzamt bekannten Verhältnisse und auf den im Gesetz bestimmten Personenkreis bezieht. Die anfragende Behörde hat dies nachvollziehbar darzulegen.

Ein für die Bearbeitung von Arbeitslosengeld II-Anträgen zuständiger Mitarbeiter einer Arbeitsgemeinschaft zur Durchführung der Aufgaben nach dem SGB II (ARGE) bat mich um datenschutzrechtliche Prüfung, ob Finanzämter zu Auskünften an Arbeitsgemeinschaften gemäß § 21 Abs. 4. SGB X verpflichtet sind, wenn damit die Angaben eines Antragstellers, der Kosten für Unterkunft und Heizung aus einem Mietverhältnis mit seinen Eltern geltend macht, auf ihren Wahrheitsgehalt geprüft werden sollen. Unter Hinweis auf § 21 Abs. 4 SGB X wollte der Mitarbeiter der ARGE jeweils wissen, ob denn die Eltern des Antragstellers die behaupteten Mietzahlungen auch steuerlich als Einnahmen erklärten. Die Finanzämter lehnten derartige Anfragen unter Hinweis auf § 30 Abs. 4 S. 2 AO u.a. deshalb ab, weil Auskünfte nur zu den betroffenen Antragstellern möglich seien, aber nicht zu deren Eltern.

Die Ablehnung der Auskunft erfolgte zu Recht: Grundsätzlich unterliegen alle Informationen, die Finanzbehörden im Zusammenhang mit der Steuererhebung erhalten, dem Steuergeheimnis nach § 30 AO. Nach § 30 Abs. 4 Nr. 2 AO ist die Offenbarung steuerlicher Verhältnisse zulässig, wenn eine gesetzliche Bestimmung dies ausdrücklich vorsieht. Zu diesen gesetzlichen Offenbarungsbefugnissen gehört § 21 Abs. 4 SGB X i.V.m. dem jeweiligen Sozialleistungsgesetz. Im vorliegenden Fall sind dies die Vorschriften zur Gewährung von Arbeitslosengeld II nach dem SGB II.

Danach besteht seitens der Finanzämter eine Auskunftsverpflichtung gegenüber den Sozialleistungsbehörden, wenn die Auskunft im jeweiligen Verfahren erforderlich ist, die Einkommens- und Vermögensverhältnisse der dort genannten Personen oder der zum Haushalt zu rechnenden Familienmitglieder erfragt werden und die gewünschten Informationen dem Finanzamt bekannt sind.

§ 21 Abs. 4 SGB X

Die Finanzbehörden haben, soweit es im Verfahren nach diesem Gesetzbuch erforderlich ist, Auskunft über die ihnen bekannten Einkommens- und Vermögensverhältnisse des Antragstellers, Leistungsempfängers, Erstattungspflichtigen, Unterhaltspflichtigen, Unterhaltsberechtigten oder der zum Haushalt rechnenden Familienmitglieder zu erteilen.

Als übermittelnde Stelle hat das Finanzamt selbst zu prüfen, ob die einschlägigen Bestimmungen eine Offenbarung der geschützten Steuerdaten nach § 30 Abs. 4 S. 2 AO zulässt. Zwar kann unterstellt werden, dass andere Behörden die einschlägigen Vorschriften beachten, bei ernsthaften Zweifeln an der Zulässigkeit der Anfrage kann die Auskunftserteilung jedoch abgelehnt werden.

Soweit - wie vorliegend geschehen - das Auskunftsbegehren allein auf § 21 Abs. 4 SGB X gestützt wird, ist eine Datenübermittlung unzulässig, da ohne weitere Darlegungen ernsthafte Zweifel an ihrer Erforderlichkeit bestehen.

Erforderlich ist die Auskunft zum einen nur, wenn die erbetenen Angaben nicht mit Hilfe der nach dem SGB auskunftspflichtigen Personen festgestellt werden können.

Die Gewährung von Arbeitslosengeld II erfolgt nach den Vorschriften des SGB II. § 60 SGB II sieht in bestimmten Fällen eine Auskunftsverpflichtung Dritter (z.B. Unterhaltspflichtige) vor. Aus dem Auskunftsersuchen ist nicht erkennbar, ob seitens der Leistungsbehörde die Vorgreiflichkeit der Datenerhebung bei den Eltern geprüft wurde.

Zum anderen muss die Aufgabenerfüllung der anfragenden Behörde ohne Verwendung der Daten unangemessen erschwert sein.

Nach SGB II hängt die Gewährung von Arbeitslosengeld II jedoch nicht von der Frage ab, ob die Eltern des Antragstellers die behaupteten Mieteinnahmen versteuern. Auch wenn von den Eltern keine Angaben zu Einkünften aus Vermietung und Verpachtung erklärt wurden, bedeutet dies nicht, dass tatsächlich auch keine Mietzahlungen geflossen sind. Dies mag ggf. auf eine Steuerverkürzung bzw. -hinterziehung durch die Eltern hindeuten, hat aber auf die Leistungsgewährung an den Antragsteller nach dem SGB II keinen Einfluss.

Weiterhin ist die Auskunft nur zulässig, wenn sie sich auf den in § 21 Abs. 4 SGB X bestimmten Personenkreis bezieht. Auch dies ist dem Ersuchen nicht zu entnehmen. Befindet sich die Unterkunft des Antragstellers z.B. in der elterlichen Wohnung, so können die Eltern als "zum Haus rechnende Familienmitglieder" von § 21 Abs. 4 SGB X erfasst werden. Hat der Antragsteller angegeben, in einer den Eltern gehörenden gesonderten Wohnung zu wohnen, so könnten die Eltern evtl. als "Unterhaltsverpflichtete" zu dem in § 21 Abs. 4 SGB X genannten Personenkreis gehören. Gehören die Eltern jedoch nicht zu dem betroffenen Personenkreis, würde eine Auskunftspflicht der Finanzbehörde entfallen.

Ob und welche dieser Voraussetzungen letztlich vorliegen, ist den Finanzbehörden in der Regel nicht bekannt. Dies ist insbesondere dann der Fall, wenn das angefragte Finanzamt nicht für den Antragsteller und die Eltern zuständig ist. Eine Auskunftspflicht der Finanzämter erstreckt sich aber nur auf ihnen bekannte Verhältnisse. Weitere Ermittlungen sind von ihnen nur durchzuführen, wenn diese aus steuerlichen Gründen erforderlich wären.

Der Hinweis auf die grundsätzliche Offenbarungsbefugnis des § 21 Abs. 4 SGB X genügt nicht. Dieser pauschale Hinweis ermöglicht der Finanzbehörde keine Prüfung der Zulässigkeit der Datenübermittlung.

Ich habe die ARGE deshalb darüber informiert, dass eine Offenbarung von Steuerdaten durch die Finanzverwaltung in den geschilderten Fällen nur dann zulässig ist, wenn neben dem Hinweis auf die Offenbarungsbefugnis des § 21 SGB X die dort

genannten Voraussetzungen unter Bezug auf das jeweilige Leistungsgesetz und den jeweiligen Einzelfall ausreichend dargestellt werden.

5. Kommunen

5.1 Ergebnisse der Prüfung von Kommunen

Wie in den beiden letzten Jahren habe ich rechtliche und technische Ausprägungen des Einsatzes der Informationstechnik in Kommunen geprüft. Die teils negativen Erfahrungen der vergangenen Jahre haben sich weitgehend bestätigt. Es gab aber auch neue Ergebnisse, die für viele Kommunen von Bedeutung sein können. Überraschenderweise musste ich feststellen, dass es noch immer Kommunen gibt, die keinen behördlichen Datenschutzbeauftragten bestellt haben.

5.1.1 Prüfumfang

Wie zuvor habe ich den Status der IT-Sicherheit und den Umfang von Datenverarbeitungen im Auftrag sowie deren vertragliche Regelungen bei hessischen Kommunen geprüft. In diesem Jahr war die gesamte Palette von der Großstadt, über Städte mittlerer Größe bis zu kleinen Kommunen vertreten. Kleine Kommunen verlassen sich dabei verständlicherweise in stärkerem Maße auf die Unterstützung Externer beim IT-Betrieb. Bei den größeren Kommunen gab es in jedem Fall eigenes Personal das nur für den IT-Betrieb zuständig war und durch den Dienstleister lediglich unterstützt wurde.

5.1.2 Einzelne Feststellungen

Bei den Prüfungen hat sich wieder gezeigt, dass viele der Schwachstellen, die ich in den letzten Jahren vorgefunden habe, erneut vorzufinden waren. Ich möchte im Folgenden nur charakteristische Ergebnisse erneut darstellen und ansonsten auf neue Sachverhalte genauer eingehen.

5.1.2.1 Organisatorische und rechtliche Sachverhalte

5.1.2.1.1 E-Mail und Internet

Ein Dauerbrenner waren Regelungen zur Nutzung von E-Mail und Internet. Hier habe ich bei den meisten Kommunen keine oder unzureichende, d.h. nicht eindeutige, Vorgaben vorgefunden. Gerade die private Nutzung wurde oft ohne schriftliche Regelungen geduldet. Die damit verbundenen Konsequenzen hatte ich bereits dargestellt (vgl. 35. Tätigkeitsbericht, Ziff. 6.1.2.1).

Eine Besonderheit ist jedoch in zwei Fällen aufgetreten. Der Administrator resp. ein Amtsleiter, der zu dem Zeitpunkt, an dem das System aufgesetzt wurde, Administrator war, hatten für alle E-Mail-Postfächer eine Leseberechtigung. Dieser Umstand war umso bedenklicher, da in beiden Fällen die private Nutzung geduldet wurde. Sie erklärten diesen Umstand durch Installationsabläufe, bei denen eine Administratorkennung als leseberechtigt eingetragen werden musste. Diese Einträge wurden aber nie zurückgenommen und die Kennung wurde auch nicht deaktiviert. Ich habe eine sofortige Änderung dieser Berechtigungen gefordert.

5.1.2.1.2 Umsetzung des HDSG

Selbst klare Anforderungen des HDSG waren nicht immer erfüllt. In zwei Fällen waren weder ein behördlicher Datenschutzbeauftragter noch ein Vertreter bestellt. In einem anderen Fall gab es keinen Vertreter. Gegenüber den betroffenen Kommunen habe ich hervorgehoben, dass die Bestellung der behördlichen Datenschutzbeauftragten kein Selbstzweck ist. Vielmehr sind gerade die Datenschutzbeauftragten vor Ort für die Erfüllung der Verpflichtungen nach dem HDSG besonders wichtig. Dieser Mangel musste deshalb schnell behoben werden.

Wenn es sie überhaupt gab, so waren die Verträge zur Datenverarbeitung im Auftrag sehr oft verbesserungswürdig. Sehr häufig fehlte eine Unterwerfungsklausel unter die Kontrolle durch den Hessischen Datenschutzbeauftragten, wie sie § 4 HDSG zwingend vorschreibt. In einem Fall fehlte für den Dienstleister, der die gesamte IT betreute, jegliche schriftliche Vereinbarung. Es gab folglich noch nicht einmal eine Übersicht, welche Aufgaben überhaupt vergeben waren.

