16. Wahlperiode

Drucksache **16/6929**

HESSISCHER LANDTAG

21. 02. 2007

Fünfunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2006
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 21. Februar 2007 · Ausgegeben am 7. März 2007
Druck: Druckerei Chmielorz GmbH, 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags, Postfach 3240, 65022 Wiesbaden

INHALTSVERZEICHNIS

Abkürzungsverzeichnis zum 35. Tätigkeitsbericht

a. a. O.	am angegebenen Ort
ABl.	Amtsblatt des Hessischen Kultusministeriums
Abs.	Absatz
AD	Active Directory
AEAO	Anwendungserlass zur Abgabenordnung
AG	Arbeitsgruppe
AK	Arbeitskreis
AK Technik	Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder
AK Steuer	Arbeitskreis Steuer der Datenschutzbeauftragten des Bundes und der Länder
ALG II	Arbeitslosengeld II
AMG	Arzneimittelgesetz
AO	Abgabenordnung
ArchivG	Archivgesetz
ARGE	Arbeitsgemeinschaft
ATDG	Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz)
AufenthG	Aufenthaltsgesetz
BA	Bundesagentur für Arbeit
BDSG	Bundesdatenschutzgesetz
Bf.	Beschwerdeführer
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKAG	Bundeskriminalgesetz
BMB	Biomaterialbanken
BMF	Bundesministerium der Finanzen
BRDrucks.	Bundesratsdrucksache
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
BTDrucks.	Bundestagsdrucksache
BtG	Betreuungsgesetz
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung der Bundesverfassungsgerichtsurteile
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungssammlung des Bundesverwaltungsgerichts
bzgl.	bezüglich
BZSt	Bundeszentralamt für Steuern
bzw.	beziehungsweise
ca.	circa
CNIL	**C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés
CSIS	Zentrales Schengener Informationssystem
DGH	Deutsche Hämophiliegesellschaft zur Bekämpfung von Bluterkrankungen e. V.
d.h.	das heißt
d. J.	dieses Jahres
DHR	Deutsches Hämophilieregister
DIN	Deutsche Industrie-Norm(en)
DMS	**D**okumenten**m**anagement**s**ystem
DNA	Desoxyribonucleinacid (Desoxyribonucleinsäure)
DNS	**D**omain-**N**ame-**S**ystem
DOMEA	**Do**kumenten-**M**anagement-(**S**ystem) **e**lektronische **A**rchivierung; Produkt der Firma Open Text eGovernment Deutschland GmbH
DSB-Konferenz	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DV	Datenverarbeitung
DVBl.	Deutsches Verwaltungsblatt
DV-Geräte	Datenverarbeitungsgeräte
EDPS	**E**uropean **D**ata **P**roctection **S**upervisor
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
ELENA	Einführung des **el**ektronischen **E**inkommens**na**chweises
EStG	Einkommensteuergesetz
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
Eurojust	Europäische Stelle zur justiziellen Zusammenarbeit
EUROPOL	Europäisches Polizeiamt
EU-Richtlinie	Richtlinie der Europäischen Union
evtl.	eventuell
EWO-Datei	Einwohnerdatei

ff.	fortfolgende/r/s
FGO	Finanzgerichtsordnung
GERVA	**G**esicherter **e**lektronischer **R**echts**v**erkehr mit **A**ttributen; Produkt der DATEV eG
GG	Grundgesetz
ggf.	gegebenenfalls
GK	Gemeinsame Kontrollinstanz
GTH	Gesellschaft für Thrombose- und Hämostaseforschung e. V.
GVBl.	Gesetz- und Verordnungsblatt
HBG	Hessisches Beamtengesetz
HBS	Hessische Bezügestelle
HCC	Hessisches Competence Center
HCN	**H**essen **C**orporate **N**etwork
HDO	Hessische Disziplinarordnung
HDG	Hessisches Disziplinargesetz
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HGO	Hessische Gemeindeordnung
HKM	Hessisches Kultusministerium
HLKA	Hessisches Landeskriminalamt
HMDF	Hessisches Ministerium der Finanzen
HMDIS	Hessisches Ministerium des Innern und für Sport
HMDJ	Hessisches Justizministerium
HMG	Hessisches Meldegesetz
HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HMWVL	Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung
HSB AO	Hauptsachbearbeiter/in Abgabenordnung
HSchulG	Hessisches Schulgesetz
HSGL AO	Hauptsachgebietsleiter/in Abgabenordnung
HSM	Hessisches Sozialministerium
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HUIG	Hessisches Umweltinformationsgesetz
HVG	Hessisches Vermessungsgesetz
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. d. F.	in der Fassung
ID-Nummer	Identifikationsnummer
i. d. R.	in der Regel
IFG	Informationsfreiheitsgesetz
IfSG	Infektionsschutzgesetz
IGH	Interessengemeinschaft Hämophiler e. V.
INPOL	Informationssystem der Polizei
Interpol	Internationale kriminalpolizeiliche Organisation
i. S. d.	im Sinne des/der
i. S. v.	im Sinne von
IT	**I**nformations**t**echnik
i. V. m.	in Verbindung mit
IWG	Informationsweiterverwendungsgesetz
IZEMA	**I**ntegriertes **Ze**it**ma**nagementsystem
Kfz	Kraftfahrzeug
Kfz-Daten	Kraftfahrzeugdaten
Kfz-Kennzeichen	Kraftfahrzeugkennzeichen
KIV	Kommunale Informationsverarbeitung in Hessen
KJHG	Kinder- und Jugendhilfegesetz
KWG	Kommunalwahlgesetz oder Gesetz über das Kreditwesen
KWO	Kommunalwahlordnung
LfDs	Landesbeauftragte für den Datenschutz
LIS	Landesinformationsstelle Sporteinsätze
LRS	Lese- und Rechtschreibschwäche
LTDrucks.	Landtagsdrucksache
m. E.	meines Erachtens
MDK	Medizinischer Dienst der Krankenversicherung
MESTA	Mehrländer-Staatsanwaltschafts-Automation
NVS	Neue Verwaltungssteuerung
OFD	Oberfinanzdirektion
o. g.	oben genannte/r/s
OLG	Oberlandesgericht
ORDB	Open Relay Database
PEI	Paul-Ehrlich-Institut
PICA	vernetztes Bibliotheksverwaltungsprogramm der holländischen Stiftung PICA
PIN	**P**ersönliche **I**dentifikations**n**ummer

PKI	**P**ublic **k**ey **i**nfrastructure
Pkw	Personenkraftwagen
POLAS-HE	Polizeiliches Auskunftssystem Hessen
popgen	Populationsrepräsentative Bevölkerungsstichprobe und Krankheitskohorte
PPP	Public Private Partnership
RFID	**R**adio **f**requency **id**entification
s.	siehe
S.	Seite
SAP R/3	In der Hessischen Landesverwaltung eingesetzte Standardsoftware zur Unterstützung betriebswirtschaftlicher Funktionen wie z.B. internes und externes Rechnungswesen, Materialwirtschaft und Personalverwaltung
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SID	Screening-ID
SigG	Signaturgesetz
SigV	Signaturverordnung
SIS	Schengener Informationssystem
SIT (Fraunhofer-)	(Fraunhofer Institut für) **S**ichere **I**nformations-**T**echnologie
SMS	System Management Server
sog.	sogenannte/r/s
SpD	Sozialpsychiatrischer Dienst
StAnz.	Staatsanzeiger
StDüV	Steuerdatenübermittlungsverordnung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
TFG	Transfusionsgesetz
TKG	Telekommunikationsgesetz
TMF	Telematikplattform für medizinische Forschungsnetze
u.a.	unter anderem
u. Ä.	und Ähnliches
u. U.	unter Umständen
UStG	Umsatzsteuergesetz
VerfSchG	Verfassungsschutzgesetz
vgl.	vergleiche
VIS	Visa-Informationssystem
VO	Verordnung
VwGO	Verwaltungsgerichtsordnung
WM	Weltmeisterschaft
z.B.	zum Beispiel
Ziff.	Ziffer
ZIS	Zentrale Informationsstelle Sporteinsätze
ZPO	Zivilprozessordnung

Register der Rechtsvorschriften

AMG	Gesetz über den Verkehr mit Arzneimitteln (Arzneimittelgesetz - AMG) i. d. F. der Bekanntmachung vom 12. Dezember 2005 (BGBl. I S. 3394), zuletzt geändert durch Art. 12 des Gesetzes vom 14. August 2006 (BGBl. I S. 1869)
AO	Abgabenordnung 1977 vom 16. März 1976 (BGBl. I S. 613), zuletzt geändert durch Art. 10 des Gesetzes vom 13. Dezember 2006 (BGBl. I S. 2878)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz - AufenthG) vom 30. Juli 2004 (BGBl. I S. 1950), zuletzt geändert durch Art. 2 des Gesetzes vom 7. Dezember 2006 (BGBl. I S. 2814)
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtsgesetz - BKAG) vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Art. 4 des Gesetzes vom 22. Dezember 2006 (BGBl. I S. 3416)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz - BZRG). Neugefasst durch Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Art. 2 des Gesetzes vom 17. Dezember 2006 (BGBl. I S. 3171)
EU-Richtlinie 1999/93/EG	EU-Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über Gemeinschaftliche Rahmenbedingungen für elektronische Signaturen Amtsblatt der Europäischen Gemeinschaften vom 19. Januar 2000 (ABl. L 13, S. 12)
EUROPOL-Abkommen	Übereinkommen auf Grund von Art. K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (EUROPOL-Übereinkommen) vom 26. Juli 1995 (ABl. der EG Nr. C 316/25), ergänzt durch Beschluss des Rates vom 3. Dezember 1998 (ABl. der EG 1999 Nr. C 26, S. 21)
FGO	Finanzgerichtsordnung vom 6. Oktober 1965 (BGBl. I S. 1477), zuletzt geändert durch Art. 10 des Föderalismusreform-Begleitgesetzes vom 5. September 2006 (BGBl. I S. 2098)
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten vom 25. Oktober 1993 (BGBl. I S. 1770), zuletzt geändert durch Art. 11 des Gesetzes vom 15. Dezember 2003 (BGBl. I S. 2676)
Gemeinsame-Dateien-Gesetz	Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder vom 22. Dezember 2006 (BGBl. I S. 3409)
GewO	Gewerbeordnung vom 21. Juni 1869 i. d. F. der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), zuletzt geändert durch Art. 144 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. I S. 1), zuletzt geändert durch das Gesetz vom 28. August 2006 (BGBl. I S. 2034)
HDG	Hessisches Disziplinargesetz vom 21. Juli 2006 (GVBl. I S. 394)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 7. Januar 1999 (GVBl. I S. 98)
HGO	Hessische Gemeindeordnung i. d. F. vom 1. April 2005 (GVBl. I S. 142), geändert durch Art. 7 Zweites Verwaltungsverfahrensrechts-ÄndG vom 21. März 2005 (GVBl. I S. 218), Art. 12 KommunalisierungsG vom 21. März 2005 (GVBl. I S. 229) und Art. 32b Drittes VerwaltungsstrukturreformG vom 17. Oktober 2005 (GVBl. I S. 674)
HMG	Hessisches Meldegesetz in der Neufassung vom 10. März 2006 (GVBl. I S. 66)

HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i. d. F. vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Art. 3 des Gesetzes vom 17. Oktober 2005 (GVBl. I S. 676)
HSchulG	Hessisches Schulgesetz i. d. F. vom 14. Juni 2005 (GVBl. I S. 442), zuletzt geändert durch Gesetz vom 13. Juli 2006 (GVBl. I S. 386)
HUIG	Hessisches Umweltinformationsgesetz vom 14. Dezember 2006 (GVBl. I S. 659)
HVG	Hessisches Gesetz über das Liegenschaftskataster und die Landesvermessung vom 2. Oktober 1992 (GVBl. I S. 453) i. d. F. vom 20. Dezember 2004 (GVBl. I S. 506)
HVwVfG	Hessisches Verwaltungsverfahrensgesetz i. d. F. vom 28. Juli 2005 (GVBl. I S. 591)
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes vom 5. September 2005 (BGBl. I S. 2722)
IfSG	Infektionsschutzgesetz vom 20. Juli 2000 (BGBl. I S. 1045), zuletzt geändert durch Art. 57 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
IWG	Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen vom 13. Dezember 2006 (BGBl. I S. 2913)
Kirchenaustrittsgesetz	Gesetz betreffend den Austritt aus den Religionsgesellschaften öffentlichen Rechts vom 30. November 1920 i. d. F. des Gesetzes zur Vereinheitlichung der Verfahrensvorschriften über den Austritt aus einer öffentlich-rechtlichen Religionsgesellschaft vom 31. Mai 1974 (GVBl. I S. 281)
KWG	Hessisches Kommunalwahlgesetz i. d. F. vom 1. April 2005 (GVBl. I S. 197)
KWG	Kreditwesengesetz in der Neufassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 1 des Gesetzes vom 17. November 2006 (BGBl. I S. 2606)
KWO	Hessische Kommunalwahlordnung i. d. F. vom 26. März 2000 (GVBl. I S. 233), zuletzt geändert durch Art. 1 der Siebten Verordnung zur Änderung der Kommunalwahlordnung vom 23. März 2005 (GVBl. I S. 254)
MeldDÜVO	Meldedatenübermittlungsverordnung vom 6. Juli 2006 (GVBl. I S. 427)
ÖPP-Beschleunigungsgesetz	Gesetz zur Beschleunigung der Umsetzung von Öffentlich Privaten Partnerschaften und zur Verbesserung gesetzlicher Rahmenbedingungen für Öffentlich Private Partnerschaften vom 1. September 2005 (BGBl. I S. 2676)
Prümer Vertrag	Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich Niederlande und der Republik Österreich vom 27. Mai 2005
SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juli 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. Juli 1990 – Schengener Durchführungsübereinkommen (BGBl. II 1993 S. 1013)
SBG IV	Viertes Buch Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung (Art. I des Gesetzes vom 23. Dezember 1976, BGBl. I S. 3845), zuletzt geändert durch Art. 3 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)
SBG VII	Siebtes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung - vom 7. August 1996 (BGBl. I S. 1254), zuletzt geändert durch Art. 260 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)

SBG VIII	Achtes Buch Sozialgesetzbuch - Kinder und Jugendhilfe - i. d. F. der Bekanntmachung vom 8. Dezember 1998 (BGBl. I S. 3546), zuletzt geändert durch Art. 1 des Gesetzes vom 8. September 2005 (BGBl. I S. 2729)
SBG X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - i. d. F. vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch die Neunte Zuständigkeitsanpassungsverordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
SBG XI	Sozialgesetzbuch (SGB) Elftes Buch (XI) - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014), zuletzt geändert durch Art. 264 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes vom 20. April 1994 (BGBl. I S. 867), zuletzt geändert durch Art. 3 der Verordnung vom 25. November 2003 (BGBl. I S. 2304)
SigG	Signaturgesetz, Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 3 Abs. 9 durch das Zweite Gesetz zur Neuregelung des Energiewirtschaftsrechts vom 7. Juli 2005 (BGBl. I S. 1970, 2013)
SigV	Signaturverordnung, Verordnung zur elektronischen Signatur vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Art. 2 des Ersten Gesetzes zur Änderung des Signaturgesetzes vom 4. Januar 2005 (BGBl. I S. 2)
StDÜV	Steuerdaten-Übermittlungsverordnung vom 28. Januar 2003 (BGBl. I S. 139), zuletzt geändert durch die Verordnung zur Änderung der Steuerdaten-Übermittlungsverordnung vom 20. Dezember 2006 (BGBl. I S. 3380)
StGB	Strafgesetzbuch i. d. F. der Fassung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch das Zweite Justizmodernisierungsgesetz vom 24. Dezember 2006 (BGBl. I S. 3416)
StPO	Strafprozessordnung i. d. F. vom 7. April 1987 (BGBl. I S. 1074), zuletzt geändert durch Art. 1 des Gesetzes vom 24. Oktober 2006 (BGBl. I S. 2350)
StVG	Straßenverkehrsgesetz vom 19. Dezember 1952 (BGBl. I S. 837), zuletzt geändert durch Art. 2 des Gesetzes vom 14. August 2006 (BGBl. I S. 1958)
StVO	Straßenverkehrsordnung vom 16. November 1970 (BGBl. I S. 1565), zuletzt geändert durch Art. 474 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
TFG	Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz - TFG) vom 1. Juli 1998 (BGBl. I S. 1752), zuletzt geändert durch Art. 36 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 273 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407)
UStG	Umsatzsteuergesetz 1999 i. d. F. vom 9. Juni 1999 (BGBl. I S. 1270), zuletzt geändert durch Art. 7 des Jahressteuergesetzes 2007 vom 13. Dezember 2006 (BGBl. I S. 2878)
VerfSchutzG	Gesetz über das Landesamt für Verfassungsschutz vom 19. Dezember 1990 (GVBl. I S. 753), geändert durch Art. 3 Nr. 4 DatenschutzG-ÄndG vom 5. November 1998 (GVBl. I S. 421) und Art. 1 ÄndG vom 30. April 2002 (GVBl. I S. 82)
Verordnung über die Verarbeitung personenbezogener Daten in Schulen	vom 30. November 1993 (Amtsblatt des Hessischen Kultusministeriums und des Hessischen Ministeriums für Wissenschaft und Kunst Nr. 2/94, S. 114, Berichtigung in ABl. Nr. 4/94, S. 206)

VwGO	Verwaltungsgerichtsordnung i. d. F. der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), zuletzt geändert durch Art. 3 des Gesetzes zur Erleichterung von Planungsvorhaben für die Innenentwicklung der Städte vom 21. Dezember 2006 (BGBl. I S. 3316)
ZPO	Zivilprozessordnung i. d. F. der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202, 2006 I S. 431), zuletzt geändert durch Art. 10 des Zweiten Gesetzes zur Modernisierung der Justiz vom 22. Dezember 2006 (BGBl. I S. 3416)

Kernpunkte

1. Zeitgemäßer Datenschutz ist nur durch ein Gleichgewicht zwischen Datenschutz und Informationszugang zu erreichen. Im Hessischen Datenschutzgesetz sind dazu bereits Ansätze enthalten, die bei der Schaffung eines Hessischen Informationsfreiheitsgesetzes genutzt werden sollten (Ziff. 1).