Bei den Verfahrensverzeichnissen war das Bild uneinheitlich. Eine Kommune hatte die Verfahrensverzeichnisse in vorbildlicher Weise geführt. Sie waren nicht nur vollständig, sondern es war durch organisatorische Maßnahmen sichergestellt, dass jede Änderung an einem Verfahren kurzfristig in das Verzeichnis übernommen wurde. Während die Verfahrensverzeichnisse ansonsten meist einige kleine Lücken besaßen, fehlten bei zwei Kommunen Verfahrensverzeichnisse völlig.

Besonders in größeren Kommunen sollte in Anlehnung an die vom BSI vorgeschlagene Vorgehensweise ein IT-Sicherheitsprozess eingerichtet werden. Die dazu nötigen organisatorischen Maßnahmen sind in aller Regel nicht getroffen. Da nicht überall das erforderliche Know-how vorhanden ist, muss fallweise der Dienstleister beratend das Thema IT-Sicherheit begleiten.

5.1.2.2 Räumliche Sicherungsmaßnahmen

In einer geprüften Gemeinde gab es ganz offensichtlich keinerlei Anweisungen zur Abschottung verschiedener Abteilungen. Auch jeder zufällig vorbeikommende Bürger hatte vielfältige Möglichkeiten, ein ungestörtes Aktenstudium zwischengelagerter Unterlagen vorzunehmen oder sich am PC an einem verlassenen Arbeitsplatz in Dateien der Verwaltung über dies

und das zu informieren. Es gab hier weder abgeschlossene Türen nach außen noch verschlossene Räume im Innern, noch passwortgeschützte Bildschirmschoner für PC.

In einem anderen Fall ließ die Unterbringung und Einrichtung der Beihilfestelle zu wünschen übrig. Hier war es dem Reinigungspersonal der Behörde ohne Weiteres möglich, Beihilfeakten zur Kenntnis zu nehmen.

Auch die Handhabung von Schließanlagen gab Anlass zur Kritik. So hatten in einer Kommune alle Magistratsmitglieder einen Generalschlüssel für alle Räumlichkeiten einschließlich des Serverraums.

In allen Fällen habe ich umgehende Abhilfe gefordert. Ich werde die Umsetzung der geforderten Maßnahmen alsbald überprüfen.

5.1.2.3 Technische Sachverhalte

Defizite gab es ebenfalls bei allgemeinen Dienstanweisungen zum Umgang mit der IT. Sie waren oft nicht vorhanden oder nur rudimentär. Es müssen aber gerade der Umgang mit Passwörtern, die Nutzung von USB-Geräten - soweit nicht technisch kontrolliert - oder die Installation privater Software geklärt sein.

Immer wieder habe ich viel zu kurze Passwörter vorgefunden. Selbst bei den Administratorkennungen war eine Passwortlänge von fünf Stellen keine Ausnahme. Die Vergabe von Passwörtern stellte sich häufig als Problem heraus. So wurden Passwörter teilweise durch die Administratoren vergeben und nur alle sechs Monate gewechselt. Dies genügt den Anforderungen aus dem Maßnahmenkatalog des BSI nicht.

Wie im letzten Jahr waren oft ungesicherte USB-Schnittstellen anzutreffen und das BIOS war in den seltensten Fällen durch ein Passwort geschützt. Fehlen solche Sicherungsmaßnahmen, ist ein Booten von USB-Sticks oder CDs mit einem eigenen Betriebssystem und damit ein unkontrollierter Zugriff auf Dateien möglich. Wegen der damit verbundenen Risiken reicht es nicht, mit Dienstanweisungen Nutzungseinschränkungen vorzugeben. Ich halte eine technische Kontrolle für erforderlich (vgl. 32. Tätigkeitsbericht, Ziff. 18.4).

Wie oben geschildert, hatten in zwei Kommunen die Administratoren standardmäßig Zugriffsrechte auf jedes E-Mail-Postfach. Es war daher anhand von Protokollen nicht nachvollziehbar, wenn ein Administrator sich auf ein Postfach schaltet.

5.1.3 Bewertung

Auch dieses Jahr hat sich bestätigt, dass die Umsetzung der Anforderungen des Datenschutzes keine Selbstverständlichkeit ist. Ich werde auch im nächsten Jahr Prüfungen vornehmen. Dabei geht es nicht nur darum, Schwachstellen festzustellen und zu beheben, sondern ich will auch die Anforderungen an die Kommunen präziser auf deren Verhältnisse ausgerichtet formulieren können.

5.2 Ergebnisse der Prüfung von Passbehörden

Die Überprüfung mehrerer Passbehörden hat gezeigt, dass die Umsetzung des neuen Passgesetzes, das nunmehr die Aufnahme von Fingerabdrücken in Pässe vorschreibt, aus datenschutzrechtlicher Sicht noch unbefriedigend abläuft. Hinsichtlich der Auskunftserteilung, der Löschung der Fingerabdrücke bei den Passbehörden sowie des Einsatzes der elektronischen Signaturen bei der Übertragung der Antragsdaten an die Bundesdruckerei müssen die Abläufe noch nachgebessert werden.

5.2.1 Die Einführung des ePass

Nach den Anschlägen vom 11. September 2001 hat es weltweit viele Aktivitäten gegeben, um auch den Reiseverkehr zu kontrollieren. Eine Maßnahme seitens der EU war die Aufnahme biometrischer Merkmale in Pässe, Visa und Aufenthaltstitel, auf die sich die Mitgliedsstaaten der EU verständigten. Die Festlegung erfolgte in der EG-Verordnung 2252/2004 vom 13. Dezember 2004 (ABlEG 2004 L 385/1 vom 29. Dez. 2004) über "Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten". Auf Basis von dieser Verordnung wurden das Passgesetz geändert und eine Reihe technischer Rahmen gesetzt (BSI TR-3104 mit Anhängen). Im Ergebnis wurde 2005 der elektronische Reisepass (ePass) der ersten Generation eingeführt; auf ihm war als biometrisches Merkmal das Passfoto gespeichert. Seit dem 1. November 2007 wird der ePass der zweiten Generation ausgegeben, auf dem zusätzlich zwei Fingerabdrücke gespeichert sind.

Die Datenschutzbeauftragten haben die Aufnahme von Fingerabdrücken in Reisedokumente stets kritisch gesehen. Insbesondere sollte verhindert werden, dass die Fingerabdrücke von Antragstellern über die Antragstellung hinaus gespeichert werden. Dem trägt das Passgesetz Rechnung. In § 4 Abs. 3 Satz 3 wird eine bundesweite Datenbank explizit ausgeschlossen, in § 16 Abs. 3 ist festgelegt, dass der Passhersteller die Daten nach der Herstellung zu löschen hat und in § 16 Abs. 2 ist festgelegt, dass die Daten in der Passbehörde nach der Aushändigung zu löschen sind.

§ 4 Abs. 3 PassG

Eine bundesweite Datenbank der biometrischen Daten nach Satz 1 wird nicht errichtet…

§ 16 Abs. 2 und 3 PassG

(2) Beantragung, Ausstellung und Ausgabe von Pässen dürfen nicht zum Anlass genommen werden, die dafür erforderlichen Angaben und die biometrischen Merkmale außer bei den zuständigen Passbehörden zu speichern. Entsprechendes gilt für die zur Ausstellung des Passes erforderlichen Antragsunterlagen sowie für personenbezogene fotografische Datenträger (Mikrofilme). Die bei der Passbehörde gespeicherten Fingerabdrücke sind spätestens nach Aushändigung des Passes an den Passbewerber zu löschen.

(3) Eine zentrale, alle Seriennummern umfassende Speicherung darf nur bei dem Passhersteller und ausschließlich zum Nachweis des Verbleibs der Pässe erfolgen. Die Speicherung der übrigen in § 4 Abs. 1 genannten Angaben und der in § 4 Abs. 3 genannten biometrischen Daten bei dem Passhersteller ist unzulässig, soweit sie nicht ausschließlich und vorübergehend der Herstellung des Passes dient; die Angaben sind anschließend zu löschen.

Um die Passbehörden bei der Umsetzung des Gesetzes zu unterstützen, hat das BSI im Auftrag des BMI eine "Handreichung Informationssicherheit für deutsche Passbehörden" erarbeitet.

Unabhängig von diesen Aktivitäten auf Bundesebene habe ich Passämter in Hessen dahingehend geprüft, wie sich die Abläufe bei der Antragstellung gestalten und ob die Daten entsprechend den o.g. Vorgaben gespeichert und gelöscht werden.

5.2.2 Wesentliche Ergebnisse der Prüfung in Passämtern

5.2.2.1 Abläufe

Obwohl es Abweichungen im Detail gab, waren die Abläufe in den Kommunen vergleichbar:

- Der Passbewerber oder die Passbewerberin beantragt einen Reisepass.
- Das Passamt prüft, ob ein Passversagungsgrund vorliegt.
  Wenn nein, werden die Daten des Passbewerbers/der Passbewerberin aus dem Melderegister übernommen.
- Er/Sie muss ein ICAO-konformes Passbild vorlegen,
- die Unterschrift leisten und
- es werden seine/ihre Fingerabdrücke erfasst.
- Aus den Daten wird der Antrag durch die Passantragssoftware generiert.

Die Antragsdaten, evtl. von mehreren Bürgern, werden auf den Rechnern im Passamt gespeichert. Für die Übertragung zum Passhersteller Bundesdruckerei werden sie signiert und so verschlüsselt, dass nur die Bundesdruckerei die Daten lesen kann. Dazu wird das Verfahren "digant" genutzt. Die Bundesdruckerei bestätigt den Empfang der Daten. Wenn keine Bestätigung der Bundesdruckerei über den korrekten Empfang eingeht, wird die Übertragung wiederholt.

Mit Ausnahme der Fingerabdrücke stehen die Antragsdaten den Sachbearbeitern der Passbehörden für Auskünfte aus dem Passregister zur Verfügung. Die kompletten Antragsdaten, inklusive der Fingerabdrücke, sind noch gespeichert, damit bei Diskrepanzen zwischen den Antragsdaten und einem ausgestellten Pass der Antrag erneut an die Bundesdruckerei übertragen werden kann.

Die Bundesdruckerei stellt den Pass her und löscht anschließend die Antragsdaten, insbesondere die Fingerabdruckdaten (§ 16 Abs. 3 PassG; Ziff. 16.3 Allgemeine Verwaltungsvorschriften zur Durchführung des Passgesetzes).

PassVwV zu § 16 PassG

16.3 Die bei der Bundesdruckerei GmbH ausschließlich zum Zwecke der Passherstellung vorübergehend gespeicherten Daten des Passbewerbers sind unverzüglich nach Versand des Passes an die Passbehörde zu löschen. Die zum Nachweis des Verbleibs der Pässe gespeicherten Seriennummern oder Lieferscheine sind nach Ablauf von 30 Jahren nach Versand des Passes an die zuständige Passbehörde zu löschen.

16.3.1 Die Bundesdruckerei GmbH darf auf Ersuchen Passbehörden und anderen Behörden im Geltungsbereich des Passgesetzes mitteilen, welche Passbehörde den Pass mit der von der anfragenden Stelle bezeichneten Seriennummer erhalten hat.

16.3.2 Auskünfte an Private oder ausländische Stellen (z.B. Botschaften) sind nicht zulässig.

Nach einiger Zeit erhält das Passamt den Pass und führt eine Qualitätskontrolle durch. Stimmen die Antragsdaten mit den Passdaten überein, unterschreibt das Passamt den Pass und setzt den Status des Antrags im Bearbeitungsprogramm auf abholbereit. Anderenfalls wird geprüft, um was für eine Abweichung es sich handelt. Je nach Fehler wird der Antrag erneut übertragen oder es muss ein neuer Antrag gestellt werden.

Der Antragsteller/die Antragstellerin wird informiert, dass sein/ihr Pass bereit liegt. Dies kann per Brief oder auf andere Art geschehen.

Wenn der Pass abholt wird, sind einige Dinge zu beachten:

- Der Antragsteller bzw. die Antragstellerin muss sich ausweisen.

- Es werden ihm bzw. ihr die im neuen Pass gedruckten und auf Wunsch die gespeicherten Daten gezeigt. Die Anzeige der gespeicherten Daten geschieht an einem Passleser. Die Fingerabdrücke werden aber nur als Bild angezeigt. Eine Prüfung, ob es tatsächlich die Abdrücke des Antragstellers/der Antragstellerin sind, findet nicht statt.
- Wenn der Pass die richtigen Daten enthält, wird der neue Pass gegen Rückgabe des alten Passes - soweit vorhanden - ausgehändigt. Im Fehlerfall muss ein neuer Antrag gestellt werden.
- Der Status des Passantrags wird auf "abgeholt" gesetzt.

Erst jetzt werden die Fingerabdrücke in den geprüften Anwendungen gelöscht.

5.2.2.2 Problempunkte und Lösungsansätze

5.2.2.2.1 Anspruch auf Löschung auch bei Datensicherungen

Nach § 16 Abs. 2 PassG sind die Fingerabdrücke nach Aushändigung des Passes zu löschen. Löschen bedeutet dabei nach der Definition des § 2 Abs. 2 Nr. 5 HDSG das Unkenntlichmachen gespeicherter Daten. In der Praxis ergeben sich Probleme mit den Datensicherungen.

Die Antragsdaten werden nicht nur auf den Rechnern der Passämter und deren Dienstleistern gespeichert, sondern auch auf Sicherungskopien, die Wochen und Monate aufbewahrt werden.

Die Fingerabdrücke werden nach der Abholung im Verfahren logisch gelöscht. Sie befinden sich jedoch noch für kurze Zeit in der Datenbank und infolge von Datensicherungen deshalb für lange Zeit noch auf Sicherungsbändern. Insoweit sind die gesetzlichen Vorgaben aus § 16 Abs. 2 PassG faktisch nicht umgesetzt. Die Passämter können eine sinnvolle Lösung allerdings nicht allein umsetzen.

Nach meiner Einschätzung kann das Problem nur durch Änderungen der Software und der Organisation gelöst werden. Die Verfügbarkeit der Daten muss weiterhin sichergestellt sein. Deshalb kann auf Datensicherungen nicht verzichtet werden und diese Sicherungen müssen auch alle Daten umfassen. Der nachfolgende Vorschlag berücksichtigt sowohl die Sicherheitsproblematik als auch die Vorgaben des Gesetzgebers zur Löschung der Fingerabdrücke.

Der Vorschlag geht von folgenden Annahmen aus:

- Es kann zu Problemen führen, Teile einer Datenbank nicht zu sichern.
  Je nach Datenstruktur der Software zur Passantragstellung kann es Probleme bereiten, Teile von der Datensicherung auszunehmen. Bei einer Rücksicherung führt es zu Fehlern, wenn Verweise (pointer) in der Datenbank, beispielsweise der Pointer auf das Abbild eines Fingerabdrucks, nicht aufgelöst werden können.
- Eine Rücksicherung macht nur für wenige Tage Sinn; dies sind zwei bis maximal drei Arbeitstage. Bei einer Rücksicherung muss aufbauend auf eine Komplettsicherung die Datenbasis rekonstruiert werden. Einzelne Teile können wegen der Verweise innerhalb der Daten nicht rekonstruiert werden. Die Datensicherung wird deshalb nur bei einem vollständigen Ausfall der Anwendung benötigt, was kurzfristig bemerkt werden muss. Andere Fehler können durch Rücksicherung nicht korrigiert werden, da die Fehler mit rekonstruiert würden; hier hilft nur, ein Programm zur Fehlerkorrektur zu schreiben. Es sollte mehr als eine Sicherungsgeneration vorliegen, um trotz eines fehlerhaften Sicherungsmediums noch eine vollständige Sicherung zu haben.
- Mehrere Tage vor der Aushändigung findet eine Qualitätssicherung durch das Passamt statt. Nach meiner Prüfung sieht die Qualitätssicherung wie folgt aus:
  Passämter kontrollieren die Pässe, wenn sie von der Bundesdruckerei kommen, bevor sie durch das Passamt unterschrieben werden. Stellen sie einen Fehler fest, wird der Fehler korrigiert und der Pass erneut, mit den noch vorhandenen Daten - inkl. Fingerabdrücken - vervollständigt, beantragt. Liegt ein aus Sicht des Passamtes fehlerfreier Pass vor, wird dieser unterschrieben. Anschließend wird die den Antrag stellende Person benachrichtigt, dass der Pass zur Abholung bereit liegt. Dies geschieht meist erst nach einigen Tagen. Weitere Fehler können erst bei der Aushändigung durch den Antragsteller/die Antragstellerin festgestellt werden.
- Bei der Aushändigung festgestellte Fehler können durch einen Neuantrag mit Abnahme von Fingerabdrücken korrigiert werden.
  Da der Passempfänger bzw. die Passempfängerin vor Ort ist, können die Fingerabdrücke erneut abgenommen werden.

Mein Lösungsvorschlag umfasst drei Punkte:

- Es werden Datensicherungen vorgenommen, die nach zwei bis maximal drei Arbeitstagen gelöscht bzw. überschrieben werden.
- Die Daten werden bei anderen Sicherungen (Wochen-, Monats-, Quartals-, Jahressicherungen …) nicht mit gesichert.
- Die Fingerabdrücke werden in der Anwendung gelöscht, sobald die Betroffenen benachrichtigt werden, dass der Pass zur Abholung vorliegt.

Die Datensicherungen beinhalten dadurch ein vollständiges, konsistentes Abbild der Daten und - fast - immer sind die Fingerabdrücke nach der Aushändigung nicht mehr auf Sicherungsmedien gespeichert. Damit wären die Anforderungen bezüglich der Verfügbarkeit erfüllt und die rechtliche Vorgabe weitgehend umgesetzt.

5.2.2.2.2 Signatur

Die Antragsdaten werden vor der Übertragung signiert und verschlüsselt. Ich musste bei meiner Prüfung aber feststellen, dass die Signatur durch den Empfänger, also den Passhersteller Bundesdruckerei, nicht geprüft wurde. So war in einem Passamt die Signaturkarte beschädigt. Auf die Frage, wann eine Ersatzkarte zugestellt werden könne, wurde dem Passamt gesagt: "Nehmen Sie die Ersatzkarte einer Nachbarkommune und signieren Sie damit." Der Leiter des Passamts war zwar irritiert, aber er folgte dem Vorschlag und besorgte sich, für eine kurze Zeit, die Karte einer anderen Kommune. Damit signierte der die Anträge. Rückfragen oder Probleme ergeben sich daraus nicht.

Die logische Konsequenz für mich ist, dass die Bundesdruckerei nicht prüft, ob die Anträge von der signierenden Kommune stammen. Damit wäre die Signatur aber auf die Funktion reduziert, Übertragungsfehler zu erkennen. Es wäre keine Analogie zu einer Unterschrift, mit der Passämter als Absender Anträge bestätigen und weiterleiten.

Seitens des BMI wurde dies damit begründet, dass Clearingstellen in die Übertragung eingeschaltet sind und die Bundesdruckerei die Signatur der Clearingstellen und nicht der Kommunen prüfe. Die Signatur wird aber immer durch die Kommune vorgenommen. Die Clearingstellen nehmen keine Signatur vor und prüfen keine, denn die Daten sind für die Bundesdruckerei verschlüsselt und können durch Clearingstellen nicht gelesen werden. Insofern kann ich der Argumentation nicht folgen.

Die Signatur der übertragenen Anträge macht nur Sinn, wenn überprüft wird, ob die Anträge von der signierenden Kommune stammen. Abweichungen muss nachgegangen werden. Diese Forderung richtet sich an den Verordnungsgeber und den Passhersteller.

5.2.2.2.3 Datenprüfung bei der Ausgabe

Die Abläufe in den Passämtern sehen vor, dass den Passempfängern bzw. -empfängerinnen, wenn sie das wollen, vor der Aushändigung an einem dafür vorgesehenen Lesegerät die gespeicherten Daten angezeigt werden. Damit wird insbesondere dem § 16 Abs. 6 PassG Genüge getan.

§ 16 Abs. 6 PassG

Auf Verlangen hat die Passbehörde dem Passinhaber Einsicht in die im Chip gespeicherten Daten zu gewähren.

Die zum Zeitpunkt der Prüfung aufgestellten Lesegeräte erlaubten den Zugriff auf alle gespeicherten Daten, auch die Fingerabdrücke. Von den Fingerabdrücken wurde aber nur das Bild auf dem - relativ - kleinen Bildschirm gezeigt. Mit diesem Bild kann niemand etwas anfangen. Es ist nur erkennbar, dass Abdrücke gespeichert sind, aber ob es Bilder der eigenen Fingerabdrücke sind, können Passinhaber nur glauben, aber nicht überprüfen.

Wenn Passinhaber es wollen, muss eine Prüfung auf Echtheit erfolgen. Es muss ein Abgleich der gespeicherten gegen ihre mit einem Fingerabdruckscanner erfassten Fingerabdrücke vorgenommen werden. Dazu muss die von der Bundesdruckerei bereitgestellte Technik geändert werden.

5.2.2.3 Ergebnisse

Die Abläufe in den Passämtern waren einheitlich. Die Software unterstützte die Abläufe unabhängig vom Hersteller. Nach der Antragstellung waren die Antragsdaten bis auf die Fingerabdrücke für Sachbearbeiter im Passregister noch einsehbar. Vor der Passaushändigung wurden alle Antragsdaten, auch die Fingerabdrücke, noch in Datenbanken gespeichert. Danach wurden zwar die Fingerabdrücke aus den Datenbanken gelöscht, sie waren jedoch weiterhin für längere Zeit auf Sicherungsmedien gespeichert. Sowohl bei diesem Punkt als auch bei den Problempunkten Signatur und Anzeige samt Prüfung von Abdrücken können die Kommunen keine eigene Lösung finden. Es sind die Anbieter und der Verordnungsgeber gefordert.