2. Kooperationsformen von Hoheitsträgern mit privaten Unternehmen (Public Private Partnerships) verschieben die Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten nicht: soweit der öffentliche Einschlag der Tätigkeiten rechtliche Wirkungen entfaltet, bleibt auch die Kontrollkompetenz des Hessischen Datenschutzbeauftragten bestehen, denn insoweit sind solche Kooperationen dem öffentlichen Bereich zugeordnet (Ziff. 2).

3. Die mit der geplanten Antiterrordatei angestrebte Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten hat verfassungsrechtlichen Vorgaben zu entsprechen. Angesichts der neuen Qualität dieser Zusammenarbeit durch Online-Zugriff auf zentral zur Verfügung stehende Daten entstehen besondere Gefährdungspotenziale für das Recht auf informationelle Selbstbestimmung und die Einhaltung des Verhältnismäßigkeitsgrundsatzes (Ziff. 4.1).

4. Auf die Änderungsnotwendigkeit des HSOG hatte bereits der 31. Tätigkeitsbericht hingewiesen. Die Entscheidung des Bundesverfassungsgerichtes zur Verfassungsmäßigkeit der Rasterfahndung bestätigt diesen Standpunkt (Ziff. 4.2).

5. Bei der Prüfung der Datenverarbeitung im Zusammenhang mit der Fußball-WM konnte ich feststellen, dass personenbezogene Daten im Wesentlichen in dem vorher festgelegten Rahmen verarbeitet wurden. Die in der Sicherheitskonzeption als unerlässlich erklärten umfassenden Überprüfungen aller rund um das Ereignis Tätigen sind jedoch nicht lückenlos durchgeführt worden, was Zweifel an der Notwendigkeit der umfänglichen Erhebung aufwirft.
   Das Vorhalten und Anbieten der für dieses singuläre Ereignis geschaffenen Infrastruktur durch das BKA sehe ich kritisch, da ich das Konzept nur vor dem Hintergrund der besonderen Lage bei der Fußball-WM für zulässig gehalten habe; das Konzept lässt sich so nicht auf andere Großveranstaltungen übertragen (Ziff. 4.3).

6. Das Recht auf Auskunft über die Speicherung von Daten zur eigenen Person ist höchstpersönlicher Natur. Eine Forderung von Dritten, z.B. Arbeitgebern bei Stellenbewerbungen, ihnen das Ergebnis eines solchen Auskunftsersuchens im Bewerbungsverfahren vorzulegen, ist rechtsmissbräuchlich. Die Praxis von gewerblichen Sicherheitsunternehmen, sich von Bewerbern Selbstauskünfte nach § 29 Abs. 1 HSOG vorlegen zu lassen, stellt einen solchen Missbrauch dar (Ziff. 5.2.2).

7. Im Bereich der medizinischen Forschung stehen Datenschutzfragen im Mittelpunkt, weil häufig höchst sensible personenbezogene Daten verarbeitet werden. Deshalb sind komplizierte Konstellationen datenschutzgerecht zu gestalten. Einerseits muss den Anforderungen an Nachweise in wissenschaftlichen Forschungen genügt werden, andererseits ist für die betroffenen Personen ein möglichst weit gehender Datenschutz zu gewährleisten. Meine Bediensteten haben beratend bei dem Aufbau des deutschen Hämophilieregisters (Ziff. 5.6.1), dem generischen Konzept für Biomaterialbanken (Ziff. 5.6.2) und bei der Lösung von Datenschutzfragen bei der Arzneimittelprüfung (Ziff. 5.6.3) mitgewirkt.

8. Mit der Verwendung von Pflegedokumentationen bei der Durchführung von Qualitätsprüfungen in Pflegeeinrichtungen muss ich mich immer wieder beschäftigen: Pflegedokumentationen dürfen nur soweit zwingend erforderlich für diesen Zweck verwendet werden (Ziff. 5.7.2).

9. Staatliche Einmischungen zugunsten des Kindeswohls sind – angesichts der tragischen Folgen von Betreuungsdefiziten – im vergangenen Jahr ein zentraler Punkt der öffentlichen Diskussion gewesen. Der spezielle kinder- und jugendhilferechtliche Datenschutz steht staatlichen Eingriffen nicht im Wege, sondern hat eine die Förderung des Kindeswohls unterstützende Funktion (Ziff. 5.8.1).

10. So breit wie das Spektrum der kommunalen Tätigkeitsfelder ist auch die Palette der Datenschutzfragen. Kommunen haben ihre automatisierte Datenverarbeitung sehr unterschiedlich strukturiert; es ergeben sich je nach Konstellation typische Datenschutzproblemfelder (Ziff. 6.1). Von der seit 2005 eröffneten Möglichkeit, Parkgebühren u.a. per Handy bezahlen zu lassen, hat die Stadt Wiesbaden Gebrauch gemacht. Wenn die Löschfristen im Verfahren ordnungsgemäß umgesetzt werden, genügt das Verfahren datenschutzrechtlichen Anforderungen (Ziff. 6.4).

11. Am Beispiel von Installationen im Fuldaer Stadtschloss, die zu Bürgerbeschwerden führten, wird deutlich, dass Videoüberwachung die Freiheitsrechte beeinträchtigt, weil sie menschliches Verhalten beeinflussen kann. Dies gilt auch dann, wenn nur der Anschein einer Videoüberwachung geweckt wird. Im Übrigen muss auf Videoüberwachung deutlich hingewiesen werden (Ziff. 6.6).

12. Eine Aufzeichnung von Telefongesprächen bei einer Sparkasse erfordert – auch bei Einwilligung des Personalrats der betroffenen Bediensteten des Call-Centers – die wirksame Einwilligung der Gesprächspartner. Dies setzt die Freiwilligkeit und die hinreichende Aufklärung über die Speicherung und

deren Zweck voraus. Auch eine freiwillige Aufzeichnung ist nur zulässig, wenn sie für den damit verfolgten Zweck erforderlich ist (Ziff. 7.2.1).

13. Hinsichtlich der Weiterentwicklung und Umsetzung des Konzeptes der zentralen DV in der Landesverwaltung hat eine Prüfung ergeben, dass es noch Schwachstellen gibt, die insbesondere die Möglichkeit eines Zugriffs der Administration auf den E-Mail-Verkehr betreffen. Für die Anforderungen einer verschlüsselten Ablage von Dokumenten und für die Signaturen beim Einsatz von Terminalservern stehen Lösungen noch aus (Ziff. 8.1). Auch der Einsatz zentraler Spam-Filter wirft datenschutzrechtliche Probleme auf (Ziff. 8.2).

14. Am Beispiel des ElsterOnline-Portals lässt sich aufzeigen, welches Verständnis von technischen Verfahren und deren Auswirkungen gefordert ist, wenn es um die Auswahl der richtigen Lösungen zur Umsetzung von rechtlichen Anforderungen geht. Mit der Verwendung von Authentisierungsschlüsseln wird nur sichergestellt, dass die Person tatsächlich diejenige ist, mit der kommuniziert werden soll. Soll ein in der Kommunikation übermitteltes Dokument inhaltlich unverändert sein und rechtsverbindlich einer bestimmten Person zugeordnet werden, ist die Signatur, nicht die Authentisierung, das einzusetzende Verfahren (Ziff. 4.4).

1. Einführung

1.1 Allgemeines

Datenschutz ist ambivalent. Einerseits dient er dazu, persönliche Daten vor den sprunghaft wachsenden technischen Zugriffsmöglichkeiten des Staates oder unbefugter Dritter abzuschirmen. Andererseits sind Informationen unter den heutigen Lebensbedingungen "Rohstoff" nicht nur der Produktion, sondern auch der Macht (vgl. Friedrich Schoch, Das Recht auf Zugang zu staatlichen Informationen, in: Die Öffentliche Verwaltung 2006, 1 ff.). Dass der Staat auf diesen Rohstoff zugreift und den Zugriff im Interesse einer effektiven Aufgabenerfüllung optimiert, liegt nahe. Hessen, Stammland und Vorreiter des Datenschutzes, prescht insoweit auch mit der Einführung von eGovernment vor, droht aber bei der Entwicklung der informatorischen Zivilgesellschaft zurückzufallen. In Anknüpfung an die Ausführungen unter Ziff. 2.1.2 meines 34. Tätigkeitsberichts beginnt der vorliegende Tätigkeitsbericht daher mit allgemeinen Ausführungen zu den Hauptstoßrichtungen eines zeitgemäßen Datenschutzes und zu jüngsten Entwicklungen des Datenschutzrechts. Die Rechtsentwicklung gibt weiterhin Anlass, die Anmerkungen der vorangegangenen Tätigkeitsberichte zur Rechts- und Aufgabenstellung und zur Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten fortzuschreiben. Sodann folgen Überblicke über die Entwicklungen des Datenschutzes auf europäischer Ebene und auf der Ebene des Bundes. Richtungweisend für die Entwicklung des Datenschutzrechts auch in Hessen ist hier namentlich die Rechtsprechung des BVerfG zur Rasterfahndung. Den Schwerpunkt dieses Tätigkeitsberichts bilden landesspezifische datenschutzrechtlich relevante Fragestellungen im Bereich der Justiz, der Polizei, Strafverfolgung und des Verfassungsschutzes, des Verkehrswesens, der Schulen und Schulverwaltung, der Forschung, des Gesundheitswesens, des Sozialwesens, des Personal- und Finanzwesens, der Kommunen und sonstigen Selbstverwaltungskörperschaften sowie der Sparkassen. Ferner werden die Entwicklungen und Empfehlungen im Bereich der Technik und Organisation dargestellt. 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 Defensiver Datenschutz

Das Grundgesetz und die Verfassung des Landes Hessen enthalten kein spezielles Grundrecht auf Datenschutz. Angesichts der mit den technischen Möglichkeiten einer automatisierten Datenverarbeitung einhergehenden Gefährdungslage hat das BVerfG im Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1) jedoch bekanntlich aus dem allgemeinen Persönlichkeitsrecht das Grundrecht auf informationelle Selbstbestimmung entwickelt. Das BVerfG führte aus, die freie Entfaltung der Persönlichkeit setze unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz sei vom Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG umfasst. Damit war faktisch ein eigenständiges Grundrecht auf Datenschutz aus der Taufe gehoben. Das Grundrecht auf informationelle Selbstbestimmung ist freilich nicht grenzenlos gewährleistet. Art. 2 Abs. 1 GG ist auch in Kombination mit Art. 1 Abs. 1 GG beschränkbar. Allerdings bestehen für die Grundrechtseinschränkung höhere Rechtfertigungsanforderungen als bei der allgemeinen Handlungsfreiheit. Einschränkungen der informationellen Selbstbestimmung bedürfen einer gesetzlichen Grundlage, aus der sich Voraussetzungen und Umfang der Beschränkungen klar und für die Betroffenen erkennbar ergeben (Gebot der Normenklarheit). Ferner setzt der Grundsatz der Verhältnismäßigkeit dem staatlichen Handeln Grenzen, die sich an der Eingriffsintensität des Datenzugriffs ausrichten. Schließlich muss jedem Datenzugriff eine klar definierte Zweckbestimmung vorangehen. Belanglose personenbezogene Informationen gibt es unter den Bedingungen moderner Datenverarbeitung nicht. Jede Datenverarbeitung ist insoweit als Eingriff zu verstehen. Der Schutz der informationellen Selbstbestimmung dient der Abwehr von solchen Eingriffen, ist also defensiv. Mit dieser Stoßrichtung wurde das Volkszählungs-Urteil in der Folgezeit weiterentwickelt und verfeinert. Über die Entscheidungen vom 3. März 2004 (BVerfGE 109, 279; 110, 33) zum sog. Lauschangriff habe ich in meinem 33. Tätigkeitsbericht, über das Urteil vom 27. Juli 2005 (BVerfGE 113, 348) zur präventiven Telekommunikationsüberwachung habe ich im 34. Tätigkeitsbericht, jeweils unter Ziff. 4.1 berichtet. In diesen Sachzusammenhang gehört auch der Beschluss des BVerfG vom 12. April 2005 zur Beschlagnahme von Datenträgern in einer Anwaltskanzlei (BVerfGE 113, 29). In den vorliegenden Berichtszeitraum fällt der Beschluss des BVerfG vom 4. April 2006 zur Verfassungsmäßigkeit der Rasterfahndung in Nordrhein-Westfalen, dessen Bedeutung für das hessische Polizeirecht unten unter Ziff. 4.2 beleuchtet wird.