5.3 Melderegisterauskünfte an Adresshändler

Das HMDIS hat den Meldeämtern empfohlen, vor der Übermittlung von einfachen Melderegisterauskünften an Adresshandelsfirmen deren Versicherung einzuholen, dass die übermittelten Daten nur an den jeweiligen Auftraggeber weitergegeben und nur zu abrechnungstechnischen Zwecken/Reklamationszwecken für einen erforderlichen Zeitraum gespeichert werden. Besser wäre es jedoch, eine eindeutige gesetzliche Grundlage eigens für Datenübermittlung zu Werbezwecken zu schaffen, um Betroffenen mindestens ein Widerspruchsrecht gegen die Datenweitergabe zu Direktwerbezwecken zu garantieren, Adresshändler zur Zweckangabe und Zweckbindung zu verpflichten und die Aufklärbarkeit bei etwaigen Missbrauchsfällen zu ermöglichen.

Gemäß § 34 Abs. 1 HMG **darf** die Meldebehörde **Einzelauskünfte** über einzelne bezeichnete Einwohner und Einwohnerinnen und **Sammelauskünfte** über eine Vielzahl bezeichneter Einwohner und Einwohnerinnen übermitteln. Die Auskunft beinhaltet Vor- und Familiennamen, Doktorgrad und Anschriften. Besondere Voraussetzungen müssen nicht dargelegt werden, eine Zweckangabe oder Zweckbindung bzgl. der Verwendung der Daten sieht das Gesetz ebenfalls nicht vor. Jedoch ist § 7 HMG zu beachten. Danach dürfen schutzwürdige Belange Betroffener nicht beeinträchtigt werden.

Aus dem systematischen Zusammenhang der Bestimmungen folgt kein Regel-Ausnahme-Verhältnis. Die Verweigerung der Auskunft beschränkt nicht die Freiheitssphäre der Auskunftsbegehrenden, sondern erweitert deren Rechtsstellung zulasten derjenigen, über deren Daten Auskunft begehrt wird. Üblicherweise geht man gleichwohl davon aus, dass deren Belange in der Regel nur dann erkennbar sind, wenn für die betroffene Person im Melderegister eine Auskunftssperre oder ein Wider-

spruch gegen eine Datenübermittlung eingetragen ist. In allen anderen Fällen soll zunächst nichts gegen eine Auskunftserteilung sprechen. Es entspricht damit der ständigen Praxis der Meldebehörden, die einfache Melderegisterauskunft - ob einzeln oder in der Vielzahl - gegen Zahlung einer entsprechenden Gebühr zu erteilen. Die Betroffenen erhalten von den Datenübermittlungen keine Kenntnis.

Diese Verfahrensweise gilt auch für Auskünfte an Adresshändler, die im Auftrag Dritter (z.B. Versicherungen) Einzelauskünfte oder umfangreiche Sammelauskünfte über eine Vielzahl bezeichneter Einwohner begehren.

Neben dem eigentlichen Zweck, die Daten an den jeweiligen Auftraggeber weiterzugeben, unterhalten die Adressfirmen häufig interne Datenbanken, in denen sie die abgefragten Daten aus den Melderegistern sammeln, abgleichen, mit anderen Daten und Informationen verbinden und bei Bedarf erneut an Dritte gegen Entgelt weitergeben können.

Eine angemessene Ermessensentscheidung, ob schutzwürdige Belange bei der Datenübermittlung an Adresshändler beeinträchtigt werden, kann die Meldebehörde nach gängigem Verständnis mangels hinreichender Anhaltspunkte nicht treffen. Wird z.B. eine Anfrage aus dem internen Datenpool einer Adresshändlerfirma beantwortet, kann eine zwischenzeitlich im Melderegister eingetragene Auskunftssperre nicht berücksichtigt werden. Der durch die Sperren im amtlichen Melderegister gewährte Schutz wird unterlaufen.

Nach meinem Verständnis ist bereits de lege lata eine restriktive Handhabung des § 34 Abs. 1 HMG geboten.

Die in der letzten Zeit aufgedeckten Datenmissbrauchsfälle haben gezeigt, dass die Verwendung der Meldedaten auch für illegale Zwecke nicht ausgeschlossen werden kann. Diese Gefahr vergrößert sich entsprechend bei der Abfrage von Sammelauskünften, die für dritte Auftraggeber eingeholt und zusätzlich im internen Datenpool eines Adresshändlers verarbeitet werden. Auch das Bundesverwaltungsgericht hat mit Urteil vom 21. Juni 2006 (Az. 6 C 05/05) festgestellt, dass die Meldebehörde eine einfache Melderegisterauskunft nicht erteilen darf, wenn diese erkennbar für Zwecke der Direktwerbung begehrt wird und der Betroffene der Übermittlung seiner Daten zu Werbezwecken widersprochen hat. Der Widerspruch geht aber ins Leere, wenn der Werbezweck nicht erkennbar ist. Der Meldebehörde ist nicht zuzumuten, generell eigene Ermittlungen darüber anzustellen, welche Zwecke die Auskunftsersuchenden im Einzelfall verfolgen. Sobald aber Indizien für Missbrauch vorliegen, reduziert sich das Ermessen der Meldebehörde auf Null. Sie muss die Auskunft verweigern.

Das HMDIS hat daher den Meldebehörden empfohlen, vor Datenübermittlungen an gewerbsmäßige Adresshändler von ihnen eine Erklärung zu fordern, dass die übermittelten Daten nur an einen Auftraggeber weitergegeben werden und nicht länger als 30 Tage (zu Abrechnungs- und Reklamationszwecken) aufbewahrt werden. Die Maßnahme geht sicherlich in die richtige Richtung, ob sie aber in der Praxis die erhoffte Wirkung zeigen kann, erscheint fraglich. So können die Mitarbeiter einer Meldebehörde nicht ohne weiteres erkennen, ob es sich bei einem Antragsteller um einen Adresshändler handelt und die Erklärung gefordert werden sollte. Hinzu kommt, dass bei automatisierten Melderegisterauskünften über Internet oder Portale (§ 34a HMG) eine solche Versicherung im Einzelfall nicht vorgesehen ist. Eine grundsätzliche Erklärung gegenüber dem Portalbetreiber, am automatisierten Verfahren nur teilzunehmen, wenn keine zweckwidrige Verwendung der Daten erfolgt, wird in der Praxis ebenfalls nicht nachprüfbar sein.

Es sollte daher eine rechtliche Grundlage speziell für Einzelauskünfte zu Direktmarketingzwecken und für Sammelauskünfte jeder Art (ähnlich den besonderen Melderegisterauskünften des § 35 HMG) geschaffen werden. Betroffene sollten mindestens ein Widerspruchsrecht erhalten, über das die Meldebehörde zu informieren hat. Auskunft suchende Adresshändler sollten angeben müssen, für welche abschließenden Zwecke (Auftrag und Abrechnung) und ggf. für welche Auftraggeber das Ersuchen gestellt wird. Damit wäre der Werbezweck für die Meldebehörde eindeutig erkennbar und die Zweckangabe bzw. Zweckbindung für die Adresshändler verpflichtend. Die Verarbeitung der Daten im eigenen Pool wäre danach kein erlaubter Zweck. Etwaige Widersprüche Betroffener könnten auch im automatisierten Verfahren beachtet werden und etwaige Missbrauchsfälle wären eher nachweisbar. Um das unzulässige Erwirken von Melderegisterauskünften zu Eigenzwecken sowie die vorsätzliche oder zweckwidrige Verwendung im internen Datenpool eines Adresshändlers zu sanktionieren, sollte die neue Regelung auch als Ordnungswidrigkeitstatbestand in § 39 HMG aufgenommen werden.

5.4 Weitergabe von Daten durch eine Stadträtin

Eine an ein Mitglied des Stadtrats persönlich gerichtete E-Mail darf nur an die beteiligten Fachämter und die zuständige Ortsverwaltung weitergeleitet werden, wenn und soweit dies sachlich erforderlich ist. Mitglieder des Ortsbeirats haben über ihnen in ihrer amtlichen Funktion bekannt gewordene Angelegenheiten die Verschwiegenheitspflichten nach § 24 Abs. 1 HGO zu beachten.

Nachdem eine hessische Kommune nach langjährigem Streit die Nutzungsverordnung für eine öffentliche Fläche erlassen hatte, äußerte ein Bürger Unmut hierüber in einer Mail gegenüber der zuständigen Stadträtin. Kurz darauf wurde er von seinem Arbeitgeber auf diese Kritik angesprochen. Er bat mich um datenschutzrechtliche Prüfung, ob seine persönliche Mail an eine Stadträtin an Mitglieder politischer Gremien dieser Stadtverwaltung weitergegeben und dann seinem Arbeitgeber übermittelt werden durfte.

Recherchen ergaben, dass die Stadträtin die an sie gerichtete Mail beantwortet hatte, sie gleichzeitig aber an die beteiligten Fachämter und die zuständige Ortsverwaltung weiterleitete. Da die Mail vom Büro-PC verschickt und das automatisch generierte Impressum nicht gelöscht worden war, nutzten Mitglieder des Ortsbeirats diese Information, um sich an den Arbeitgeber des Bürgers zu wenden.

Da die Mail an die Stadträtin aber keinerlei Anträge oder Fragen enthielt, sondern lediglich Unmutsäußerungen zu einer politischen Entscheidung, konnte ich den Argumenten, dass es sich bei der Weiterleitung der Mail um eine verwaltungsinterne sowie verwaltungsübliche und damit zulässige Datenübermittlung handelte, nicht folgen. Zum einen war die Weiterleitung der Mail an die zuständige Ortsverwaltung nicht erforderlich, da keine weiteren Aktivitäten erwartet wurden, zum anderen war sie auch nicht verwaltungsintern, da einer Stadträtin bekannt sein muss, dass die Ortsverwaltung als Geschäftsstelle des Ortsbeirats immer auch die Ortsbeiratsmitglieder informiert.

Die personenbezogene Weitergabe der Mail war nicht erforderlich und damit nach § 11 HDSG auch unzulässig. Ich habe neben der betroffenen Stadträtin auch den Datenschutzbeauftragten der Kommune aufgefordert, alle Mitarbeiter nochmals auf die erforderliche Sorgfalt bei der Nutzung der Weiterleitungsfunktion des E-Mail-Systems hinzuweisen. Bevor eine Mail an andere Stellen weitergeleitet wird, muss grundsätzlich in jedem Einzelfall geprüft werden, ob dies in personenbezogener Form tatsächlich erforderlich ist.