1.3 Datenzugangsschutz

Der Datenschutz, verstanden als Gewährleistung der Teilhabe am "Rohstoff" Information ist bereits in § 1 Abs. 1 Nr. 2, § 24 Abs. 2 Satz 1, § 29 Abs. 1 HDSG angelegt, wonach der Hessische Datenschutzbeauftragte darauf zu achten hat, dass die automatisierte Datenverarbeitung nicht zu einer Verschiebung der informationellen Gewaltenteilung im innerstaatlichen Bereich führt. Die Konsequenzen für das Staat-Bürgerinnern/Bürger-Verhältnis hat der Landesgesetzgeber noch nicht gezogen, obwohl sich die Bedeutung der Informationszugangsfreiheit in einem freiheitlichen und demokratischen Gemeinwesen immer deutlicher abzeichnet. Schon im Beschluss des BVerfG vom 3. Oktober 1969 (BVerfGE 27,71, 81 f.) heißt es hierzu, für die in Art. 5 Abs. 1 Satz 1 GG gewährleistete Informationsfreiheit seien zwei Komponenten wesensbestimmend: "Einmal ist es der Bezug zum demokratischen Prinzip des Art. 20 Abs. 1 GG: Ein demokratischer Staat kann nicht ohne freie und möglichst gut informierte öffentliche Meinung bestehen. Daneben weist die Informationsfreiheit eine individualrechtliche, aus Art. 1, 2 Abs. 1 GG hergeleitete Komponente auf. Es gehört zu den elementaren Bedürfnissen des Menschen, sich aus möglichst vielen Quellen zu unterrichten, das eigene Wissen zu erweitern und sich so als Persönlichkeit zu entfalten. Zudem ist in der modernen Industriegesellschaft der Besitz von Informationen von wesentlicher Bedeutung für die soziale Stellung des Einzelnen. Das Grundrecht der Informationsfreiheit ist wie das Grundrecht der freien Meinungsäußerung eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie (vgl. BVerfGE 7, 198 [208]). Erst mit seiner Hilfe wird der Bürger in den Stand gesetzt, sich selbst die notwendigen Voraussetzungen zur Ausübung seiner persönlichen und politischen Aufgaben zu verschaffen, um im demokratischen Staat verantwortlich handeln zu können. Zur Begründung

eines Teilhabegrundrechts an Verwaltungsinformationen ließ sich diese Aussage freilich noch nicht heranziehen. Die Informationsfreiheit galt nur als Abwehrrecht (BVerfGE 103, 44, 60), welches den Staat hindert, den Informationsfluss aus "allgemein zugänglichen Quellen" zu unterbinden. Behördenakten zählten nach herkömmlichem Verständnis nicht dazu. Insoweit hat aber in Deutschland mit dem Inkrafttreten des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes (IFG vom 5. September 2005, BGBl. I S. 2722) am 1. Januar 2006 und mit der Verabschiedung des Gesetzes über die Weiterverwendung von Informationen, öffentlichen Stellen (Informationsweiterverwendungsgesetz - IWG vom 13. Dezember 2006, BGBl. I S. 2913) ein Paradigmenwechsel stattgefunden. Durch das IFG sollen die demokratischen Rechte jedes Einzelnen durch einen allgemeinen und voraussetzungslosen Zugang zu amtlichen Informationen des Bundes unter Berücksichtigung des Daten- und Geheimnisschutzes verstärkt werden (BTDrucks. 15/4493, S. 1). Das IFG knüpft an entsprechende Gesetze in den meisten EU-Mitgliedstaaten an, die sich ihrerseits an dem schon 1766 in Schweden eingeführten Öffentlichkeitsprinzip und dem Freedom of Information Act der USA von 1966 orientieren. In Deutschland haben mittlerweile die Länder Brandenburg, Berlin, Schleswig-Holstein, Nordrhein-Westfalen und das Saarland Informationsfreiheitsgesetze erlassen. Daneben bestehen spezielle Informationszugangsgesetze wie das vom 14. Dezember 2006 (GVBl. I S. 659) verabschiedete Hessische Umweltinformationsgesetz (HUIG). Zweck dieser Gesetze ist es, durch ein umfassendes Informationsrecht das in Akten festgehaltene Wissen und Handeln öffentlicher Stellen unter Wahrung des Schutzes personenbezogener Daten unmittelbar zugänglich zu machen, um über die bestehenden Informationsmöglichkeiten hinaus die demokratische Meinungs- und Willensbildung zu fördern und eine Kontrolle des staatlichen Handelns zu ermöglichen (BVerwG, DVBl. 2006, 1245; BVerwGE 125, 40). Die Informationsfreiheit hat zurückzutreten, wenn ein umfassender Informationsanspruch dem Schutzzweck eines Spezialgesetzes oder dem generellen Schutzzweck des Schutzes persönlicher Daten zuwiderlaufen würde. Die internationale und nationale Rechtsentwicklung läuft somit auf die Anerkennung eines Rechts auf Zugang zu Behördeninformationen zu, das mit Belangen des defensiven Datenschutzes und Geheimnisschutzes kollidieren kann.

1.3.1 Offensiver Datenschutz

Die vorstehenden Ausführungen lassen sich wie folgt zusammenfassen und mit einer rechtspolitischen Anregung verbinden: Sowohl der defensive Datenschutz als auch der Zugang zum "Rohstoff" Information haben ihre Wurzel im allgemeinen Persönlichkeitsrecht. Informationszugangsrechte können mit Belangen des defensiven Datenschutzes kollidieren. Erforderlich wird dann eine Güterabwägung. In diese Abwägung ist der Hessische Datenschutzbeauftragte ohnehin eingebunden. Er hat obendrein bereits nach bestehender Rechtslage auf die informationelle Gewaltenteilung zu achten. Was liegt daher näher, als ihm institutionell auch die Aufgabe Gewährleistung des demokratisch legitimierten und legitimierenden Informationszugangsrechts zu übertragen und ihm im Sinne eines umfassenden offensiven Datenschutzes die Optimierung seiner bereits bestehenden Aufgaben zu ermöglichen? Die Chance, mit dem HUIG einen ersten Schritt in diese Richtung zu tun, wurde vergeben. Die Chance zur Korrektur bietet sich indessen im Zuge der Beratungen eines Hessischen Informationsfreiheitsgesetzes. Sie sollte, wie auch das 15. Wiesbadener Forum Datenschutz "Informationsfreiheit und Datenschutz" vom 8. Juni 2006 ergeben hat, genutzt werden.

Die Broschüre zu dieser Veranstaltung kann bei mir angefordert werden.

2. Datenschutzfragen bei Public Private Partnerships

Bereits in meinem 33. Tätigkeitsbericht habe ich dargelegt, weshalb sich die Kontrollbefugnis des Hessischen Datenschutzbeauftragten auf den gesamten Bereich staatlich gewährleisteter Daseinsvorsorge erstreckt. Wie, in welcher Rechtsform und von wem die Aufgaben der Daseinsvorsorge wahrgenommen werden, ist nachrangig. Daseinsvorsorge bedeutet lediglich, dass öffentlich-rechtliche Grundsätze gelten. Das schließt nicht aus, dass der Staat sich zur Erfüllung seiner Aufgaben Privater und zur eigenen Betätigung der Regelungen im Rahmen öffentlich-rechtlicher Vorgaben des Privatrechts bedient (Verwaltungsprivatrecht). Diese Erwägungen erfassen damit zugleich den gesamten Bereich der sog. Public Private Partnerships (PPP). Das Modell der PPP stammt aus dem angloamerikanischen Rechtskreis und fasste auch in Deutschland Fuß. Als PPP werden beispielsweise so unterschiedliche Projekte wie die Teilprivatisierung der Justizvollzugsanstalt Hünfeld und die Privatfinanzierung von Fernstraßen angesehen. Das Gesetz zur Beschleunigung der Umsetzung von Öffentlich Privaten Partnerschaften und zur Verbesserung gesetzlicher Rahmenbedingungen für Öffentlich Private Partnerschaften vom 7. September 2005 (BGBl. I S. 2676) enthält keine Legaldefinition. Unter der Bezeichnung PPP werden daher die unterschiedlichsten Kooperationsformen von Hoheitsträgern mit privaten Wirtschaftssubjekten zusammengefasst. Im engeren Sinne betrifft das Model der PPP aber die Zusammenarbeit der öffentlichen Hand mit der Privatwirtschaft bei der Erbringung öffentlicher Leistungen, sei es, dass Kultur- und Sporteinrichtungen bis hin zu Großprojekten wie die Sportarena Frankfurt am Main gemischt finanziert werden, sei es, dass Privaten staatliche Ausgleichszahlungen für Verpflichtungen des öffentlichen Dienstes geleistet werden. Soweit der öffentlich-rechtliche Einschlag der Tätigkeiten der PPP Ausnahmen vom europäischen Vergaberecht (vgl. zur "Inhouse"- Rechtsprechung EuGH, Urteil vom 18. November1999, Rs. C-107/98 - Teckal; Urteil vom 7. Dezember 2000, Rs. C 94/9 - ARE Gewässerschutz; Urteil vom 11. Januar 2005, Rs. C-26/03 - Stadt Halle) und Beihilferecht (EuGH, Urteil vom 22. November 2001, Rs. C-53/00 - Ferring; Urteil vom 24. Juli 2003, Rs. C 280/00 Altmark Trans) rechtfertigt, ist der öffentliche Bereich und damit die Kontrollbefugnis des Hessischen Datenschutzbeauftragten eröffnet. Umgekehrt würde eine "Flucht" aus der Kontrolle durch den Hessischen Datenschutzbeauftragten die Berechtigung der Ausnahmen vom europäischen Beihilfe- und Vergaberecht in Frage stellen, weil ohne öffentlich-rechtliche Umhegung für die PPP nur die Maximen ökonomischer Rationalität maßgeblich wären. Das ist jedoch nicht der Zweck von PPP, der in der Begründung zum Gesetz vom 7. September 2005 als eine dauerhafte, "in beiderseitigem Vorteil liegende, dem Gemeinwohl dienende Kooperation zwischen öffentlichen Händen und Privatwirtschaft" umschrieben wird (BTDrucks. 15/5668, S. 10). Damit ist die PPP dem öffentlichen Bereich zugeordnet.

3. Europa

3.1 Gemeinsame Kontrollinstanz für das Schengener Informationssystem

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 Berichtsjahr dar.

Im Berichtszeitraum fanden fünf Sitzungen der Gemeinsamen Kontrollinstanz statt, an der meine Mitarbeiterin als Ländervertreterin teilnahm. Die zehn neuen Beitrittsländer sowie Irland und das Vereinigte Königreich haben noch einen Beobachterstatus, da das Schengener Durchführungsübereinkommen (SDÜ) ihnen gegenüber noch nicht in Kraft gesetzt wurde. Dies gilt auch für die Schweiz, die aufgrund eines Assoziierungsabkommens mit der Europäischen Union an der Schengener Zusammenarbeit teilnimmt. Vergleichbar mit der Bundesrepublik Deutschland hat die Schweiz neben dem Vertreter auf Bundesebene auch einen Vertreter der Kantone in die Gemeinsame Kontrollinstanz entsandt.

Das bisher von sieben Schengenstaaten abgeschlossene Schengen III-Abkommen, der sog. Prümer Vertrag vom 27. Mai 2005, wurde von fast allen Unterzeichnerstaaten ratifiziert. Weitere Staaten wie Italien, Portugal, Slowenien sind am Beitritt interessiert. Parallel dazu gibt es Überlegungen den Vertrag in die Europäische Union zu integrieren. Damit wiederholt sich eine Entwicklung, die bereits beim Schengen-Abkommen festzustellen war und kritisiert wurde: Einige wenige Staaten gehen im Rahmen eines "Laboratoriums" voran, die andern müssen das Regelwerk in toto übernehmen oder bleiben außen vor. Während beim Schengener Informationssystem (SIS) alle Staaten auf einen inhaltlich identischen Datenbestand Zugriff haben, verfolgt der Prümer Vertrag ein anderes Konzept, bei dem der gegenseitige Zugriff auf nationale Datenbanken (Fingerabdrücke, DNA, Fahrzeugregister) eingeräumt wird.

Derzeit ist eine Gruppe der nationalen Datenschutzbehörden auf Anregung der Commission Nationale de l'Informatique et des Libertés (CNIL) dabei, die Implementierung des Prümer Vertragswerks zu begleiten und vor allem datenschutzfreundliche technische Verbesserungen einzubringen. Zu diesem Zweck fand im Juli 2006 ein Treffen beim Bundesbeauftragten für den Datenschutz und Informationsfreiheit statt, an dem ich teilgenommen habe.

3.1.1 Entwicklungen des Schengener Informationssystems

Wichtigstes Thema in der Gemeinsamen Kontrollinstanz war wiederum die Diskussion von Plänen zur Erweiterung des SIS, zum sog. SIS II. Das SIS soll zum einen für einen erweiterten Teilnehmerkreis von mindestens 25 Staaten zuzüglich der Schweiz, Rumänien und Bulgarien ausgelegt werden, allerdings soll es auch neue Funktionen erhalten, um damit effizienter den Interessen der Nutzer dienen zu können.

Inzwischen gibt es gegenüber dem im 33. Tätigkeitsbericht, Ziff. 3.1.2.1 und 34. Tätigkeitsbericht, Ziff. 3.3.1 beschriebenen Stand für das SIS II neue Entwürfe für – säulenbedingt getrennte – Rechtsakte vom Juli 2006 [Vorschlag für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) vom 17. Juli 2006 und Vorschlag für eine Verordnung über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) vom 17. Juli 2006].

Die Gemeinsame Kontrollinstanz hat in einer Arbeitsgruppe, an der ich beteiligt war, eine Stellungnahme zu diesen Vorschlägen erarbeitet. Die wichtigsten Probleme sollen hier genannt werden:

- Eine Verbesserung gegenüber dem von mir im 34. Tätigkeitsbericht, Ziff. 3.3.1, angesprochenen Stand ist bei der datenschutzrechtlichen Kontrolle für das Zentrale Schengener Informationssystem (CSIS) vorgesehen. Da die Kommission nunmehr nicht nur für das Betriebsmanagement des CSIS, sondern auch für die operationelle Handhabung zuständig sein soll, ist für diesen ganzen Bereich die Kontrollzuständigkeit des Europäischen Datenschutzbeauftragten (EDPS) gegeben, der ausdrücklich die Befugnisse aus der Verordnung (EG) 45/2001 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr vom 18. Dezember 2000 (ABl. Nr. L 008 vom 12. Januar 2001) erhält.

  Art. 46 Verordnung EG (45/2001)
  Der EDPS

  a) führt und prüft Beschwerden und unterrichtet die betroffene Person innerhalb einer angemessenen Frist über die Ergebnisse seiner Prüfung,

  b) führt von sich aus oder aufgrund einer Beschwerde Untersuchungen durch und unterrichtet die betroffenen Personen innerhalb einer angemessenen Frist über die Ergebnisse seiner Untersuchungen …

  Art. 47 Abs. 1 Verordnung EG (45/2001)
  Der EDPS kann

  a) betroffene Personen bei der Ausübung ihrer Rechte beraten;

  b) bei einem behaupteten Verstoß gegen die Bestimmungen für die Verarbeitung personenbezogener Daten den für die Verarbeitung Verantwortlichen mit der Angelegenheit befassen und ggf. Vorschläge zur Behebung dieses Verstoßes und zur Verbesserung des Schutzes der betroffenen Personen machen.

  c) …

  d) …

e) die Berichtung, Sperrung, Löschung oder Vernichtung aller Daten, die unter Verletzung der Bestimmungen für die Verarbeitung personenbezogener Daten verarbeitet wurden und die Meldung solcher Maßnahmen an Dritte, denen die Daten mitgeteilt wurden anordnen,

f) die Verarbeitung vorübergehend oder endgültig verbieten …

Die nationalen Datenschutzbeauftragten sind - wie bisher - für die Kontrolle der nationalen Schengener Informationssysteme zuständig. Neu ist, dass die Institution der Gemeinsamen Kontrollinstanz entfällt und durch eine formalisierte Zusammenarbeit der nationalen Datenschutzbeauftragten mit dem EDPS (mindestens zweimal jährliches Treffen, eigene Geschäftsordnung) ersetzt wird.

- Ein offener Punkt ist die in den Entwürfen vorgesehene Nutzung von Fingerabdrücken nicht nur zur Verifikation, sondern auch Identifizierung einer Person. Die Gemeinsame Kontrollinstanz sieht in dieser allgemeinen Formulierung eine Funktionserweiterung des SIS und fordert, dass die Nutzung zur Identifizierung auf die Ausschreibungszwecke begrenzt wird.

  Die Vorschläge der Gemeinsamen Kontrollinstanz wurden in den Rechtsaktsentwürfen (Stand 29. September 2006), auf die sich der Rat in der Sitzung Anfang Oktober einigte, leider nicht berücksichtigt. Im Gegenteil wurde eine aus datenschutzrechtlicher Sicht gravierende Verschlechterung eingefügt. Eine neue Formulierung lässt es erstmals zu, dass auch Nachrichtendienste einen Zugriff auf die Ausschreibungen von Drittstaatsangehörigen zur Einreiseverweigerung im SIS haben.