Sehr viel kritischer ist hier allerdings die weitere Nutzung dieser Mail durch Mitglieder des Ortsbeirats zu bewerten. Mit der Information des Arbeitsgebers des Betroffenen haben diese nicht nur den Datenschutz verletzt, sondern auch gegen ihre Verschwiegenheitspflichten aus § 24 Abs. 1 HGO verstoßen. Dies wurde den Beteiligten eingehend vor Augen geführt.

5.5 Vorlage von Scheidungsurteilen bei erneuter Eheschließung

Die Standesämter können bei der Anmeldung der Eheschließung geschiedener Personen nicht die Vorlage eines kompletten Scheidungsurteils verlangen. Vielmehr ist die Vorlage des Tenors der Entscheidung ausreichend.

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, dass die Standesämter bei der Anmeldung einer Eheschließung von geschiedenen Personen die Vorlage eines oder ggf. mehrerer kompletter Scheidungsurteile verlangen, um zu prüfen, ob der Eheschließung ein Ehehindernis entgegensteht. Die Standesämter stützen dieses Begehren auf § 5 Abs. 2 PStG i.V.m. § 159 Abs. 2 Nr. 2 der Dienstanweisung für Standesbeamte.

§ 5 Abs. 1 und 2 PStG

(1) Die Verlobten haben bei der Anmeldung der Eheschließung dem Standesbeamten ihre Abstammungsurkunden, beglaubigte Abschriften des Familienbuchs oder Auszüge aus diesem vorzulegen.

(2) Der Standesbeamte hat zu prüfen, ob der Eheschließung ein Ehehindernis entgegensteht. Reichen die nach Abs. 1 vorgelegten Urkunden nicht aus, so hat der Standesbeamte weitere Urkunden zu fordern.

§ 159 Abs. 2 Nr. 2 der Dienstanweisung für Standesbeamte

Wer verheiratet war oder eine Lebenspartnerschaft begründet hatte, hat alle früheren Ehen und Lebenspartnerschaften und die Art der Auflösung anzugeben. Die Auflösung der letzten Ehe oder Lebenspartnerschaft muss er nachweisen, bevor er eine neue Ehe eingehen kann. Dies gilt auch, wenn das Nichtbestehen einer Ehe oder Lebenspartnerschaft gerichtlich festgestellt ist. Als Nachweis dienen
…
2. eine mit dem Zeugnis der Rechtskraft versehene Ausfertigung der Entscheidung eines deutschen Gerichts über die Scheidung, die Aufhebung, die Nichtigerklärung oder das Nichtbestehen der Ehe oder die Aufhebung der Lebenspartnerschaft.

In dem mir vorgetragenen Fall stammte das Scheidungsurteil aus einer Zeit, in der noch das Verschuldensprinzip bei Ausspruch der Ehescheidung Geltung hatte. Derartige Urteile enthalten in der Regel eine Fülle höchst sensibler personenbezogener Daten, die für die Beurteilung der Frage, ob ein Ehehindernis der Eheschließung entgegensteht oder nicht, von keiner Relevanz sind. Entscheidend ist, dass keine gültige Ehe mehr besteht. Dieser Nachweis kann auch durch die Vorlage eines beglaubigten Tenors der Gerichtsentscheidung erbracht werden. Diese Auffassung wurde auch vom hessischen Innenministerium geteilt, das für das Personenstandswesen zuständig ist. Ich habe das Ministerium gebeten, bei der derzeit anstehenden Überarbeitung der Dienstanweisung für Standesbeamte auf eine Konkretisierung des § 159 Abs. 2 Nr. 2 in diesem Sinne hinzuweisen.

6. Stiftungsaufsicht

6.1 Hessisches Stiftungsverzeichnis

Mit der im September 2007 in Kraft getretenen Änderung des Hessischen Stiftungsgesetzes wurde die Bereitstellung auch von personenbezogenen Daten zu Hessischen Stiftungen im Internet ermöglicht. Bei der Entwicklung des IT-Verfahrens zum Abruf der Daten durch die Öffentlichkeit und die Stiftungsaufsicht habe ich darauf hingewirkt, dass datenschutzrechtliche Belange berücksichtigt und das Persönlichkeitsrecht beeinträchtigende Auswirkungen der Veröffentlichung im Internet weitgehend vermieden werden.

Im Jahr 2007 hatte ich mich im Gesetzgebungsverfahren zur Änderung des HStiftG gegen eine Aufnahme der Namen für die Stiftung vertretungsberechtigter Personen in den Datenkatalog ausgesprochen, der im Internet zur Einsicht bereitgestellt wird (§ 17a Abs. 3 i.V.m. Abs. 2 Nr. 6).

§ 17a Abs. 1 bis 3 HStiftG

(1) Für Stiftungen im Sinne dieses Gesetzes führen die Aufsichtsbehörden ein Stiftungsverzeichnis.

(2) In das Stiftungsverzeichnis sind einzutragen:
1. der Name der Stiftung,
2. die Rechtsnatur der Stiftung,
3. der Sitz der Stiftung,
4. der Zweck der Stiftung,
5. die Anschrift der Stiftung,
6. die vertretungsberechtigten Organe und Personen sowie die Art ihrer Vertretungsberechtigung,
7. das Datum der Anerkennung,
8. die zuständige Aufsichtsbehörde.

Änderungen hat die Stiftung der Aufsichtsbehörde unverzüglich mitzuteilen.

(3) Das Stiftungsverzeichnis ist allgemein zugänglich. Es kann im Internet veröffentlicht werden. Eintragungen im Stiftungsverzeichnis begründen nicht die Vermutung der Richtigkeit.

Hintergrund meines Votums war, dass durch die freie Einstellung der Daten im Internet Beeinträchtigungen des Persönlichkeitsrechts der betroffenen Personen ermöglicht werden. Dies ist z.B. der Fall, wenn die Daten infolge der freien Einstellung ins Internet durch Suchmaschinen recherchierbar sind. Dadurch können Rechte der Betroffenen auf Änderung oder Löschung von Daten nicht sichergestellt werden, weil die Daten im Internet vielfältig verfügbar gehalten bleiben. In diesem Fall können auch dem ursprünglichen Zweck nicht entsprechende Auswertungen nicht verhindert werden (vgl. 36. Tätigkeitsbericht, Ziff. 5.1.2.4).

Der Gesetzgeber hat sich meinem Votum nicht angeschlossen. Bei der (Fort-)Entwicklung des Verfahrens zur Bereitstellung der Daten im Internet war ich beteiligt. Die vom HMDIS in Auftrag gegebene IT-Lösung hat bereits im Ansatz einen Großteil der befürchteten Probleme vermieden: Das Portal-basierte Verfahren führt dazu, dass die bereitgestellten Daten nicht einfach von Suchmaschinen abgegriffen werden können. Die Daten werden nicht wie auf einer Internetseite offen bereitgestellt, sondern die gewünschten Informationen sind erst nach einer Anmeldung einzusehen.

Durch die Gestaltung des Verfahrens und die vorgesehenen Suchabfragen ist sichergestellt, dass dem Zweck der Bereitstellung der Daten nicht entsprechende Abfragen, wie z.B. die Eingabe des Namens einer vertretungsberechtigten Person zur Suche ob die Person mehrere Stiftungen vertritt, nicht möglich sind.

Der Fragebogen, mit dem bei den Stiftungen Angaben zur Aktualisierung des Hessischen Stiftungsverzeichnisses abgefragt werden sowie das Anschreiben hierzu an die Stiftungen, wurden auf meine Anregung hin überarbeitet. Die Pflichtangaben nach § 17a Abs. 2 sind nunmehr von den freiwilligen Angaben deutlich getrennt und für die freiwilligen Angaben wird die ausdrückliche Einwilligung zur Veröffentlichung im elektronischen Stiftungsverzeichnis im Internet eingeholt. Werden freiwillige Angaben gemacht, aber nicht in deren Veröffentlichung eingewilligt, stehen diese Angaben nur der Stiftungsaufsicht zur Verfügung.

Nachfragen zu dem mir übersandten Benutzerhandbuch und zum Verfahrensverzeichnis machten deutlich, dass die im Verfahren vorgesehenen Berechtigungen noch nicht exakt den Rechtsgrundlagen entsprachen. Die obere Stiftungsaufsicht beim HMDIS konnte ihren Aufgaben entsprechend zentrale Auswertungen und Statistiken aus dem Kreis aller hessischen Stiftungen veranlassen. Die regional den jeweiligen Regierungspräsidien zugewiesene Stiftungsaufsicht konnte allerdings nicht nur Daten der ihrer Zuständigkeit unterliegenden Stiftungen verarbeiten, sondern hatte lesenden Zugriff auf alle Daten aller hessischen Stiftungen. Im Zugriff standen nicht nur die ohnehin im Internet jedermann zur Verfügung stehenden Daten des öffentlichen Stiftungsverzeichnisses, sondern sämtliche die Stiftung betreffende Daten, also z.B. auch Daten zur Finanzlage (Jahresrechnung und Vermögensübersicht). Die Erforderlichkeit dieser Zugriffe konnte nicht belegt werden; die Zugriffsrechte sollen deshalb entsprechend eingeschränkt werden. Zum Ende des Berichtszeitraums befand sich die geänderte Verfahrensversion in der Testphase.

Eine Besonderheit weisen die Regelungen im HStiftG bei den Stiftungen mit Sitz in Frankfurt am Main auf: Teile der Stiftungsaufsicht nimmt hier die Stadt Frankfurt am Main wahr. Dies ergibt sich daraus, dass das Regierungspräsidium Darmstadt von der Delegationsmöglichkeit nach § 28 HStiftG durch Ermächtigung vom 16. September 1966 Gebrauch gemacht hat.

§ 28 HStiftG

Das Regierungspräsidium in Darmstadt wird ermächtigt, die Befugnisse des § 12 für Stiftungen, die ihren Sitz in Frankfurt am Main haben, auf den Magistrat der Stadt Frankfurt am Main zu übertragen.

Die Stadt Frankfurt pflegt für Stiftungen mit Sitz in Frankfurt auch die Daten des Stiftungsverzeichnisses nach § 17a. Die Berechtigungen im Verfahren sind so ausgestaltet, dass sowohl das RP Darmstadt als auch die Stadt Frankfurt schreibenden Zugriff auf diese Daten haben.

Nach § 17a Abs. 1 haben die Aufsichtsbehörden das Verzeichnis zu führen. § 28 schafft nur die Rechtsgrundlage für die Delegation der Befugnisse nach § 12 (Unterrichtungs- und Prüfungsrechte) auf die Stadt Frankfurt; das Stiftungsverzeichnis nach § 17a ist nicht erwähnt. Derzeit gibt es keine Rechtsgrundlage für die Einräumung der Berechtigungen für Datenspeicherung und -veränderung der Daten zu Stiftungsverzeichnis an die Stadt Frankfurt - auch wenn die Wahrnehmung der Aufgabe sachgerecht sein mag. Sollte die Aufgabenverteilung weiterhin so gewollt sein, muss das HStiftG entsprechend

geändert werden. Bei der nächsten Änderung, die spätestens mit Ablauf der Befristung des Gesetzes (31. Dezember 2012) erfolgen muss, ist dies zu berücksichtigen.