  Die Öffnung des Schengener Informationssystems für Nachrichtendienste zeigt sich auf nationaler Ebene auch dadurch, dass der Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes (BTDrucks. 16/2991) durch einen neuen Abs. 3 des § 17 BVerfSchG die Ausschreibung zur verdeckten Registrierung nach Art. 99 Abs. 3 SDÜ durch Nachrichtendienste erstmals vorsieht.

  § 17 Abs. 3 Entwurf BverfSchG
  Soweit dies für die Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz, des militärischen Abschirmdienstes und des Bundesnachrichtendienstes erforderlich ist, können diese Behörden eine Person oder eine in Art. 99 Abs. 1 des Schengener Durchführungsübereinkommens genannte Sache im polizeilichen Informationssystem zur Mitteilung über das Antreffen ausschreiben, wenn die Voraussetzungen des Art. 99 Abs. 3 sowie tatsächliche Anhaltspunkte für einen grenzüberschreitenden Verkehr vorliegen. …

3.1.2 Gemeinsame Überprüfung von Ausschreibungen zur verdeckten Registrierung

Die Gemeinsame Kontrollinstanz hat eine Überprüfung von Ausschreibungen nach Art. 99 SDÜ initiiert, die in allen Schengen-Staaten nach gleichen Kriterien durchgeführt wurde.

Art. 99 SDÜ
(1) Daten in Bezug auf Personen oder Fahrzeuge werden nach Maßgabe des nationalen Rechts der ausschreibenden Vertragspartei zur verdeckten Registrierung oder zur gezielten Kontrolle gemäß Abs. 5 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.

Anlass zu der Überprüfung war unter anderem die Feststellung, dass die Anzahl der von den jeweiligen Schengen-Staaten eingegebenen Ausschreibungen sehr unterschiedlich ist. Mit Stand vom 19. Januar 2006 hatte Italien beispielsweise über 10.000 Datensätze, Deutschland ca. 1.100 und die Niederlande keine eingegeben. Es gab weiterhin Behauptungen, diese Ausschreibungskategorien würden von einigen Regierungen auch zur Überwachung von politisch Andersdenkenden wie Gewerkschaftlern, Menschenrechts- oder Umweltaktivisten verwandt.

3.1.2.1 Überprüfung in Hessen

Zur Sicherung der schengenweiten Einheitlichkeit der Prüfung hat die Gemeinsame Kontrollinstanz einen Fragenkatalog erarbeitet, der vom BfDI und von allen LfDs bei der Prüfung des jeweils ihres Zuständigkeitsbereiches unterliegenden Datenbestandes zugrunde gelegt wurde. Es wurde darum gebeten, mindestens 25 v. H. des Datenbestandes der Prüfung zu unterziehen.

In Hessen existierten zum Zeitpunkt meiner Überprüfung 55 schengenweite Ausschreibungen zur polizeilichen Beobachtung. Davon wurden 30 Ausschreibungen der Polizeipräsidien Frankfurt, Südhessen und Westhessen zur näheren Prüfung ausgewählt.

Nach dem Fragenkatalog waren zunächst die nationalen Rechtsgrundlagen, die den schengenweiten Maßnahmen nach Art. 99 Abs. 1 SDÜ zugrunde liegen, zu erheben. Für den Bereich der Strafverfolgung ist dies in Hessen wie auch in den anderen Bundesländern und bei den Bundesbehörden die Regelung des § 163e StPO.

§ 163e stopp

(1) Die Ausschreibung zur Beobachtung anlässlich von polizeilichen Kontrollen, die die Feststellung der Personalien zulassen, kann angeordnet werden, wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat von erheblicher Bedeutung begangen wurde. Die Anordnung darf sich nur gegen den Beschuldigten richten und nur dann getroffen werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Gegen andere Personen ist die Maßnahme zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit dem Täter in Verbindung stehen, oder eine solche Verbindung hergestellt wird, dass die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Täters führen wird und dies auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre.

(2) …

(3) Im Falle eines Antreffens können auch personenbezogene Informationen eines Begleiters der ausgeschriebenen Person oder des Führers eines ausgeschriebenen Kraftfahrzeugs gemeldet werden.

(4) Die Ausschreibung zur polizeilichen Beobachtung darf nur durch den Richter angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Hat die Staatsanwaltschaft die Anordnung getroffen, so beantragt sie unverzüglich die richterliche Bestätigung der Anordnung. Die Anordnung tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem Richter bestätigt wird. Die Anordnung ist auf höchstens ein Jahr zu befristen. § 100b Abs. 2 Satz 5 gilt entsprechend.

Die Ausschreibung zu präventiven Zwecken ergeht dagegen nach dem landesrechtlichen Polizeirecht. In Hessen ist dies § 17 HSOG.

§ 17 HSOG

(1) Die Polizeibehörden können die Personalien einer Person sowie das amtliche Kennzeichen und sonstige Merkmale des von ihr benutzten oder eingesetzten Kraftfahrzeugs im polizeilichen Fahndungsbestand automatisiert zur polizeilichen Beobachtung speichern (Ausschreibung zur Polizeilichen Beobachtung), damit andere Polizeibehörden des Landes, Polizeibehörden und -dienststellen des Bundes und der anderen Länder sowie, soweit sie Aufgaben der Grenzkontrolle wahrnehmen, die Zollbehörden das Antreffen der Person oder des Fahrzeugs melden können, wenn dies bei Gelegenheit einer Überprüfung aus anderem Anlass festgestellt wird.

(2) Die Ausschreibung zur Polizeilichen Beobachtung ist zulässig, wenn

1. die Gesamtwürdigung der Person und ihre bisherigen Straftaten erwarten lassen, dass sie auch künftig Straftaten mit erheblicher Bedeutung begehen wird, oder
2. die Voraussetzungen für die Anordnung einer Observation (§ 15 Abs. 2 Satz 1 und 2) gegeben sind und tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die aufgrund der Ausschreibung gemeldeten Erkenntnisse über Ort und Zeit des Antreffens der Person, etwaiger Begleitpersonen, des Kraftfahrzeugs und der Führerin oder des Führers des Kraftfahrzeugs sowie über mitgeführte Sachen, Verhalten, Vorhaben und sonstige Umstände des Antreffens für die Verhütung von Straftaten mit erheblicher Bedeutung erforderlich sind.

(3) …

(4) Die Ausschreibung darf nur durch die Behördenleitung oder eine von dieser beauftragte Bedienstete oder einen von dieser beauftragten Bediensteten angeordnet werden. Die Anordnung ergeht schriftlich und ist auf höchstens zwölf Monate zu befristen. Sie muss die Person, die ausgeschrieben werden soll, so genau bezeichnen, wie dies nach den zur Zeit der Anordnung vorhandenen Erkenntnissen möglich ist. Spätestens nach Ablauf von jeweils drei Monaten ist zu prüfen, ob die Voraussetzungen für die Anordnung noch bestehen; das Ergebnis dieser Prüfung ist aktenkundig zu machen.

(5) Zur Verlängerung der Laufzeit über zwölf Monate hinaus bedarf es einer richterlichen Anordnung. Für das Verfahren gilt § 39 Abs. 1 mit der Maßgabe, dass das Amtsgericht zuständig ist, in dessen Bezirk die ausschreibende Polizeibehörde ihren Sitz hat.

Bei der Maßnahme geht es also nicht etwa darum, dass nach der Person gezielt oder öffentlich gefahndet wird, um sie zu verhaften, sondern es soll beim zufälligen Antreffen, z.B. bei einer Verkehrs- oder Grenzkontrolle u.a. Ort, Zeit und Anlass festgehalten und der ausschreibenden Stelle übermittelt werden.

Von den geprüften 30 Fällen waren 27 auf § 17 HSOG und drei auf § 163e StPO gestützt.

Es folgte die Frage, inwieweit nicht die eigentliche Zielperson, sondern eine Kontaktperson (in Deutschland s. § 163e Satz 3 StPO) im Fokus der Maßnahme stand. In Hessen war dies bei keinem der geprüften Fälle gegeben. Es wurde immer nach der Zielperson gefahndet.

Weitere Fragen, ob die gespeicherten Daten zutreffend, aktuell und rechtmäßig gespeichert waren, ob die Ausschreibungen für noch erforderlich zu erachten und nicht verfristet sind, waren bezüglich aller geprüften Fälle zu bejahen. Auch die in den drei zitierten Normen unterschiedlich beschriebene Schwere der Fälle bzw. Gesamtwürdigung der Gefährlichkeit der betroffenen Person war in jedem der geprüften Fälle zutreffend. Auch alle erforderlichen richterlichen Anordnungen haben vorgelegen.

Als ergänzende Anmerkungen wurden für Hessen dem BfDI noch folgende Feststellungen übermittelt:

- Die Frist für eine Ausschreibung von einem Jahr wurde in jedem Einzelfall ausgeschöpft. Kürzere Fristen waren nicht verfügt.
- Eine Verlängerung der Frist nach Ablauf eines Jahres war in zwei der 30 Fälle ergangen.

Dieses Ergebnis wurde dem BfDI zur Zusammenfassung mit dem eigenen und den Ergebnissen der Datenschutzbeauftragten der anderen Bundesländer übermittelt.

3.1.2.2 Ergebnis der gemeinsamen Überprüfung für die Bundesrepublik Deutschland

Die Ergebnisse der gemeinsamen Überprüfung hat der BfDI in einem Bericht an die Gemeinsame Kontrollinstanz für die Bundesrepublik Deutschland zusammengestellt. Er wird darüber in seinem nächsten Tätigkeitsbericht berichten. Ich möchte diesem Bericht nicht vorgreifen. Zusammenfassend ist festzustellen, dass die Skala der getroffenen Feststellungen von "keine Beanstandungen" bis "die formellen Voraussetzungen zur Ausschreibung nach Artikel 99 SDÜ lagen in Einzelfällen nicht vor" reicht. Es überwiegen offensichtlich die Fälle ohne Beanstandungen.

3.1.2.3 Gesamtergebnis der schengenweiten Überprüfung

Die Ergebnisse der Überprüfung werden in einem Bericht der Gemeinsamen Kontrollinstanz zusammengestellt, dessen letzte Fassung Ende 2006 noch nicht vorlag.

Unter anderem können folgende Feststellungen getroffen werden:

- Bei der stichprobenhaften Überprüfung wurde keine Ausschreibung zu politisch Andersdenkenden etc. gefunden.
- Die Ausfüllung des Begriffs "außergewöhnlich schwere Straftat" in Art. 99 Abs. 2a SDÜ war unterschiedlich. Dies hängt auch damit zusammen, dass das der Ausschreibung zugrunde liegende nationale Recht große Differenzen aufweist.
- Diejenigen Staaten, die das Verfahren zur Ausschreibung nicht oder nur sehr spärlich geregelt haben, sollten entsprechende Vorschriften erlassen.
- Anzustreben ist eine Harmonisierung der Ausschreibungsgründe und des Verfahrens im nationalen Recht.

3.1.3 Vollzug von Entscheidungen eines Schengen-Staats in einem anderen Land

Die Gemeinsame Kontrollinstanz beschäftigt sich seit einiger Zeit mit dem Antrag eines Bürgers aus einem Drittstaat. Dieser möchte eine rechtskräftige Entscheidung der österreichischen Datenschutzkommission in Frankreich vollziehen lassen. In der Entscheidung der österreichischen Datenschutzkommission wird festgestellt, dass die Löschung der Ausschreibung der Daten des Betroffenen im SIS durch Urteil eines französischen Verwaltungsgerichts ausgesprochen und deshalb zu vollziehen ist.

Rechtsgrundlage für diese komplizierte Konstellation ist Art. 111 SDÜ.

Art. 111 SDÜ
(1) Jeder hat das Recht, im Hoheitsgebiet jeder Vertragspartei eine Klage wegen einer seiner Person betreffenden Ausschreibung, insbesondere auf Berichtigung, Löschung, Auskunftserteilung oder Schadensersatz vor dem nach nationalem Recht zuständigen Gericht oder der zuständigen Behörde zu erheben.

(2) Unbeschadet des Art. 116 verpflichten sich die Vertragsparteien, unanfechtbare Entscheidungen der Gerichte oder Behörden nach Abs. 1 zu vollziehen.

Diese Vorschrift lässt keine andere Interpretation zu, als dass die bestandskräftige Entscheidung oder das rechtskräftige Urteil der Behörde bzw. des Gerichts des einen Schengen-Staats von dem anderen vollzogen werden muss, wenn der Betroffene dies begehrt.

Der der Gemeinsamen Kontrollinstanz vorliegende Fall wird allerdings dadurch noch kompliziert, dass das Urteil des französischen Gerichts, auf das sich die österreichische Datenschutzkontrollinstanz bezieht, noch nicht rechtskräftig ist, die Datenschutzkommission bei Erlass ihrer Entscheidung von dieser Tatsache aber keine Kenntnis hatte.

An diesem Fall zeigt sich, wie wichtig eine gute Kooperation der verschiedenen Institutionen in den jeweiligen Schengen-Staaten gerade auch im Interesse der Betroffenen ist.

3.2 Gemeinsame Kontrollinstanz für EUROPOL

Im Berichtszeitraum fanden fünf Sitzungen der Gemeinsamen Kontrollinstanz statt, an denen meine Mitarbeiterin teilnahm.

Der Vorsitz in der Gemeinsamen Kontrollinstanz (GK) hat von dem Spanier Emilio Aced Félez zu dem Delegierten des Vereinigten Königreichs David Smith gewechselt.
Im Oktober fand in Brüssel eine von der GK organisierte Konferenz mit dem Titel "DATA PROTECTION AT EUROPOL, A PERMANENT CHALLENGE" statt, an der meine Mitarbeiterin teilnahm. Vortragende waren u.a. der Vizepräsident der Europäischen Kommission und zuständige Kommissar für Inneres Franco Frattini, der Europäische Datenschutzbeauftragte Peter Hustinx, der Direktor von EUROPOL Max-Peter Ratzel, ein Mitglied des Europäischen Parlaments und ein

Vertreter des Generalsekretariats der Justiz und Inneres des Rates sowie ein Vertreter von Statewatch und ein Wissenschaftler der Universität Gent. Die Redebeiträge sind zu erhalten unter http://europoljsb.ue.eu.int.

3.2.1 Entwicklung von EUROPOL

Unter österreichischer Präsidentschaft im Ministerrat im ersten Halbjahr 2006 wurde die Diskussion über die Zukunft von EUROPOL forciert. Zum einen betrifft dies eine inhaltliche Veränderung des Vertragstextes des EUROPOL-Abkommens durch drei Protokolle, die im Februar 2007 in Kraft treten sollen. Diese Protokolle sind schon seit 2001 bzw. 2002 verabschiedet, bedurften aber der Ratifizierung durch alle Mitgliedstaaten.

Zum andern wurde vorgeschlagen, das völkerrechtliche EUROPOL-Abkommen durch einen Beschluss nach Art. 34 Abs. 2c Europäischer Unionsvertrag zu ersetzen, um damit eine leichtere, weniger zeitaufwändige Abänderbarkeit des Rechtsakts zu erreichen. Ein erster Entwurf für einen derartigen Beschluss liegt nunmehr vor und wird - da er auch einige inhaltliche Änderungen vorsieht - von der Gemeinsamen Kontrollinstanz (GK) geprüft. Die Stellungnahme wird derzeit erarbeitet.

Weiterhin liegen eine Reihe von Rechtsaktsentwürfen im Rahmen der sogenannten secondary legislation vor. Dabei handelt es sich um Rechtsakte, die für die Implementierung der Änderung des EUROPOL-Vertragstextes notwendig werden. Zu allen Entwürfen hat die GK Stellung genommen. Dies betrifft unter anderem:

- Vorschriften für die Datenverarbeitung zum Zweck der Prüfung, ob die entsprechenden Informationen für EUROPOL relevant sind,
- Durchführungsbestimmungen zu Arbeitsdateien zu Analysezwecken,
- Vorschriften zur Teilnahme von Drittstaaten und Drittstellen (z.B. EUROJUST, INTERPOL) bei der Errichtung von Arbeitsdateien zu Analysezwecken,
- Vorschriften zur Teilnahme von EUROPOL-Beamten in gemischten Untersuchungsteams.

3.2.2 Zugriff von EUROPOL auf das Visa-Informationssystem

Ein anderes Thema, mit dem sich die GK auseinandergesetzt hat, ist der in einem Entwurf für einen Ratsbeschluss (Beschluss betreffend den Zugang zum Visa-Informationssystem [VIS] für Sicherheitsbehörden und EUROPOL für die Zwecke der Verhütung und Ermittlung von terroristischen und anderen schweren Straftaten vom 24. November 2005 [COM 2005 600]) vorgesehene Zugriff unter anderem von EUROPOL auf das VIS.

Die Entscheidung zur Einrichtung des VIS erfolgte bereits mit Entscheidung des Rates vom 8. Juni 2005 (ABl. EU Nr. L 213/5 vom 15. Juni 2004). Zweck von VIS ist danach, die nationalen Behörden in die Lage zu versetzen, Visa-Datensätze über ein zentrales Informationssystem auszutauschen. Neben den alphanumerischen Daten über den Antragsteller und über Einzelheiten der Ausstellung des Visums sollen auch biometrische Daten (digitalisierte Lichtbilder und Fingerabdrücke) gespeichert werden (Art. 3 des Verordnungsvorschlags über das VIS und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt [BRDrucks. 25/05 vom 10. Januar 2005]). Genutzt werden soll das VIS vor allem bei Visa-Verfahren, aber auch im Asylverfahren und zur Identifizierung und Rückführung illegaler Einwanderer. In dem oben genannten Ratsbeschluss vom 24. November 2005 ist nunmehr der Zugriff von EUROPOL auf das VIS vorgesehen.

Die GK hat in einer Stellungnahme dargelegt, dass es sich bei diesem Zugriff um eine Durchbrechung der Zweckbestimmung von VIS handelt, die nur unter bestimmten Voraussetzungen zulässig ist. Es darf sich nach Auffassung der GK keinesfalls um einen regelmäßigen Zugriff handeln, sondern er muss auf konkret genannte Aufgaben von EUROPOL beschränkt sein.

3.2.3 Kontrolle von EUROPOL

Die GK hat im Jahre 2006 wieder eine Kontrolle bei EUROPOL durchgeführt. Der Bericht über diese Kontrolle ist vertraulich.

4. Bund

4.1 Antiterrordatei

Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss den verfassungsrechtlichen Vorgaben entsprechen, insbesondere dem Recht auf informationelle Selbstbestimmung und dem Grundsatz der Verhältnismäßigkeit. Die im Aufbau befindliche Antiterrordatei wird dem nicht in allen Punkten gerecht.

Die Diskussion um die Möglichkeit gemeinsamer Datenbestände von Polizei und Verfassungsschutz zur Bekämpfung des Terrorismus hat durch die am 1. Dezember 2006 im Bundestag erfolgte Verabschiedung des Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) ein vorläufiges Ende gefunden (BGBl. I 2006, S. 3409 ff.). Mit dem Gesetz wurde eine Rechtsgrundlage für die Errichtung einer gemeinsamen standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern geschaffen. Geführt wird diese Datei beim Bundeskriminalamt.

Damit wird eine neue Qualität der Zusammenarbeit zwischen Nachrichtendiensten und Polizei begründet – nicht mehr im Einzelfall wird zunächst geprüft, ob eine Übermittlungsbefugnis gegeben ist, sondern alle Daten werden in einen großen Topf gestellt, auf den für eine Vielzahl von beteiligten Stellen ein Online-Zugriff besteht.

Auch ich stelle mich nicht gegen notwendige Optimierungen des Informationsaustausches, gerade im Lichte der in der Begründung des Gesetzentwurfs geltend gemachten hohen Bedrohung durch den internationalen Terrorismus. Die verfassungsrechtlichen Vorgaben, insbesondere das Recht auf informationelle Selbstbestimmung und der Grundsatz der Verhältnismäßigkeit, müssen jedoch bei der Schaffung neuer Instrumentarien gewahrt werden. Auch bei der nunmehr verabschiedeten Fassung des Gesetzes sehe ich verfassungs- und datenschutzrechtliche Risiken, auch wenn gegenüber dem ursprünglichen Entwurf einige Änderungen erfolgt sind.

4.1.1 Betroffener Personenkreis

Die beteiligten Stellen sind verpflichtet, die bei ihnen vorhandenen Daten in diese Datei einzustellen, wenn sie gemäß der jeweils für sie geltenden Rechtsvorschriften über Erkenntnisse verfügen, die tatsächliche Anhaltspunkte begründen, dass eine Person zu dem im Gesetz definierten Personenkreis gehört. Dies sind zum einen solche Personen, die einer terroristischen Vereinigung nach § 129a StGB angehören oder eine solche unterstützen, und Personen, die rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden bzw. diese Anwendung unterstützen.

Darüber hinaus sind sogenannte Kontaktpersonen betroffen. Hierfür war es ursprünglich ausreichend, dass tatsächliche Anhaltspunkte die Annahme begründen, dass sie mit oben genannten Personen in Verbindung stehen oder durch sie Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus gewonnen werden können. Dies war von vielen Seiten im Gesetzgebungsverfahren als unverhältnismäßig kritisiert worden. Damit konnten auch Menschen betroffen sein, gegen die selbst keinerlei belastende Umstände vorlagen und die nur erfasst würden, weil sie soziale Kontakte zu anderen Betroffenen haben. Dies erschien auch mir im Lichte des Verhältnismäßigkeitsgrundsatzes zumindest bedenklich. Im Rahmen der parlamentarischen Beratungen ist jetzt eine Präzisierung erfolgt, die meine ursprünglichen Bedenken in diesem Punkt weitgehend ausräumt.

§ 2 Satz 1 Nr. 3 ATDG

Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den in Nummer 1 Buchstabe a oder in Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind (Kontaktpersonen), oder …

Nur in extremen Ausnahmefällen - weil besondere Geheimhaltungsinteressen oder besonders schutzwürdige Interessen des Betroffenen dies ausnahmsweise verlangen - kann von der Speicherung einzelner Daten abgesehen werden bzw. diese verdeckt erfolgen. Die Ergänzung im Interesse der Betroffenen ist durch den Innenausschuss des Bundestages erfolgt. Dabei soll dies nur im absoluten Ausnahmefall erfolgen, da grundsätzlich schon das Gesetz die Abwägung zwischen den Rechten der Betroffenen und den mit der Datei verfolgten Sicherheitsinteressen bzw. den dieses tragenden verfassungsrechtlichen Schutzgütern getroffen habe (BTDrucks. 16/3642 S. 37 f.). Ob und wie die beteiligten Stellen in der Praxis damit umgehen, wird zu beobachten sein.

4.1.2 Zu speichernde Daten

Gespeichert werden sowohl sogenannte Grunddaten als auch erweiterte Grunddaten.

§ 3 ATDG

(1) In der Antiterrordatei werden, soweit vorhanden, folgende Datenarten gespeichert:

1. zu Personen
   a) nach § 2 Satz 1 Nr. 1 bis 3: der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder, die Bezeichnung der Fallgruppe nach § 2 und, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen und dies zur Identifizierung einer Person erforderlich ist, Angaben zu Identitätspapieren (Grunddaten),
   b) nach § 2 Satz 1 Nr. 1 und 2 sowie zu Kontaktpersonen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie von der Planung oder Begehung einer in § 2 Satz 1 Nr. 1 Buchstabe a genannten Straftat oder der Ausübung, Unterstützung oder Vorbereitung von rechtswidriger Gewalt im Sinne von § 2 Satz 1 Nr. 2 Kenntnis haben, folgende weiteren Datenarten (erweiterte Grunddaten):
      aa) eigene oder von ihnen genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte,
      bb) Adressen für elektronische Post,
      cc) Bankverbindungen,
      dd) Schließfächer,
      ee) auf die Person zugelassene oder von ihr genutzte Fahrzeuge,
      ff) Familienstand,

gg) Volkszugehörigkeit,

hh) Angaben zur Religionszugehörigkeit, soweit diese im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sind,

ii) besondere Fähigkeiten, die nach den auf bestimmten Tatsachen beruhenden Erkenntnissen der beteiligten Behörden der Vorbereitung und Durchführung terroristischer Straftaten nach § 129a Abs. 1 und 2 des Strafgesetzbuches dienen können, insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen,

jj) Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung und zum ausgeübten Beruf,

kk) Angaben zu einer gegenwärtigen oder früheren Tätigkeit in einer lebenswichtigen Einrichtung im Sinne des § 1 Abs. 5 Sicherheitsüberprüfungsgesetz oder einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel oder Amtsgebäude,

ll) Angaben zur Gefährlichkeit, insbesondere Waffenbesitz oder zur Gewaltbereitschaft der Person,

mm) Fahr- und Flugerlaubnisse,

nn) besuchte Orte oder Gebiete, an oder in denen sich in § 2 Satz 1 Nr. 1 und 2 genannte Personen treffen,

oo) Kontaktpersonen nach § 2 Satz 1 Nr. 3 zu den jeweiligen Personen nach § 2 Satz 1 Nr. 1 Buchstabe a oder Nr. 2,

pp) die Bezeichnung der konkreten Vereinigung oder Gruppierung nach § 2 Satz 1 Nr. 1 Buchstabe a oder b,

qq) der Tag, an dem das letzte Ereignis eingetreten ist, das die Speicherung der Erkenntnisse begründet, und

rr) auf tatsächlichen Anhaltspunkten beruhende zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen zu Grunddaten und erweiterten Grunddaten, die bereits in Dateien der beteiligten Behörden gespeichert sind, sofern dies im Einzelfall nach pflichtgemäßem Ermessen geboten und zur Aufklärung oder Bekämpfung des internationalen Terrorismus unerlässlich ist.

2. .....

In der Antiterrordatei werden von Kontaktpersonen dann auch erweiterte Grunddaten gespeichert, soweit tatsächliche Anhaltspunkte vorliegen, dass sie Kenntnis haben von der Planung oder Ausübung bestimmter Straftaten bzw. von dem Einsatz rechtswidriger Gewalt. Für das Vorliegen tatsächlicher Anhaltspunkte reichen den Verfassungsschutzbehörden bereits konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht aus. Aufgrund der hohen Prognoseunsicherheit im Vorfeldbereich können diese Anhaltspunkte Bestandteil eines legalen Verhaltens der Betroffenen sein mit der Folge, dass die an der Antiterrordatei beteiligten Polizeibehörden auf die Daten auch dieser Kontaktpersonen unmittelbaren Zugriff erhalten, obgleich nach den für sie geltenden bereichsspezifischen Befugnisnormen sie selbst solche nicht erheben dürften.

4.1.3 Ausgestaltung der Datenübermittlung

Alle beteiligten Stellen haben einen jederzeitigen Online-Zugriff auf die Grunddaten. Auf die erweiterten Grunddaten erhält die abfragende Behörde Zugriff dann, wenn die eingebende Behörde diesen im Einzelfall auf Ersuchen gewährt. Dazu prüft sie vorab, ob die geltenden Übermittlungsvorschriften einen Zugriff durch die anfragende Stelle auf diese Daten zulassen.

Gleichzeitig werden aber durch das Gesetz neue Übermittlungsbefugnisse - insbesondere zwischen der Polizei und den Nachrichtendiensten - geschaffen. Ausgesprochen wird dies - und das auch nur indirekt - lediglich in der Gesetzesbegründung im Zusammenhang mit Ersuchen um Übermittlung weiterer - nicht in der Datei enthaltener - Erkenntnisse. Es erscheint bedenklich, ob damit die Anforderungen an eine normenklare Regelung wirklich erfüllt sind. Dies gilt zum einen natürlich für die Grunddaten, auf die jede beteiligte Behörde nunmehr einen jederzeitigen vollen Online-Zugriff hat. Wenn zur Abwehr einer gegenwärtigen Gefahr für hochrangige Rechtsgüter die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann, darf die Behörde aber auch unmittelbar auf die erweiterten Grunddaten zugreifen. Darüber hat die Behördenleitung zu entscheiden. Diese Entscheidung ist mit Gründen zu dokumentieren. Der Zugriff auf die Daten wird dann mit einer entsprechenden Kennzeichnung protokolliert.

Damit wird ebenfalls eine neue Übermittlungsbefugnis geschaffen. Hier sehe ich ein nicht unerhebliches Gefährdungspotential, da nur im Nachhinein festgestellt werden kann, ob wirklich die Übermittlungsvoraussetzungen vorlagen. Dabei ist insbesondere zu berücksichtigen, dass in der Antiterrordatei auch sensible weiche, das heißt auf ungesicherten Erkenntnissen beruhende, personenbezogene Daten der Nachrichtendienste gespeichert werden müssen, die von den Diensten im Vorfeldbereich der Gefahrenabwehr auf der Grundlage bereichsspezifischer - im Vergleich zu polizeilichen Eingriffsnormen - niedrigerer Eingriffsschwellen erhoben worden sind. Dies gilt erst recht, soweit es sich um die Daten von Kontaktpersonen handelt.

Im Rahmen der allgemeinen Debatte um Verschärfung der Sicherheitsgesetze aufgrund der Entwicklung des internationalen Terrorismus war auch dieses Projekt Gegenstand der Beratungen und Beschlussfassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Ziff. 10.5 und Ziff. 10.6).

4.2 Folgerungen aus der Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung

Das Bundesverfassungsgericht hat mit seiner Entscheidung zur Rasterfahndung Kriterien entwickelt, an denen die gesetzlichen Grundlagen für eine verfassungskonforme Rasterfahndung zu messen sind.

4.2.1 Die Entscheidung des Bundesverfassungsgerichts

Das BVerfG hat in einem Beschluss des 1. Senats vom 4. April 2006 (Az. 1 BvR 518/02) zur Verfassungsmäßigkeit der Rasterfahndungsregelung im Nordrhein-Westfälischen Polizeigesetz erneut Rahmenbedingungen für den Einsatz von verdeckten Erhebungsmaßnahmen formuliert. Kernpunkt ist die Aussage, dass ein solcher Eingriff in das Recht auf informationelle Selbstbestimmung nur dann angemessen ist, wenn der Eingriff von der Schwelle einer hinreichend konkreten Gefahr für bedrohte hochrangige Verfassungsgüter abhängig gemacht wird.

Das BVerfG stellt fest, dass die Anordnung an Dritte, Daten für eine Rasterfahndungsmaßnahme zu übermitteln, einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, da sie die Grundlage für die Erfassung und die Speicherung der Daten sowie für ihren Abgleich mit weiteren Daten schafft. Auch dann, wenn die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere (technische) Verkleinerung der Treffermenge bildet, kann in der Datenerhebung bereits ein Eingriff liegen. Das Gleiche gilt für den eigentlichen Akt des (technischen) Abgleichs und alle in diesem Kontext notwendigen Datenspeicherungen, vor allem auch für den Personenkreis, dessen Daten nach dem Abgleich Gegenstand weiterer polizeilicher Maßnahmen werden.

Schließlich hat das BVerfG sich mit der Intensität des Eingriffs im Rahmen einer Rasterfahndung auseinandergesetzt. Es führt dazu aus, dass für die rechtliche Beurteilung der Art des durch die Ermächtigung ermöglichten Eingriffs u.a. bedeutsam ist, wie viele Grundrechtsträger intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben. Maßgebend sind also die Gestaltung der Eingriffsschwellen, die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung. Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden.