7. Sonstige Selbstverwaltungskörperschaften

7.1 Rundfunk

7.1.1 Verbesserter Datenschutz bei der Befreiung von der Rundfunkgebührenpflicht

Als Beleg für einen Anspruch auf Befreiung von der Rundfunkgebührenpflicht genügt auch eine Bescheinigung über den Empfang von Sozialleistungen - Antragsteller müssen der GEZ nicht mehr den Sozialleistungsbescheid vorlegen.

Rundfunkteilnehmer mit geringem Einkommen können sich von der Rundfunkgebührenpflicht befreien lassen. Der Personenkreis ist im Rundfunkgebührenstaatsvertrag genau definiert. Antragsberechtigt sind neben Sozialhilfeempfängern u.a. Empfänger von Grundsicherung im Alter und bei Erwerbsminderung, von Sozialgeld oder Arbeitslosengeld II und BAföG-Empfänger, die nicht bei den Eltern leben. Die Anträge werden zentral von der GEZ für die Landesrundfunkanstalten bearbeitet. Nach der bis Ende August 2008 geltenden Fassung des § 6 Abs. 2 RGebStV musste der Antragsteller durch die Vorlage des Sozialleistungsbescheides im Original oder in beglaubigter Kopie die Erfüllung der Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht nachweisen. Die Regelung hat dazu geführt, dass die GEZ über eine in Deutschland einmalige Sammlung von Sozialleistungsbescheiden verfügt. Im Jahr 2007 führte die GEZ laut Geschäftsbericht 2,9 Millionen private befreite Teilnehmerkonten, ca. 50 v.H. davon entfielen auf Sozialhilfe- und Sozialgeldempfänger und Empfänger von Arbeitslosengeld II. Die Sozialleistungsbescheide enthalten eine Vielzahl äußerst sensibler Angaben, wie z.B. über Einkommens- und Vermögensverhältnisse oder Wohnsituation des Antragstellers, die die GEZ auch nach eigener Einschätzung für die Bearbeitung der Befreiungsanträge nicht benötigt.

Aufgrund der Kritik der Landesdatenschutzbeauftragten an diesem Zustand wurde eine Arbeitsgruppe, bestehend aus Vertretern der Landesdatenschutzbeauftragten, der Rundfunkdatenschutzbeauftragten, der Rundfunkreferenten der Landesregierungen sowie Vertretern der Gebührenabteilungen und der Rechtsabteilungen der Landesrundfunkanstalten gebildet, die sich mit einer datenschutzgerechten Gestaltung des Befreiungsverfahrens beschäftigte. Von den Landesdatenschutzbeauftragten wurde auch ein Vertreter meines Hauses in die Arbeitsgruppe entsandt. Die Arbeitsgruppe schlug vor, den Antragstellern alternative datensparsamere Nachweismöglichkeiten für das Vorliegen der Voraussetzungen für eine Befreiung von der Rundfunkgebührenpflicht einzuräumen. Sie empfahl, dem Antragsteller zu gestatten, den Nachweis auch durch eine Bescheinigung des Sozialleistungsträgers, in der dieser lediglich Gewährung und Dauer der Sozialleistung bestätigt, zu führen. Dieser Vorschlag fand Eingang in den Zehnten Rundfunkänderungsstaatsvertrag, der am 1. September 2008 in Kraft getreten ist. Durch Art. 5 (Änderung des Rundfunkgebührenstaatsvertrages) Nr. 1 des Zehnten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge (GVBl. I S. 740, 754) wurde § 6 Abs. 2 RGebStV entsprechend geändert.

§ 6 Abs. 2 RGebStV

Der Antragsteller hat die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht durch Vorlage einer entsprechenden Bestätigung des Leistungsträgers im Original oder die Vorlage des entsprechenden Bescheides im Original oder in beglaubigter Kopie nachzuweisen.

7.1.2 Änderung der "Impressumspflicht" für Beiträge im Offenen Kanal

Eine Beschwerde führte zur Änderung der Impressumspflicht im Offenen Kanal.

Ein Filmamateur, der regelmäßig im Offenen Kanal seine Filme zeigt, störte sich daran, dass er gesetzlich gezwungen war, am Beginn und am Ende jedes Films seinen Namen und seine Anschrift anzugeben. Er fühlte sich dadurch in seiner Sicherheit beeinträchtigt und bat mich, die Vorschrift zu überprüfen.

7.1.2.1 Gleiche Bedingungen für Rundfunkveranstalter und Nutzer eines Offenen Kanals

§ 39 Abs. 2 Satz 4 HPRG a.F. verlangte, dass am Anfang und am Schluss jedes Beitrages im Offenen Kanal Name und Anschrift des Nutzungsberechtigten (d.h. des für die Sendung Verantwortlichen) anzugeben seien. Mit dieser Regelung sollte die presserechtliche Impressumspflicht entsprechend auf Sendungen im Offenen Kanal übertragen werden.

Die Impressumspflicht dient dem Persönlichkeitsschutz des von der Berichterstattung Betroffenen. Er soll problemlos den Verantwortlichen der Sendung identifizieren können, um ggf. zivilrechtliche Ansprüche auf Unterlassung, Widerruf, Sendung einer Gegendarstellung oder Schadensersatz geltend machen zu können. Die Angaben Name und Anschrift des Verantwortlichen liefern dem durch die Sendung Verletzten die notwendige zustellungs- und ladungsfähige Anschrift des für die Rechtsverletzung Verantwortlichen.

Sie erleichtern außerdem eine Beschlagnahme und Einziehung von Beiträgen mit strafbaren Inhalten und eine strafrechtliche Verfolgung des Verantwortlichen.

Schließlich sind die Angaben auch bedeutsam für die mit dem Beitrag im Offenen Kanal verfolgte öffentliche Meinungsbildung. Diese kann nur sachgerecht erfolgen, wenn die Zuschauer feststellen können, wer den Meinungsbildungsprozess initiiert hat und beeinflusst.

Vorschriften, die auf die problemlose Identifizierbarkeit des Verantwortlichen einer Rundfunk- oder Fernsehsendung zielen, sind kein unangemessener gesetzgeberischer Eingriff in dessen Recht auf informationelle Selbstbestimmung.

Für Presseerzeugnisse ist es grundsätzlich unverzichtbar, dass Name und Anschrift des Verantwortlichen auf dem Druckwerk vermerkt sein müssen, um die Identifizierbarkeit zu gewährleisten. Hessen war lange Zeit das einzige Bundesland, in dem das Pressegesetz nur die Angabe des Namens verlangte. Diese Regelung wurde in der Fachliteratur scharf kritisiert. Der hessische Gesetzgeber hat darauf reagiert und den Inhalt der Impressumspflicht um die Anschrift erweitert.

Für Rundunk- und Fernsehsendungen stellt sich die Situation jedoch anders dar. Im Gegensatz zur Presse bedürfen Rundfunkveranstalter und jeder Sendebeitrag im Offenen Kanal einer staatlichen Zulassung, über die gemäß §§ 4, 5 Abs. 1 und 39 Abs. 4 HPRG die Hessische Landesanstalt für privaten Rundfunk und neue Medien entscheidet. Der Veranstalter der Sendung und der Nutzungsberechtigte eines Offenen Kanals sind somit einer zentralen staatlichen Stelle bekannt. Es erschwert die Identifizierung des Verantwortlichen nicht wesentlich, wenn am Anfang oder im Abspann einer im Offenen Kanal ausgestrahlten Sendung lediglich der Name des Nutzungsberechtigten angegeben wird. Sollte sich jemand durch den Beitrag in seinen Rechten verletzt sehen, kann er über die Landesanstalt die für die Rechtsverfolgung notwendige Anschrift erfahren.

Für Rundfunkveranstalter sieht das Hessische Privatrundfunkgesetz genau dieses Verfahren vor: Am Ende des täglichen Programms sind lediglich die Namen des Veranstalters und des verantwortlichen Redakteurs anzugeben. Auf Verlangen muss die Landesanstalt jedem den Namen oder die Firma sowie die Anschrift des von ihr zugelassenen Rundfunkveranstalters mitteilen. Der Veranstalter ist verpflichtet, jedem Name und Anschrift des verantwortlichen Redakteurs mitzuteilen (§ 25 Abs. 1 und 2 HPRG).

Ein Grund für die unterschiedliche Regelung der "Impressumspflicht" für Rundfunkveranstalter und Nutzungsberechtigte von Offenen Kanälen war weder aus den Gesetzesmaterialien noch sonst erkennbar. Wenn für Sendungen von Rundfunkveranstaltern die Angabe des Namens und ein Auskunftsanspruch gegenüber der Landesanstalt für privaten Rundfunk und neue Medien als ausreichend erachtet werden, muss dies auch für Beiträge im Offenen Kanal gelten.

7.1.2.2 Gesetzesänderung

Die Landesregierung und der Hessische Landtag haben meinen Hinweis auf den Wertungswiderspruch im Hessischen Privatrundfunkgesetz und meine Empfehlung, das Gesetz zu ändern, aufgegriffen. § 39 Abs. 2 Satz 4 HPRG ist durch Nr. 9 des Art. 2 (Änderung des Hessischen Privatrundfunkgesetzes) des Gesetz zu dem Zehnten Staatsvertrag zur Änderung rundfunkrechtliche Staatsverträge (Zehnter Rundfunkänderungsstaatsvertrag) und zur Änderung rundfunkrechtlicher Vorschriften vom 10. Juni 2008 (GVBl. I S. 740) geändert worden und lautet nunmehr:

"Der Name des Nutzungsberechtigten ist am Anfang und am Ende jedes Beitrags anzugeben. Auf Verlangen teilt die Landesrundfunkanstalt die Anschrift des Nutzungsberechtigten mit."

Die Landesregierung hat in der Begründung zu ihrem Gesetzentwurf (LTDrucks. 17/45, S. 6) zu Recht angemerkt, dass es dem Nutzer eines Offenen Kanals selbstverständlich unbenommen bleibt, seinen Beitrag mit Namen und Adresse auszustrahlen, wenn er dies möchte.

8. Entwicklungen und Empfehlungen im Bereich der Technik

8.1 Orientierungshilfe Internet

Die Orientierungshilfe Internet der Datenschutzbeauftragten des Bundes und der Länder ist aktualisiert worden; sie beleuchtet neben technischen auch rechtliche Aspekte.

Die "Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" aus dem Jahre 2000 entsprach nicht mehr dem Stand der Technik und musste dringend aktualisiert werden. Eine Arbeitsgruppe des Arbeitskreises "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, in der ich durch eine Mitarbeiterin vertreten war, hat sich dieser Aufgabe angenommen. In Abstimmung mit dem Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde die Orientierungshilfe komplett überarbeitet.

Die Orientierungshilfe erhielt eine neue Struktur. Sie behandelt

- die Planung einer sicheren Internetanbindung,
- Sicherheitsgateways und modulare Erweiterungen,
- Grundschutzmaßnahmen,
- Zusatzmaßnahmen bei der Verarbeitung sensibler Daten und
- Fragen der Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sie zustimmend zur Kenntnis genommen. Die aktuelle Fassung ist in meinem Internetangebot unter www.datenschutz.hessen.de abrufbar.

9. Bilanz

9.1 Online-Durchsuchungen (36. Tätigkeitsbericht, Ziff. 1.3.3 und 4.1)

Über meine grundsätzlichen Bedenken im Zusammenhang mit der Einführung der Online-Durchsuchung hatte ich im letzten Jahr berichtet.

Die breite öffentliche Diskussion im Rahmen der Novellierung des BKA-Gesetzes hat mich in meiner grundsätzlichen Skepsis gegenüber der Online-Durchsuchung bestätigt. Dies gilt zum einen für die Möglichkeiten, eine dazu notwendige Erhebungsbefugnis im Rahmen der Vorgaben der Verfassung für zulässige Eingriffe in Grundrechte der Bürgerinnen und Bürger auszugestalten. Aber auch datenschutzpolitisch halte ich die Online-Durchsuchung weiterhin für fragwürdig.

Die Novellierung des BKA-Gesetzes war - nicht nur wegen der möglichen Einführung der Online-Durchsuchung - mehrmals Gegenstand der Beratungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Die Einschätzung zur Online-Durchsuchung - im Anschluss an die Rechtsprechung des BVerfG - wurde auf der 75. Konferenz nochmals bekräftigt (s. Ziff. 10.4).

Ihre Kritik an dem Entwurf des Bundesinnenministeriums zum BKA-Gesetz haben die Datenschutzbeauftragten mit der Forderung nach "Mehr Augenmaß bei der Novellierung des BKA-Gesetzes" zusammengefasst (s. Ziff. 10.3). Der Gesetzgeber hat leider bei seiner Entscheidung im Dezember die Forderung kaum berücksichtigt.

9.2 Änderungen im Personenstandswesen (36. Tätigkeitsbericht, Ziff. 4.3)

Im letzten Jahr hatte ich über den Stand der technischen Umsetzung der automatisierten Registerführung im Personenstandswesen berichtet. Vorgaben zur konkreten Umsetzung des Gesetzes sollen in der "Verordnung zur Ausführung des Personenstandsgesetzes (Personenstandsverordnung - PStV)" gemacht werden. Diese wurde im Jahr 2008 in verschiedenen Versionen und Entwürfen diskutiert. In der BTDrucks. 713/08 wurde der Entwurfsstand vom 26. September 2008 veröffentlicht und wurde gleichlautend am 28. November im Bundesgesetzblatt verkündet (BGBl. I S. 2263).

Hiervon ausgehend muss ich feststellen, dass der in Hessen erarbeitete Ansatz hinsichtlich der Speicherung von Dokumenten, das "Kombimodell PDF/A plus XML", wobei das PDF-Format das führende Speicherformat ist, nicht favorisiert wurde. Es ist eine Speicherung im XML-Format vorgesehen, mit der zusätzlichen Speicherung eines PDF-Dokumentes. Beurkundungen sind dann die im XML-Format gespeicherten Haupteinträge und Folgebeurkundungen.

§ 9 Personenstandsregister, Registerinhalt

(1) Die nach § 3 Abs. 1 des Gesetzes zu führenden Personenstandsregister bestehen aus Registereinträgen, die auf Dauer lesbar und unveränderbar zu speichern sind.

(2) Die Registereinträge enthalten die für die Beurkundung der Personenstandsfälle nach dem Gesetz erforderlichen Daten einschließlich der dauerhaft überprüfbaren qualifizierten elektronischen Signatur des beurkundenden Standesbeamten sowie die Hinweise und die entsprechenden Registrierungsdaten nach § 16 Abs. 2 Satz 1.

(3) Die Beurkundungsdaten werden vom Standesamt in strukturierter Form im Format Extensible Markup Language (XML) und zusätzlich als Dokument im Format Portable Document-Format (PDF/A) in dem entsprechenden Personenstandsregister gespeichert.

(4) Beurkundungen im Sinne des § 54 des Gesetzes sind die im Format XML gespeicherten Haupteinträge und Folgebeurkundungen.

In der Begründung (A. Allgemeiner Teil, II. Schwerpunkte der Verordnung, 1. Allgemeine Verfahrensbestimmungen, a) Datenformat) wird dargelegt, warum man zu diesem Ergebnis gelangt ist. Konkret wird in den Erläuterungen zu § 9 Abs. 3 und 4 klargestellt, dass die im PDF-Format gespeicherten Dokumente vor allem dazu dienen, die Verfügbarkeit der Registereinträge zu gewährleisten, wenn nicht vorhergesehene Probleme mit dem XML-Format auftreten.

Begründung aus Entwurf der PStV vom 26. September 2008 zu § 9 Abs. 3 und 4

Abs. 3 legt fest, dass die Beurkundungsdaten sowohl im Format XML als auch im Format PDF/A gespeichert werden. Da bisher keine Erfahrungen mit Langzeitspeicherungen vorliegen, ist eine redundante Verwendung unterschiedlicher Dokumentenformate geeignet, Risiken hinsichtlich der dauerhaften Verfügbarkeit von Personenstandsdaten zu minimieren. Eine Kombination der Datenformate XML und PDF/A bei der technischen Ausgestaltung des Registers gewährleistet insbesondere

a) eine langfristige Verfügbarkeit der Registereinträge, auch wenn eines der verwendeten Datenformate zukünftig nicht mehr weiterentwickelt werden sollte,
b) eine fehlerfreie Darstellung der Eintragshistorie in den Registereinträgen,
c) die problemlose Umsetzung zukünftiger Migrationsprozesse,
d) einen zusätzlichen Sicherheitsgewinn durch die Möglichkeit, die beiden Darstellungen eines Registereintrags abzugleichen.

Abs. 4 legt den im Format XML gespeicherten Registereintrag als verbindliche Beurkundung fest. Die im Format PDF/A gespeicherten Registerdaten dienen lediglich Kontrollzwecken, wenn Zweifel an der Integrität der Beurkundungsdaten bestehen, z. B. weil die Signaturprüfung negativ verlaufen ist. Der Vorrang des XML-Dokuments erleichtert im Übrigen den auf XML basierenden strukturierten Datenaustausch.

Auch wenn ich der Begründung nicht in allen Punkten folgen kann, sollte im Ergebnis eine technische Realisierung möglich sein, die den Anforderungen des Gesetzes genügt.

Die von der Hessischen Arbeitsgruppe zur Umsetzung des Gesetzes erarbeiteten Ansätze betrafen nicht nur das Speicherformat. Es wurden auch Vorstellungen zur technischen Registerführung durch einen Dienstleister erarbeitet. Diese Überlegungen sind in ein Projekt eingeflossen, bei dem die ekom21 bis Anfang 2009 ein Verfahren zur automatisierten Registerführung als Pilot erstellen will. Die Anbieter der Fachverfahren werden die Schnittstellen der Anwendungssoftware beisteuern. Ich beabsichtige dieses Verfahren weiter zu begleiten.

9.3 Räumliche Situation der Ausländerbehörde in Fulda (36. Tätigkeitsbericht, Ziff. 5.4.1.3)

In meinem letzten Tätigkeitsbericht hatte ich von Mängeln in der räumlichen Situation bei der Ausländerbehörde der Stadt Fulda berichtet. Die Defizite führten zu ungewollten und nicht zu verhindernden datenschutzrechtlichen Beeinträchtigungen der Besucher. Abhilfe war zugesagt, stand aber noch aus. Nach mehreren Erinnerungen bat mich der Bürgermeister der Stadt Fulda, meine Anforderung nach Beseitigung dieser Mängel zurückzustellen. Er beabsichtige mit dem Landkreis Fulda eine Kooperation nach § 85 Abs. 3 HSOG zur Erfüllung der Aufgaben des Ausländerwesens einzugehen. Deshalb wolle er die ursprünglichen Umbau- und Umräumpläne der Ausländerbehörde der Stadtverwaltung nicht umsetzen.

§ 85 Abs. 3 HSOG

Die Regierungspräsidien können nach Anhörung der beteiligten kreisfreien Städte und Landräte benachbarte Kreisordnungsbehörden zu einem gemeinsamen Kreisordnungsbehördenbezirk zusammenfassen, in dem die Aufgabe der Kreisordnungsbehörden ganz oder teilweise durch einen Oberbürgermeister oder einen Landrat für den gemeinsamen Kreisordnungsbehördenbezirk zu erfüllen sind. Satz 1 gilt entsprechend für die Zusammenfassung von kreisfreien Städten und Landräten mit Gemeinden mit mehr als 50.000 Einwohnern zu gemeinsamen Ordnungsbehördenbezirken. …

Falls die Kooperation zustande komme, würden die Aufgaben der Ausländerbehörde der Stadtverwaltung künftig in den Räumen des Landratsamtes wahrgenommen. Ich bin dieser Bitte nachgekommen. Die Kooperation kam mit Wirkung vom 1. Juli 2008 zustande (s. StAnz. S. 1928). Gegen Ende des Berichtszeitraumes habe ich die Räumlichkeiten des neuen Ordnungsbehördenbezirks, dessen Aufgabenbereich sich auf die Zuständigkeiten der Ausländerbehörden beschränkt, in Augenschein genommen.

Die im Gebäude des Landratsamtes Fulda untergebrachte Ausländerbehörde ist räumlich ausreichend ausgestattet. Die Organisation der Arbeitsabläufe wirkt nun datenschutzrechtlichen Beeinträchtigungen ausdrücklich entgegen.

Damit sind die in meinem letzten Bericht aufgezeigten Mängel obsolet.

9.4 LUSD - Zentrale Lehrer- und Schülerdatenbank (36. Tätigkeitsbericht, Ziff. 5.6.1)

In vorherigen Tätigkeitsbericht hatte ich mich ausführlich mit der zentralen Lehrer- und Schülerdatenbank (LUSD) beschäftigt.

In der Stellungnahme der Landesregierung zu dem Bericht akzeptiert das HKM meine Ausführungen und beschreibt sie als zutreffend.

Die zentrale LUSD soll die Verwaltungsarbeit in den Schulen vereinfachen, den Informationsfluss zwischen den Schulen, Schulämtern und dem Ministerium durch ein landesweites Schulnetz verbessern und durch aktuelle Daten auch die Unterrichtsplanung und Schulentwicklung optimieren. Diesen Anforderungen wurde das Verfahren Ende 2007 aus vielerlei Gründen nicht gerecht. So waren die Schulen und Schulträger nicht ausreichend auf die auf sie zukommenden Aufgaben, die Anbindung an das Schulnetz und die Gestaltung eines sicheren LUSD-Arbeitsplatzes, vorbereitet. Fehlende Sicherheitskonzepte in den Schulen vergrößerten das Problem und der Einsatz einer unausgereiften Software mit erheblichen Mängeln führte letztendlich zu dem bekannten Desaster. Die wichtigsten datenschutzrechtlichen Forderungen für das Jahr 2008 waren die Erstellung von Mustersicherheitskonzepten für Schulen und bei der Fortentwicklung der LUSD 2007 die Integration einer auswertbaren Protokollierung in der LUSD 2008.