Das BVerfG fordert daher, dass der Gesetzgeber rechtsstaatliche Anforderungen dadurch wahrt, dass er den Eingriff erst von der Schwelle einer hinreichend konkreten Gefahr für die bedrohten Rechtsgüter an vorsieht. Im Vorfeld einer konkreten Gefahr scheide hingegen eine Rasterfahndung aus. Zudem müsse im Hinblick auf den Verhältnismäßigkeitsgrundsatz im engeren Sinne die Ausgewogenheit zwischen der Art und Intensität der Grundrechtsbeeinträchtigung einerseits und den zum Eingriff berechtigenden Tatbestandselementen andererseits, wie der Einschreitschwelle, der geforderten Tatsachenbasis und dem Gewicht der geschützten Rechtsgüter, gewahrt werden. Darüber hinaus betont das BVerfG die grundrechtssichernde Bedeutung des Richtervorbehalts und der nachträglichen individuellen Benachrichtigung der Betroffenen.

4.2.2 Änderungsbedarf im HSOG

Aus der Rechtsprechung des BVerfG ergibt sich auch die Notwendigkeit der Novellierung des HSOG.

§ 26 Abs. 1 HSOG

Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Verhütung von Straftaten erheblicher Bedeutung gegen den Bestand oder die Sicherheit des Bundes oder eines Landes oder bei denen Schäden für Leben, Gesundheit oder Freiheit oder gleichgewichtige Schäden für die Umwelt zu erwarten sind, die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich und dies auf andere Weise nicht möglich ist.

Schon mein Amtsvorgänger hatte bei der Novellierung des § 26 HSOG aus Anlass der Rasterfahndungsmaßnahmen im Anschluss an die Ereignisse des 11. September 2001 darauf hingewiesen, dass damit die Einsatzschwelle nicht mehr an eine wirkliche Gefahrenlage geknüpft sei (vgl. 31. Tätigkeitsbericht, Ziff. 2.2).
Auch das BVerfG hat § 26 HSOG als eine Norm bezeichnet, die als polizeiliche "Vorfeldbefugnis" ausgestaltet ist, d.h. die eine Rasterfahndung auch ohne das Vorliegen einer konkreten Gefahr ermöglicht (Presseerklärung 40/2006 vom 23. Mai 2006).

Die Entscheidung des BVerfG hat die FDP-Fraktion im Hessischen Landtag zum Anlass genommen, einen entsprechenden Änderungsantrag einzubringen (LTDrucks. 16/5773).

§ 26 Abs. 1 Satz 1 erhält folgende Fassung:
Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Abwehr einer konkreten Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich und dies auf andere Weise nicht möglich ist.

Im Rahmen der parlamentarischen Beratung fand im November eine schriftliche Anhörung statt. Dabei habe ich mich insoweit für die Umsetzung dieses Antrages ausgesprochen. Das Gesetzgebungsverfahren ist derzeit noch nicht abgeschlossen.

Bei den anderen verdeckten Erhebungsmaßnahmen bestimmt das HSOG eine Einsatzschwelle, die an eine bestimmte Gefahrensituation anknüpft, sodass insoweit die Regelungen verfassungskonform sind. Hier kommt es im Einzelfall darauf an,

das Instrument entsprechend einzusetzen, d.h. bei der Beurteilung der Situation den vom BVerfG formulierten Maßstab zu berücksichtigen.

4.3 Datenschutzfragen nach der Fußball-WM

Im Zusammenhang mit der Weltmeisterschaft erfolgte die Verarbeitung der personenbezogenen Daten in dem vorab festgelegten Rahmen. Die für dieses besondere Ereignis getroffenen Vereinbarungen dürfen aber nicht auf jedes Ereignis, bei dem mit einer Vielzahl von beteiligten Personen zu rechnen ist, übertragen werden.

4.3.1 Das Akkreditierungsverfahren

Um es vorab zu sagen: insgesamt ist die hessische Polizei mit diesem Komplex und der Menge der dabei zu verarbeitenden Daten sensibel umgegangen. Das zeigt sich nicht zuletzt daran, dass nur ein extrem niedriger Anteil an Beschwerden beim HLKA einging. Von den 10.980 zu bearbeitenden Datensätzen hatte das HLKA in 152 Fällen Bedenken geäußert. Dort gingen dann 16 Beschwerden ein. Nach nochmaliger Prüfung wurde in neun Fällen das Votum noch zugunsten der Betroffenen geändert.
Bei meiner Dienststelle gab es zu diesem Komplex zwar eine Fülle von Presseanfragen, aber keine Beschwerden von Betroffenen.

Nach dem Ende der Weltmeisterschaft habe ich beim HLKA die Verarbeitung der Daten geprüft. Diese erfolgte entsprechend dem in meinem letzten Tätigkeitsbericht beschriebenen Konzept (vgl. 34. Tätigkeitsbericht, Ziff. 4.3). Bei der durchgeführten Stichprobe der von der Sachbearbeitung zu beurteilenden Anträge konnte ich feststellen, dass alle Datensätze im Rahmen des vorgegebenen Bewertungsmaßstabes bearbeitet worden sind. Die vorgenommenen Ermittlungsmaßnahmen und - soweit notwendig - das Ergebnis der Beurteilung waren ausreichend dokumentiert, sodass im Falle einer Nachfrage Auskunft erteilt werden konnte.

Die Abwicklung erfolgte mit Unterstützung einer Crime-Datenbank. Bei Trefferfällen in den Datenbanken waren Einzelheiten dokumentiert. Dazu gehörte eine Kopie der POLAS-Auskunft, welche Fälle für den Betroffenen vorliegen. Dem Datensatz angehängt war in der Regel auch ein Vermerk, der die Nachforschungen bei anderen Stellen - andere LKÄ, Staatsanwaltschaften, ggf. auch Bundeszentralregister - kurz wiedergibt. Soweit es nicht offensichtlich war - etwa bei einer Vielzahl von Fällen bzw. bei schweren Fällen - war auch eine kurze Begründung für die Ablehnung enthalten. Wenn trotzdem ein approved ("keine Bedenken") vergeben wurde, war dies mit knapper Begründung im Datensatz vermerkt: "eine nochmalige Prüfung hat pos. Votum begründet" oder ähnlich.

Es war beabsichtigt, alle Datensätze noch ein Jahr - gerechnet vom Ende der Veranstaltung WM 2006 - aufzubewahren. Diese Frist ist nach meiner Einschätzung zu lang. Zumindest für die Datensätze, die mit "approved" beantwortet sind, ist mir kein Grund ersichtlich, der eine weitere Speicherung - wenn auch gesperrt für die Sachbearbeitung - begründen könnte. Notwendig für die Bearbeitung möglicher Rückfragen/Beschwerden können allenfalls nur die Fälle sein, in denen mit "reject" reagiert wurde.

Bei der Überprüfung habe ich zudem festgestellt, dass die Datensätze aus den Veranstaltungen "Confed-Cup" ebenfalls noch vorhanden waren. Auch diese sollten bis ein Jahr nach Ende der WM aufbewahrt werden. Zudem wurden die Datensätze bei der Bearbeitung der Anträge zur WM 2006 mit herangezogen.

Dieses Vorgehen war nicht zulässig. Die Einwilligung der Antragsteller im Confed-Cup bezog sich jeweils auf die Überprüfung im Zusammenhang einer Akkreditierung für eine bestimmte Veranstaltung. Die Verwendung im Rahmen einer anderen Veranstaltung stellt eine Zweckänderung dar, die von der Einwilligung nicht gedeckt ist.

Im Übrigen waren die Daten inzwischen eigentlich gesperrt, damit würde auch § 27 Abs. 7 HSOG eine solche neue Verwendung verbieten.

§ 27 Abs. 7 HSOG
Gesperrte Daten dürfen nur zu den in Abs. 6 Satz 1 genannten Zwecken oder sonst mit Einwilligung der betroffenen Person verarbeitet werden. In den Fällen des Abs. 6 Satz 1 Nr. 2 dürfen die Daten nur zur Unterrichtung der betroffenen Person und zur gerichtlichen Kontrolle verarbeitet werden.

Das HLKA hat daraufhin die Datenbestände entsprechend bereinigt.

4.3.2 Prüfung im Frankfurter Stadion

An einem der Spieltage hatte eine meiner Mitarbeiterinnen Gelegenheit, die Kollegen des Regierungspräsidiums Darmstadt bei der Überprüfung der Umsetzung der verschiedenen Maßnahmen vor Ort im Frankfurter Stadion zu begleiten.

Dort wurden verschiedene Beschäftigte und Volunteers befragt, wie sich für sie die Abwicklung des Akkreditierungsverfahrens dargestellt hat. Alle haben geschildert, dass das Verfahren aus ihrer Sicht - auch bei der Abwicklung über die Arbeitgeber - entsprechend den Vorgaben der Konzepte stattgefunden hatte.

Im Vorfeld war unter datenschutzrechtlichen Aspekten problematisiert worden, ob es wirklich notwendig ist, eine so große Anzahl von Personen - unabhängig von ihrem konkreten Einsatzort - zu überprüfen. Die dazu vom Organisationskomitee vorgetragenen Argumente hatten mich letztlich von der Notwendigkeit überzeugt.

Bei der Überprüfung vor Ort war festzustellen, dass zumindest für eine Konstellation nicht sichergestellt war, ob die engen Anforderungen an die Überprüfung der Personen, die das Stadiongelände betreten durften, durchgehend eingehalten worden sind. Für Lieferanten, bzw. die Fahrer von Fahrzeugen, die Material - etwa für das Catering - bringen sollten, war festgelegt, dass die einzelnen Fahrzeuge angemeldet werden mussten, und jeweils ein Verantwortlicher vor Ort auch bestätigen musste, dass die zum Fahrzeug gehörenden Personen zum entsprechenden Unternehmen gehören und für eine konkrete Aufgabe auf dem Gelände benötigt wurden. Die betreffenden Mitarbeiter mussten dann ihren Ausweis bei der Zufahrtskontrolle hinterlegen und bekamen einen besonderen Ausweis zum Betreten des Geländes. Es ließ sich allerdings auch auf Nachfragen nicht wirklich klären, ob bei der Anmeldung der Fahrten eine Kontrolle erfolgte, ob für dieses Unternehmen grundsätzlich ein Befahren des Geländes erlaubt war. Zudem wurde auch auf dem Platz festgestellt, dass nicht durchgehend sichergestellt war, dass diese Personen, die ja vorab nicht selbst von den Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft worden waren, sich nur in Begleitung von akkreditierten Personen bewegen konnten.

Grundsätzlich ist dies zunächst eine Frage der Sicherheitskonzeption, die sich der datenschutzrechtlichen Bewertung entzieht. Allerdings drängt sich dann die Frage nach der Verhältnismäßigkeit und der Erforderlichkeit der Überprüfung des weiten Personenkreises auf.

4.3.3 Personalisierte Tickets

Die Gestaltung der Tickets war im Vorfeld der WM eines der - nicht nur im Kreis der Datenschutzinteressierten - am meisten diskutierten Themen. Dabei ging es sowohl um die Frage, ob wirklich alle Tickets personalisiert sind, als auch darum, wie die Kontrolle realisiert wird, dass tatsächlich nur berechtigte Ticketinhaber ins Stadion kommen.

Die Verantwortung für die Gestaltung und Handhabung der Tickets lag in der Verantwortung des Organisationskomitees und unterfiel somit der datenschutzrechtlichen Kontrolle durch das Regierungspräsidium Darmstadt als zuständige Aufsichtsbehörde.

Festzustellen bleibt, auch als Ergebnis der Kontrolle vor Ort, dass grundsätzlich das technische Konzept funktioniert hat und die Verarbeitung der Daten auch im beschriebenen Rahmen erfolgte. Allerdings gab es nicht personalisierte Tickets, Tickets, die im Schwarzmarkt verkauft, aber auch solche, die ohne Umschreibung an Dritte, etwa an Freunde oder Familienmitglieder, weitergegeben worden waren. Die Zahl der wirklichen Stichproben, wer mit dem Ticket das Stadion betrat, war gering.
Letztlich bleibt es aber Sache der jeweiligen Veranstalter, für sich zu bewerten, ob ein solcher Aufwand gewollt ist und wie hoch das notwendige Sicherheitsniveau angesetzt wird.

4.3.4 Zukünftige Akkreditierungsverfahren

Beim BKA war zur Abwicklung der Akkrediterungsverfahren eine technische Infrastruktur aufgebaut worden, mit deren Hilfe die Kommunikation zwischen dem Organisationskomitee und den beteiligten Sicherheitsbehörden abgewickelt wurde. Beim BKA wurden damit gleichzeitig verschiedene zentrale Datenbestände des Polizeilichen Informationssystems abgefragt.

Diese Infrastruktur ist weiterhin vorhanden und wird vom BKA auch zur Abwicklung weiterer Veranstaltungen, bei denen eine "Sicherheitsüberprüfung" einer Vielzahl von Personen für notwendig angesehen wird, angeboten.

Dies ist aus meiner Sicht problematisch. Die Einbeziehung des großen Personenkreises auf Grundlage einer Einwilligung hatte ich für die Durchführung der Weltmeisterschaft als singuläres Ereignis von besonderer Bedeutung akzeptiert. Ich hatte schon im letzten Jahr darauf hingewiesen, dass dieses Verfahren die Ausnahme sein müsse. An dieser Einschätzung hat sich nichts geändert.

4.4 Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren am Beispiel ElsterOnline-Portal

Die aktuellen Änderungen in der Abgabenordnung und der Steuerdaten-Übermittlungsverordnung sowie die besondere Entwicklung im Bereich des ElsterOnline-Portals zur Abgabe elektronischer Steuererklärungen, machen es notwendig, erneut auf die unterschiedlichen Anwendungsfelder für den Einsatz von Signaturschlüsseln und von Authentisierungsschlüsseln hinzuweisen.

Bereits im 32. Tätigkeitsbericht (Ziff. 18.5) habe ich mich mit der elektronischen Authentisierung mit Schlüsseln befasst. In diesem Beitrag geht es um die unterschiedlichen Einsatzfelder von Authentisierung und Signatur und die daraus resultierenden Folgerungen.

Durch das Justizkommunikationsgesetz vom 23. März 2005 (BGBl. I S. 837) wurde in verschiedenen Prozess- und Verwaltungsordnungen eine Öffnungsklausel eingeführt, nach der neben der qualifizierten elektronischen Signatur auch ein sog. "anderes sicheres Verfahren" zugelassen werden kann, vorausgesetzt, es stellt die Authentizität und die Integrität des übermittelten Dokuments sicher (z.B. § 55a VwGO, § 52a Abs. 1 FGO). Detaillierte technische Vorgaben wurden nicht getroffen.
Eine entsprechende Regelung wurde nun auch in § 87a Abs. 6 AO übernommen, wobei im Finanzbereich mit dem ElsterOnline-Portal - auf der Grundlage der StDÜV - die bisher erste praktische Umsetzung dieser Öffnungsklausel erfolgen soll.

4.4.1 Vorgeschichte ElsterOnline

Bereits durch das Steueränderungsgesetz 2003 vom 15. Dezember 2003 (BGBl. I S. 2645, BGBl. I S. 710) wurde § 18 Abs. 1 Satz 1 UStG geändert. Danach haben Unternehmer bereits ab 1. Januar 2005 ihre Umsatzsteuer-Voranmeldung auf

elektronischem Weg nach Maßgabe der Steuerdatenübermittlungsverordnung abzugeben. Ausnahmen erfolgen lediglich in unbilligen Härtefällen. Der Einsatz der qualifizierten Signatur ist nicht vorgesehen, da die Voranmeldung bereits gesetzlich keiner Unterschrift bedarf. Der elektronische Zugang zur Finanzbehörde ist das ElsterOnline-Portal.
Im Jahr 2004 beschloss die Finanzverwaltung einen Strategiewechsel auch für elektronische Jahressteuererklärungen (ELSTER), z.B. Lohnsteuererklärungen, die bisher im Papierverfahren die Unterschrift und die Wahrheitsversicherung der Steuerbürger voraussetzten. Für die Nutzung des ElsterOnline-Portals soll auf die Unterschrift und die Wahrheitsversicherung und damit auch auf die Anwendung der qualifizierten elektronischen Signatur verzichtet werden. Als Ersatz wurde ein Authentisierungsverfahren geschaffen, das den Datenübermittler registriert und die Authentizität und Integrität des Dokuments gewährleisten soll. Seit dem 1. Januar 2006 ist das ElsterOnline-Portal in allen 16 Bundesländern in Betrieb. Zum Redaktionsschluss dieses Tätigkeitsberichtes war die Steuerkontoabfrage nur bei den Finanzämtern der Länder Bayern, Berlin, Hessen und Sachsen möglich. Um diesem Verfahren die bislang fehlende gesetzliche Grundlage zu verschaffen, wurde eine Änderung des § 87a AO (Elektronische Kommunikation) und eine entsprechende Änderung der Steuerdaten-Übermittlungsverordnung eingeleitet.

Wegen der grundsätzlichen Unterschiede zwischen Authentisierungs- und Signaturverfahren hatte ich prinzipielle Bedenken gegen die Planungen.

4.4.2 Unterschiede zwischen Signatur- und Authentisierungsverfahren

4.4.2.1 Dokumente und Daten

Beide Verfahren nutzen zwar mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren; sie unterscheiden sich aber grundlegend im Inhalt ihrer Aussagen. Die Signatur bezieht sich auf **Dokumente**, die Authentisierung dagegen auf **Daten**.
Für den Begriff "elektronisches Dokument" gibt es keine Definition durch den Gesetzgeber. Er setzt den Begriff vielmehr beispielsweise im Verwaltungsverfahrensgesetz als bekannt oder klar voraus. Deshalb versuche ich zunächst, diesen Begriff zu erläutern, ohne Anspruch auf eine rechtsverbindliche Definition zu erheben:

Elektronisches Dokument:
Technisch ist ein **elektronisches Dokument** meistens in Form einer Datei abgelegt.
Es kann verschiedene Merkmale haben:
formale Eigenschaften (Aufbau, Gestaltung u.Ä.),
strukturelle Eigenschaften (Text, Tabelle, Bild u.Ä.),
inhaltliche Eigenschaften (Inhalt, Bezug u.Ä.),
charakterliche Eigenschaften (Rechtscharakter, Archivierungswürdigkeit u.Ä.),
zeitliche Eigenschaften (Erzeugungsdatum, Verfallsdatum, letzte Benutzung u.Ä.).
Dokumente haben Erzeugende (Ersteller, Autoren, Absender u.Ä.) und Nutzende (Empfangende, Bearbeitende, Lesende u.Ä.).
Der Inhalt kann eine Willenserklärung enthalten.

Der Begriff "Daten" wird in der technischen Norm DIN 443000 definiert:

Daten sind Informationen, die durch Zeichen oder kontinuierliche Funktionen aufgrund bekannter oder unterstellter Abmachungen zum Zweck der Verarbeitung dargestellt werden.

Aus dem Vergleich der beiden Definitionen ergibt sich unmittelbar, dass der Datenbegriff wesentlich weiter ist; er umfasst auch maschineninterne Befehle, Daten zur Abwicklung von Kommunikationsprotokollen und vieles andere mehr.

4.4.2.2 Signaturverfahren

Elektronische Signaturen liefern Aussagen über elektronische **Dokumente**, insbesondere über deren Authentizität (das Dokument stammt von dem oder der Signierenden) und Integrität (das Dokument ist unverfälscht). Die Verfahren zur Erzeugung und Prüfung elektronischer Signaturen über Dokumenten sind rechtlich geregelt und sicherheitstechnisch genau definiert (vgl. hierzu das Signaturgesetz [SigG], die Signaturverordnung [SigV] und die EU-Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen).

Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente (s. 30. Tätigkeitsbericht, Ziff. 4). Hier seien beispielhaft der Urkundenbeweis und der schriftformbedürftige elektronische Verwaltungsakt genannt. Der Urkundenbeweis liefert nach § 371a Abs. 1 ZPO für private elektronische Dokumente den Anschein der Echtheit, nach § 371a Abs. 2 ZPO für öffentliche elektronische Dokumente sogar die Vermutung der Echtheit des Dokuments. Der Anschein der Echtheit kann nach § 371a Abs. 1 Satz 2 ZPO nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüsselinhaber stammt; die Vermutung der Echtheit ist nur durch einen Gegenbeweis zu entkräften.
Für den schriftformbedürftigen elektronischen Verwaltungsakt kann nach § 37 Abs. 4 HVwVfG die dauerhafte Überprüfbarkeit der Signatur und damit auch des zugehörigen Zertifikates vorgeschrieben werden.

4.4.2.3 Authentisierungsverfahren

Authentisierungsverfahren liefern dagegen lediglich eine Aussage über die Identität einer **Person** oder einer Systemkomponente, nämlich dass sie diejenige ist, die sie vorgibt zu sein.

Solche Verfahren sind unter anderem zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet.
Hierfür verwendet ein Authentisierungsverfahren (beliebige) Daten, die i.d.R. nicht von der zu authentisierenden Person stammen, sondern von technischen Verfahren vorgegeben werden, und eine oder mehrere Aktion(en) der Person (z.B. Freischalten des Authentisierungsschlüssels), mit dem ausschließlichen Ziel, die Person zu authentifizieren. Hier geht es nicht um ein Dokument und schon gar nicht um eine als Dokumentinhalt formulierte Willenserklärung. Die einzige Willenserklärung bei diesem Verfahren liegt in der Erklärung, sich durch die Aktion authentisieren zu wollen.
Die hierbei übertragenen Informationen können beispielsweise aus einer beliebigen Zeichenfolge oder aus Zufallszahlen bestehen oder aus einer spezifischen geheimen Information, verbunden mit Datum und Uhrzeit, um ein unbemerktes Abfangen und Wiederverwenden zu verhindern. Sie unterliegen also in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner. Sie beziehen sich vielmehr ausschließlich auf den technischen Identifizierungsprozess und ermöglichen bei Bedarf zusätzlich die geheime Absprache eines symmetrischen Schlüssels zur vereinfachten Verschlüsselung der nachfolgenden Kommunikation.

Es versteht sich von selbst, dass diese Daten nicht als elektronisches Dokument aufgefasst werden dürfen. Daher sind mit diesem Verfahren auch keine Aussagen über die Authentizität und Integrität eines Dokumentes (oder gar einer Willenserklärung) möglich. Folglich dürfen an die rechtliche Bewertung von Authentizität und Integrität der übertragenen **Daten** auch nicht die gleichen Rechtsfolgen geknüpft werden, wie sie für ein (qualifiziert) signiertes elektronisches **Dokument** geregelt sind.

Die für ein Authentisierungsverfahren verwendeten technischen Verfahren und Parameter sind nicht im Einzelnen festgelegt. So ist beispielsweise offen, ob die Authentisierungsinformation zuerst - analog zum Signaturverfahren - auf eine vorgegebene feste Länge komprimiert ("gehasht") wird oder nicht, bevor der eigentliche Authentisierungsschlüssel angewendet wird.
Im Gegensatz zur qualifizierten elektronischen Signatur (vgl. dazu oben Ziff. 4.4.2.2) existieren für Authentisierungsverfahren auch keine gesetzlichen Regelungen über Verfahren und sicherheitstechnische Anforderungen.

4.4.2.4 Unterschiedliche Funktion von Signatur und Authentisierung berücksichtigen

Der grundlegende Unterschied von Signatur und Authentisierung muss sowohl bei der Planung von Verfahren als auch bei deren Einsatz berücksichtigt werden. Die Aufrechterhaltung der unterschiedlichen Funktion und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung von Signatur- und Authentisierungsverfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Gefährdungspotenziale für die Nutzenden zu erwarten:

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicherweise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen (z.B. Spende eines großen Geldbetrages, Kauf eines überteuerten Gegenstandes etc.) tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine "Warnfunktion" mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

4.4.3 Authentisierungslösung ElsterOnline-Portal

Wegen dieser notwendigen Unterscheidung zwischen Authentisierungs- und Signaturfunktion habe ich die weitere Entwicklung des ElsterOnline-Portals aufmerksam verfolgt und mich besonders für die konkrete Ausgestaltung des Authentisierungsverfahrens interessiert.

4.4.3.1 Technisches Verfahren

Im Frühjahr d.J. erhielt ich eine mündliche Beschreibung des inzwischen pilotierten Verfahrens; eine schriftliche Verfahrensbeschreibung liegt mir noch nicht vor: Die Steuererklärungen bzw. -anmeldungen werden mit dem Authentisierungsschlüssel "signiert". D.h., dass vom technischen Verfahren her eine elektronische Signatur durchgeführt wird; man verwendet aber, um nicht die hohen Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllen zu müssen, einen Authentisierungsschlüssel. Probleme sind dabei insbesondere dann vorprogrammiert, wenn derselbe Schlüssel gleichzeitig in anderen DV-Verfahren auch in seiner eigentlichen Funktion zur Authentisierung verwendet wird. Im Sommer erhielt ich dann noch den Hinweis, dass für die "Signatur" im ElsterOnline-Portal der Authentisierungsschlüssel des zukünftigen Personalausweises verwendet werden soll.

Wegen der oben beschriebenen Intransparenz für die Nutzenden einerseits und der sehr problematischen Rückwirkung der möglichen unerwünschten Rechtsfolgen auf die wirklichen Authentisierungsverfahren andererseits wurden die Planungen und ihre Auswirkungen im AK Steuer und im AK Technik der DSB-Konferenz beraten, und vom AK Technik wurde eine Entschließung der DSB-Konferenz vorbereitet. Die DSB-Konferenz hat wegen der Eilbedürftigkeit, die sich aus dem in Bundestag und Bundesrat parallel laufenden Gesetzgebungsverfahren zur Änderung des § 87a Abs. 6 AO (Elektronische Kommunikation) im Rahmen des Jahressteuergesetzes 2007 ergab, diese Entschließung im Umlaufverfahren am 11. Oktober 2006 verabschiedet. Sie ist unter Ziff. 10.9 abgedruckt.

4.4.3.2 Neue Rechtliche Regelungen für ElsterOnline

a) § 87a Abs. 6 AO
Der Entwurf des Jahressteuergesetzes 2007 sah in Artikel 10 ursprünglich vor, § 87a Abs. 6 AO folgendermaßen zu ändern:

Das Bundesministerium der Finanzen kann durch Rechtsverordnung mit Zustimmung des Bundesrates für die Fälle der Absätze 3 und 4 neben der qualifizierten elektronischen Signatur auch ein anderes sicheres Verfahren zulassen, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Einer Zustimmung des Bundesrates bedarf es nicht, soweit Verbrauchsteuern mit Ausnahme der Biersteuer betroffen sind. Soweit ein anderes sicheres Verfahren zugelassen worden ist, gilt Abs. 5 Satz 2 sinngemäß.

In Abs. 5 Satz 2 heißt es:
Der Anschein der Echtheit eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz übermittelten Dokuments, der sich aufgrund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass das Dokument mit dem Willen des Signaturschlüssel-Inhabers übermittelt worden ist.

Entgegen meiner obigen Darlegungen bzgl. Authentisierungsverfahren (s. Ziff. 4.4.2.3) sollte an das "andere sichere" (aber nicht näher bezeichnete) "Verfahren" eine Anscheinsbeweisregelung geknüpft werden, wie sie bislang nur für ein mit qualifizierter elektronischer Signatur versehenes Dokument nach dem Signaturgesetz geregelt ist. Im Rahmen meiner Möglichkeiten in einem Bundesgesetzgebungsverfahren Stellung zu nehmen, habe ich gegenüber dem Bundesdatenschutzbeauftragten und dem Hessischen Ministerium der Finanzen meine Einwände, insbesondere in Bezug auf das bereits laufende Verfahren ElsterOnline-Portal, vorgebracht:
Die Nutzenden haben auf das im ElsterOnline-Portal eingesetzte "andere Verfahren" keinen Einfluss und auch keine weiteren Informationen. Sie werden also Tatsachen, die einen Anscheinsbeweis erschüttern könnten, kaum vortragen können. Wenn aber die Finanzverwaltung auf die qualifizierte elektronische Signatur - und damit auf die Möglichkeit der Gleichstellung mit der gesetzlich vorgeschriebenen Schriftform - zugunsten eines anderen Verfahrens verzichtet, muss sie auch selbst die möglichen Risiken tragen, die sich daraus ergeben, und darf sie nicht auf die Nutzenden abwälzen. Ferner ist zu beachten, dass die "Warnfunktion" durch die Eingabe einer eigenen PIN für die Erstellung einer qualifizierten Signatur bei dem "anderen Verfahren" für die Nutzenden nicht gegeben ist.

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit hat - unterstützt durch die Entschließung der Konferenz und entsprechende Stellungnahmen von Landesdatenschutzbeauftragten - erreicht, dass die vorgesehene analoge Anwendung der für qualifiziert signierte Dokumente geltenden Anscheinsbeweisregelung für die "anderen Verfahren" gestrichen und die Öffnungsklausel für solche Verfahren bis 31. Dezember 2011 befristet wird. Außerdem ist eine Evaluierung vorgesehen.

b) Steuerdaten-Übermittlungsverordnung (StDÜV)
In § 6 des Entwurfs zur Änderung der StDÜV wird von der Möglichkeit des § 87a Abs. 6 AO, ein anderes sicheres Verfahren anzuwenden, für automatisierte Datenübermittlungen vom Steuerbürger an die Finanzbehörden - also für das ElsterOnline-Portal - Gebrauch gemacht.

Die Regelung übernimmt jedoch nicht die Vorgabe aus § 87a AO, den Einsatz des "anderen **sicheren** Verfahrens" **neben** der qualifizierten elektronischen Signatur zuzulassen, sondern geht von dem Ersatz der qualifizierten Signatur durch das andere Verfahren aus. Dies wird bereits durch die bisherigen Erfahrungen aus der Praxis mit ElsterOnline belegt: Wer seine Steueranträge mit qualifizierter elektronischen Signatur einreichen möchte wird zurückgewiesen! Auch die Sicherheit des anderen Verfahrens wird hier nicht gefordert.
Weiterhin sieht der StDÜV-Entwurf lediglich ein Verfahren vor, das Authentizität und Unversehrtheit der Daten gewährleistet, während § 87a Abs. 6 AO ein Verfahren fordert, das die Authentizität und Integrität des Dokuments sicherstellt. Den Unterschied habe ich oben unter Ziff. 4.4.2.1 dargestellt. Damit werden die Anforderungen der AO abgeschwächt, um die Nutzung von Authentisierungsverfahren zum Signieren zu ermöglichen.

Leider hat der Bundesrat die Forderungen und Vorschläge der Datenschutzbeauftragten für die Regelungen in der StDÜV nicht berücksichtigt.
Darüber hinaus sind die Anforderungen an die Sicherheit der elektronischen Übermittlung nicht mehr - wie im Entwurf vorgesehen - im Einvernehmen, sondern nur noch im Benehmen mit dem BSI festzulegen.

Ich werde weiterhin darauf dringen, dass die Regelungen für das eingesetzte Verfahren die gesetzlichen Vorgaben in § 87a Abs. 6 AO erfüllen.

4.4.4 Bewertung

Die einzigen Verfahren, die die sicherheitstechnischen Voraussetzungen der Öffnungsklausel für ein anderes sicheres Verfahren erfüllen, sind Signaturverfahren. Authentisierungsverfahren (s.o. Ziff. 4.4.2.3) leisten das nicht. Auch, wenn man das im Jahr 2004 im Finanzbereich offenbar anders gesehen hat (s. Ziff. 4.4.1). Statt Authentisierungsverfahren zweckentfremdet einzusetzen, könnten höchstens fortgeschrittene Signaturen mit bestimmten Zusatzvoraussetzungen zugelassen werden. In der AO wird keine der qualifizierten Signatur explizit **vergleichbare** Sicherheit verlangt, aber die Authentizität und die Integrität des übermittelten elektronischen Dokuments sollen **"sichergestellt"** werden. Hierfür müssten verlässliche Kriterien definiert werden, und die Folgen der geringeren Sicherheit müssen von den Behörden getragen werden, die diese Verfahren akzeptieren.