Das HKM hatte das neue Programm LUSD 2008 für Mitte 2008 angekündigt. Die Aufgabe, die Mängel in der Software zu beheben, erwies sich aufwändiger und komplexer als erwartet. Im gesamten Berichtsjahr war das HKM damit beschäftigt, das Programm LUSD 2007 zu überarbeiten, um den Schulen ein geeignetes Arbeitsmittel zur Verfügung zu stellen und den o.g. Anforderungen an ein modernes Schulverwaltungssystem gerecht zu werden. Die Integration einer auswertbaren Protokollierung wurde aus Zeitgründen programmtechnisch noch nicht umgesetzt. Sie ist für ein späteres Release vorgesehen.

In meinem 36. Tätigkeitsbericht hatte ich berichtet, dass eine Arbeitsgruppe sich mit der Erstellung von Sicherheitskonzepten befassen sollte. Die Fertigstellung war seinerzeit für Mitte 2008 vorgesehen.

Die Aufgabe wurde der Unterarbeitsgruppe IT-Sicherheit der Medieninitiative "Schule@Zukunft" übertragen, an deren Sitzungen ich beratend teilnahm. Zunächst wurden datenschutzrechtliche Fragen im Umfeld der Schulen und Schulträger

diskutiert. Eine Orientierungshilfe "DV-Dienstleistungen für Schulen durch Schulträger und deren Auftragnehmer (Stand: 22. August 2008) Wartung, Fernwartung und Fernbetreuung" entstand auf Anregung der Arbeitsgruppe und ist unter www.datenschutz.hessen.de (Service - Fachthemen - Datenschutz in Schulen) auf meiner Homepage abrufbar. Die Mustersicherheitskonzepte stehen noch aus.

Zusammenfassend ist festzustellen, dass die im 36. Tätigkeitsbericht beschriebenen datenschutzrechtlichen Mängel und Unzulänglichkeiten nach wie vor vorhanden sind. Das HKM hat mir zugesagt, dass alle meine Forderungen aus 2007 in 2009 erfüllt werden.

9.5 Löschung von Daten im SAP R/3 HR-System (36. Tätigkeitsbericht, Ziff. 5.10.3.2)

Das bereits im Jahr 2005 fertiggestellte Konzept für die Löschung von Bewerberdaten im Bereich des Kultusministeriums wurde bisher immer noch nicht produktiv gesetzt. Die fertiggestellten Programme werden zurzeit getestet. Das HCC geht davon aus, das die Produktivsetzung in Kürze erfolgen kann.

Auch die Löschung von Daten im SAP-Standard ist immer noch nicht möglich. Am 10. September 2008 und am 10. Dezember 2008 hat sich bei der SAP AG der Arbeitskreis "Löschen von Personaldaten im SAP-System im Rahmen von Fristen und Datenschutzvorschriften" getroffen, um zunächst die Anforderungen zu definieren. In diesem Arbeitskreis sind neben Vertretern von Unternehmen auch Vertreter des Landes Hessen und ein Mitarbeiter meines Hauses vertreten. Liegen die Anforderungen vor, wird die SAP AG die technischen Umsetzungsmöglichkeiten prüfen und ein Konzept zur Löschung von Daten erstellen. Der zeitliche Umfang für dieses Projekt kann zum jetzigen Zeitpunkt nicht abgesehen werden.

9.6 Business-Warehouse-HR (HEPISneu) (36. Tätigkeitsbericht, Ziff. 5.10.3.5

In meinem 36. Tätigkeitsbericht habe ich dargestellt, dass nach meiner Auffassung vor der Entwicklung eines Data-Warehouses zunächst die Aufgaben konkret definiert werden müssen und dann in einem ersten Schritt festgelegt werden muss, welche Art von Berichten erstellt werden soll.

Ich habe in diesem Jahr an zahlreichen Sitzungen des Vorprojekts BW/HEPISneu teilgenommen und das Projekt beratend begleitet. Das aus dieser Arbeit resultierende Konzept für ein Data-Warehouse lehnten die Ressorts ab. Deshalb beschloss der Kabinettsausschuss "Verwaltungsreform und Verwaltungsinformatik", 2009 ein neues Projekt zu starten, um ein Data-Warehouse zu konzipieren. Zunächst soll eine fachliche Befragung der Führungsebene der Ressorts durchgeführt werden.

Bis zur Produktivsetzung des Data-Warehouses soll die bisher beim HMDIS auf der Grundlage des § 120 HBG geführte "Personaldatenbank" als Übergangslösung für landesweite bzw. ressortweite Auswertungen genutzt werden. Hierzu soll eine Arbeitsgruppe eingerichtet werden, die ein entsprechendes Konzept erarbeiten soll. Auch an der Erarbeitung dieser Konzeption werde ich mich beratend beteiligen.

9.7 Personalkostenhochrechnung (35. Tätigkeitsbericht, Ziff. 5.9.1.3 und 36. Tätigkeitsbericht, Ziff. 5.10.3.4)

In den beiden Tätigkeitsberichten habe ich über die Problematik des Zugriffs auf Einzelabrechnungsergebnisse der Bediensteten bei der Personalkostenhochrechnung berichtet. Daraufhin wurde ein Projekt "PKPL-Neu" gegründet, das die Aufgabe hatte, die Personalkostenhochrechnung neu zu konzipieren. Ich habe in diesem Projekt mitgearbeitet und die Belange des Datenschutzes eingebracht. In dem Abschlussbericht des Projekts wurde festgestellt, dass aufgrund der unterschiedlichen Definition und Nutzung des Infotypen 9001 (Abordnungen) im SAP R/3 HR-Systems eine Neukonzeption keine Verbesserung des bestehenden Verfahrens darstellen würde, da auch diese kundeneigene Abbildungen der Abordnungen nicht berücksichtigen kann. Das Problem liegt darin, dass im Datensatz das Feld Abordnung unterschiedlich genutzt wird und deshalb landesweite Auswertungen "falsche" Ergebnisse bringen müssen.

Nach meinen Erkenntnissen hat die Gesamtprojektleitung diesen Abschlussbericht bisher nicht beschlossen. Ein neues Konzept für die Personalkostenhochrechnung gibt es nicht; stattdessen wird weiterhin das bisherige datenschutzrechtlich unzulässige Verfahren eingesetzt.

10. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

10.1 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Berliner Erklärung:
Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste

Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

10.2 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Medienkompetenz und Datenschutzbewusstsein in der jungen "Online-Generation"

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge "Online-Generation", die in der Altersgruppe der 14- bis 19-Jährigen zu 96 v.H. regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

   Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto "Datenschutz macht Schule" wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z.B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

   Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema "Datenschutz" aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen - schon im Grundschulalter deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

10.3 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme ("Online-Durchsuchung") in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d.h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z.B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur "Online-Durchsuchung" vom 27. Februar 2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur "Online-Durchsuchung", sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

10.4 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

1. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer "elektronischen Ausforschung" schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von eGovernment- und eCommerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenübersteht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   - Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

   - Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

   - Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

   - Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

   - Für die Durchführung von "Quellen-Telekommunikationsüberwachungen", die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z.B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

10.5 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z.B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft ("fremdbestimmte Selbstauskunft") selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche "Einwilligung des Betroffenen" ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem "Führungszeugnis" dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum "Fragerecht des Arbeitgebers" getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern - neben den in ein "Führungszeugnis" aufzunehmenden Daten - auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem "Führungszeugnis" nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten - über den Umweg über die Polizei oder einen Nachrichtendienst - für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

10.6 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte "Zentralstelle" übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z.B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter "allgemeine Hinweise" gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und -Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe "ins Blaue hinein", also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[1], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.

Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

10.7 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11. März 2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

10.8 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. April 2008

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

[1] RL 2004/82 EG vom 29. April 2004 ABlEG 2004/L 261/24, Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein Datenschutz förderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms "Technologien für die Informationsgesellschaft" gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z.B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

10.9 Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008

Entschlossenes Handeln ist das Gebot der Stunde

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger-Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt - zuletzt in ihrer Berliner Erklärung vom 4. April d.J. - auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden. Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung in die Datenübermittlung zu Werbezwecken zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabschöpfung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragen als Organ der Selbstkontrolle
- Spezialisierung der Strafverfolgungsbehörden
- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig von Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

10.10 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Der auf dem "Datenschutzgipfel" im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die aufgrund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim "Datenschutzgipfel" gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22. Oktober 2008) zieht mit der Einwilligungslösung - bei aller Verbesserungswürdigkeit im Detail - die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

10.11 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Gegen Blankettbefugnisse für die Software-Industrie

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach *"jede natürliche oder juristische Person mit einem berechtigten Interesse"* berechtigt sein soll, Verkehrsdaten zu verarbeiten, um "technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder

privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung" zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die "Informationssicherheit" rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

10.12 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen - grundsätzlich auch alle öffentlichen Stellen - gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

10.13 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Abfrage von Telekommunikationsverkehrsdaten einschränken:

Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotenzial in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. die Entschließung vom 8./9. März 2007; s. mein 36. Tätigkeitsbericht, Ziff. 10.3) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche

Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z.B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von drei Monaten waren nach der Studie 98 v.H. der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substanziierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen - trotz hoher Belastungen in der Praxis - unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist - unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik - unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage - auch im Vergleich zu anderen möglichen Maßnahmen - mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

10.14 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potenzial an volkswirtschaftlichem Nutzen und sind geeignet, vielen eGovernment- und eCommerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben aufgrund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BTDrucks. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

10.15 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.

- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.

- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.

- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten.

- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

- Das Schengener Informationssystem wird weiter ausgebaut, u.a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).

- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.

- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.

- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.

- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 ("Schwedische Initiative") ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z.B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 "Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen"). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die so genannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

- Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

- Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

- Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

- Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

10.16 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Besserer Datenschutz bei der Umsetzung der "Schwedischen Initiative" zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. "Schwedische Initiative") vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der "Schwedischen Initiative" verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln.

- Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,

- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,

- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,

- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,

- vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

- normenklare Bestimmung, welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

10.17 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (BRDrucks. 547/08) sollen u.a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur,

da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1. Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2. Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3. Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

10.18 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BTDrucks. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substanziierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des *technisch-organisatorischen Datenschutzes* noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden (z.B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.

- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.

- Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.

- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.

- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.

- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

10.19 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2008

Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und struktu-

rierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.
Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

- Wenn Versicherte - zu welchem Zeitpunkt auch immer - eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.