Besonders kritisch betrachte ich die Entwicklung, weil nach meiner Einschätzung die Regelungen in AO und StDÜV und ihre Anwendung beim ElsterOnline-Portal "Pilotcharakter" haben: Wenn dort jetzt Authentisierungsverfahren zugelassen werden, wird das im Zweifel zu ebenso problematischen Folgewirkungen in den anderen oben genannten Rechtsbereichen (s.o. Ziff. 4.4) und damit zur Eskalation der unerwünschten Rechtsfolgen und der Intransparenz führen.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die letzten beiden Forderungen sind für die Nutzung des Authentisierungschlüssels auf dem neuen Personalausweis besonders wichtig, weil die zentrale Funktion des Personalausweises in der Authentifizierung besteht. Soll er diese Authentifizierungsfunktion erfüllen, darf er keinesfalls für Signaturzwecke zweckentfremdet werden.

4.4.5 Datenschutzrechtliche Forderungen

Die Begründung des Gesetzgebers für die genannten problematischen Regelungen und Aktivitäten ist immer die gleiche: die mangelnde Verbreitung von qualifizierten Signaturen bei den Bürgern als Nutzenden. Anstatt aber die Verbreitung mit geeigneten Mitteln zu unterstützen, werden durch Einführung von Verfahren mit geringeren Anforderungen oder durch Einsatz von ungeeigneten Verfahren, die anderen Zwecken dienen, die Regelungen des Signaturgesetzes ausgehöhlt.

So fehlt es immer noch an einer interoperablen Signatur-Prüfsoftware auf Seiten der Empfangenden, im Beispiel des ElsterOnline-Portals also bei den Finanzbehörden. Eine solche Software könnte alle qualifizierten Signaturen einheitlich und zuverlässig prüfen, unabhängig davon, mit welcher Software sie erzeugt, auf welcher Karte mit welchem Betriebssystem der Schlüssel gespeichert ist und von welchem Zertifizierungsdienstanbieter das Signaturzertifikat ausgestellt wurde.

Das Henne-Ei-Problem der qualifizierten Signaturen - es gibt zu wenig Anwendungen, weil es zu wenige Signaturschlüsselinhaber und Signaturschlüsselinhaberinnen gibt und umgekehrt - feiert schon sein zehnjähriges Bestehen und auch andere große Anwendungsverfahren sind an seiner Lösung gescheitert. Es wird Zeit, endlich dieses Grundproblem in den Fokus zu nehmen und es sauber und zügig zu lösen.

Ich appelliere deshalb an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam mit den Datenschutzbeauftragten die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie ElsterOnline, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundes-, die Landesregierung und der Gesetzgeber sollten verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundes-, die Landesregierung und der Gesetzgeber sollten daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

5. Land

5.1 Justiz

5.1.1 Löschung von Daten der Polizei nach Ablehnung der Eröffnung des Hauptverfahrens beim Amtsgericht

Wenn ein Gericht die Eröffnung des Hauptverfahrens ablehnt, weil es der Überzeugung ist, dass der Beschuldigte keine Straftat begangen hat, muss die Staatsanwaltschaft die Polizei darüber informieren. Die Polizei muss ihre Daten löschen. Ein automatisiertes Verfahren zur Übermittlung der Information durch die Staatsanwaltschaft existiert. Eine automatische Weiterverarbeitung der von der Staatsanwaltschaft übermittelten Information seitens der Polizei findet nicht statt.

Ein hessischer Sportschütze, der im Besitz einer entsprechenden Genehmigung seiner Waffenscheinbehörde war, erwarb bei einer hessischen Firma eine Schusswaffe. Tags darauf zeigte er bei der Waffenscheinbehörde den Erwerb der Waffe an. Die Waffenscheinbehörde vertrat die Ansicht, der ihm erteilte Berechtigungsschein gelte für die erworbene Waffe nicht. Der Lauf der Waffe sei zu kurz; sie sei vom Schießsport ausgeschlossen. Also habe er ohne Erlaubnis eine Schusswaffe erworben und besessen. Sein Einwand, der Erwerbsberechtigungsschein enthalte keine entsprechende Einschränkung, half nichts. Auch ein Nachweis, wonach es für die von ihm ausgeübte sportliche Disziplin eine Ausnahmebestimmung bzgl. der Länge des Laufs gibt, stimmte die Behörde nicht um. Sie stellte die Waffe vorläufig sicher, schaltete die Polizei ein und erstattete Strafanzeige bei der Staatsanwaltschaft.

Auch die Staatsanwaltschaft konnte der Betroffene nicht überzeugen. Sie erhob Anklage wegen unerlaubten Waffenbesitzes und -erwerbes. Erst das zuständige Amtsgericht gab ihm Recht. Es lehnte die Eröffnung der Hauptverhandlung wegen eines Verstoßes gegen das Waffengesetz ab. Die Kosten des Verfahrens wurden der Staatskasse auferlegt. Nach dem Beschluss ermächtigte die von der Waffenscheinbehörde erteilte Genehmigung sowohl zum Erwerb als auch zum Besitz des tatgegenständlichen Revolvers.

Dennoch waren mit dieser eindeutigen Entscheidung noch nicht alle Spuren des Vorganges beseitigt. Als der Betroffene etwa ein halbes Jahr später in eine Polizeikontrolle geriet, wurde er nach Überprüfung seiner Personalien nach seiner Empfindung gründlicher kontrolliert als andere Personen. Auf Nachfrage erklärten ihm die Beamten, das sei schon so richtig, schließlich sei er schon einmal wegen eines Verstoßes gegen das Waffengesetz polizeilich in Erscheinung getreten. Nun wandte er sich an mich und fragte, ob er die Datenspeicherung der Polizei hinnehmen muss.

Meine Überprüfung hat ergeben, dass es im polizeilichen Auskunftssystem POLAS-HE eine Datenspeicherung zu dem Betroffenen gab. Sie lautete unter Angabe seiner Personalien und des staatsanwaltschaftlichen Aktenzeichens sinngemäß "Unbefugter Erwerb und Besitz einer Waffe - Revolver -". Wie das Verfahren ausgegangen war, war der Polizei nicht bekannt. Richtig wäre es gewesen, wenn die Staatsanwaltschaft der Polizei mitgeteilt hätte, dass die Eröffnung des Hauptverfahrens abgelehnt worden war, weil keine Straftat vorlag und wenn die Polizei daraufhin ihre Daten gelöscht hätte. Nach § 20 Abs. 4 HSOG sind Daten, die die Polizei bei der Verfolgung von Straftaten gewonnen hat, zu löschen, wenn der Verdacht entfallen ist. Dies war hier der Fall.

§ 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.

Dem behördlichen Datenschutzbeauftragten der zuständigen Polizeibehörde übersandte ich ein Exemplar des Gerichtsbeschlusses und bat ihn, die Rechtmäßigkeit der Datenspeicherung selbst zu prüfen. Er verfügte daraufhin sofort die Löschung. Nach einer Bestätigung der Umsetzung dieser Verfügung informierte ich den Betroffenen.
Warum die Polizei die Daten nicht gelöscht hatte, war nicht festzustellen. Es ist möglich, dass die Staatsanwaltschaft die Polizei nicht über den Ausgang des Verfahrens informiert hat. Es ist auch möglich, dass eine Information stattfand, aber nicht mitgeteilt wurde, dass der Verdacht entfallen ist und daher die Daten gelöscht werden müssen. Rechtsgrundlage für die Informationspflicht der Staatsanwaltschaft bildet § 484 Abs. 1 und 2 StPO.

§ 484 Abs. 1 und Abs. 2 stopp

(1) Die Staatsanwaltschaft teilt der Polizeibehörde, die mit der Angelegenheit befasst war, ihr Aktenzeichen mit.
(2) Sie unterrichtet die Polizeibehörden in den Fällen des Abs. 1 über den Ausgang des Verfahrens durch Mitteilung der Entscheidungsformel, der entscheidenden Stelle, sowie des Datums und der Art der Entscheidung. Die Übersendung eines Abdrucks der Mitteilung zum Bundeszentralregister ist zulässig, im Falle des Erfordernis auch des Urteils oder einer mit Gründen versehenen Einstellungsentscheidung.

Ebenso ist es möglich, dass die notwendige Information erging, aber von der Polizei nicht verarbeitet wurde. Ich mache "seit Jahren" (zuletzt 34. Tätigkeitsbericht, Ziff. 5.3.4, 33. Tätigkeitsbericht, Ziff. 5.1.4, 29. Tätigkeitsbericht, Ziff. 6.1.4, 28. Tätigkeitsbericht, Ziff. 5.3) darauf aufmerksam, dass die Polizei den Ausgang der von ihr bearbeiteten Ermittlungsverfahren nicht registriert. Die Landesregierung führt in ihren Stellungnahmen zu meinen Berichten, was die evtl. fehlende Informationsübermittlung durch die Staatsanwaltschaften angeht an, es handele sich um Einzelfälle und meine Quantifizierungen, nach denen die Polizei "oft" oder "häufig" nicht vom Verfahrensausgang informiert ist, seien nicht empirisch gesichert. Doch mit der Einführung von MESTA, dem Datenverarbeitungsverfahren der Staatsanwaltschaften, sollte es möglich sein, dieses Problem automatisiert zu lösen. Seitens der Polizei - hier wiederhole ich ein Verlangen aus dem Vorjahresbericht (Ziff. 5.3.4.2) - mangelt es an einer elektronischen Weiterverarbeitung der von der Justiz übermittelten Information über den Verfahrensausgang. Konkrete Schritte, wie sie in der Stellungnahme der Landesregierung zu meinem letzten Tätigkeitsbericht angekündigt sind, sind dazu bislang nicht zu erkennen.

5.1.2 Ist die Übermittlung von Daten über eine Lebenspartnerschaft an die Kirche bei einem Kirchenaustritt zulässig?

Die hessischen Amtsgerichte informieren die Kirchengemeinden über Kirchenaustritte ihrer Mitglieder. Aufgrund von kirchensteuerlichen Regelungen sind bei verheirateten Personen dabei auch Angaben über die Eheschließung und den Ehepartner notwendig. Bei Personen, die nicht verheiratet sind, sondern eine eingetragene Lebenspartnerschaft begründet haben, sind solche Angaben unzulässig.

Ein Frankfurter Einwohner hat sich an mich gewandt und angeführt, das Frankfurter Amtsgericht habe ihm schweren Schaden zugefügt. Es habe dem Gesamtverband der katholischen Kirchengemeinden in Frankfurt am Main eine Mitteilung über seinen Kirchenaustritt gemacht und dabei hinzugefügt, dass, seit wann und mit wem er in einer eingetragenen Lebenspartnerschaft steht. Der Gesamtverband der katholischen Kirchengemeinden in Frankfurt am Main habe diese Information an die Kirchengemeinde seines Heimatdorfes weitergegeben. Da er aus einer sehr dörflichen Gegend stamme, wisse nun sein

ganzes Heimatdorf und seine Familie von seiner gleichgeschlechtlichen Ausrichtung. Seine Familie habe mit ihm gebrochen. In seinem Heimatdorf werde er wie ein Aussätziger behandelt.

Er wandte sich an mich und legte mir eine Kopie der Mitteilung des Amtsgerichts vor. Sie trägt die Eingangsstempel von zwei Kirchengemeinden einschließlich der erwähnten Angaben. In nicht präziser Bezeichnung trägt die Mitteilung, bei der es sich nicht um ein Formular handelt, noch die Angabe wann und wo die "Eheschließung" stattfand.

Rechtsgrundlage der Datenübermittlung an die Kirchengemeinde ist ein seit dem Jahre 1920 geltendes Gesetz, betreffend den Austritt aus den Religionsgesellschaften öffentlichen Rechts i.d.F. des hessischen Gesetzes zur Vereinheitlichung der Verfahrensvorschriften über den Austritt aus einer öffentlich-rechtlichen Religionsgesellschaft vom 31. Mai 1974. Nach § 1 Abs. 1 dieses Gesetzes ist der Kirchenaustritt bei dem Amtsgericht zu erklären, das für den Wohnsitz des Betreffenden zuständig ist. Obwohl das Gesetz aus dem Jahre 1920 stammt, genügt die Regelung über die Information der Kirchengemeinde allgemeinen datenschutzrechtlichen Anforderungen:

§ 1 Abs. 3 Kirchenaustrittsgesetz
Die Geschäftsstelle des Amtsgerichts hat von der Abgabe und der etwaigen Zurücknahme der Austrittserklärung unverzüglich den Vorstand der Religionsgesellschaft, der der Erklärende angehört, zu benachrichtigen und demnächst dem Ausgetretenen eine Bescheinigung über den vollzogenen Austritt zu erteilen.

Damit ist grundsätzlich gegen eine Information der Kirchengemeinde über den Austritt ihres Mitgliedes nichts einzuwenden. Fraglich ist der Umfang der Datenübermittlung: Da das Gesetz einen genauen Datensatz nicht aufzählt, gilt der sich aus dem allgemeinen Datenschutzrecht herleitende Erforderlichkeitsgrundsatz. Erforderlich ist sicherlich eine Mitteilung über die Identifizierungsdaten des Betroffenen, also den Name, Vorname und Geburtsdatum. Als weiteres Identifizierungsdatum noch den Geburtsort anzugeben, wird nicht beanstandet. Auch zur Zuordnung von örtlichen Zuständigkeiten, die Adresse mit Wohnort und Straße zu bezeichnen, ist sicherlich erforderlich. Im Laufe der Geltung der Vorschrift hat sich die Verwaltungspraktik ergeben, bei verheirateten Personen auch noch Daten über die Eheschließung und den Ehepartner anzugeben. Soweit solche Informationen zur Feststellung des Wegfalles oder des Fortbestehens der Kirchensteuerpflicht notwendig sind, ist auch dagegen nichts einzuwenden. Eine steuerliche Gleichstellung von Eheschließungen und eingetragenen Lebenspartnerschaften ist aber gerade nicht erfolgt. Angaben über eine eingetragene Lebenspartnerschaft und über den Partner haben keine kirchensteuerrechtlichen Auswirkungen. Solche Angaben zu machen, war daher nicht erforderlich und damit unzulässig.

Mit der Feststellung, dass die in Rede stehende Datenübermittlung rechtswidrig erscheint, habe ich das Amtsgericht Frankfurt am Main um eine Stellungnahme gebeten. Das Amtsgericht Frankfurt am Main hat eingeräumt, dass die Niederschrift über den Kirchenaustritt der betreffenden Person insofern nicht korrekt war, als dort von einer "Eheschließung" die Rede war. Dabei habe es sich allerdings lediglich um eine versehentliche Falschbezeichnung gehandelt. Zur Anwendung des Erforderlichkeitsgrundsatzes in Bezug auf den zu übermittelnden Datenumfang widersprach mir das Gericht. Die Niederschrift über den Austritt erfolge auf der Grundlage eines bestimmten amtlichen Vordruckes des Oberlandesgerichts Frankfurt am Main. Dieser Vordruck sehe nun einmal die in Rede stehenden Angaben über die eingetragene Lebenspartnerschaft nebst den Angaben über den Lebenspartner vor. Bei der Mitteilung an die Kirchengemeinde sah sich das Gericht an die Angaben des Vordruckes gebunden.

Die sich nun aufdrängende Auseinandersetzung mit der Justizverwaltung erübrigte sich aus folgendem Grunde: In der Zwischenzeit hatte die betroffene Person beim Oberlandesgericht Frankfurt am Main Ansprüche auf immateriellen Schadensersatz geltend gemacht. Das Oberlandesgericht hat solche Ansprüche verneint, hat aber bezüglich des übermittelten Datenumfanges festgehalten, dass die Angaben "verpartnert" sowie wann, wo und mit wem die fälschlich so bezeichnete "Eheschließung" erfolgte, rechtswidrig waren. Es teilte meine Auffassung, dass neben dem eingangs zitierten Gesetz die allgemeinen Vorschriften des Datenschutzrechtes Anwendung finden und dass die Übermittlung von Angaben über eine eingetragene Lebenspartnerschaft nicht erforderlich und damit nicht zulässig ist. Dass der Vordruck, mit dem die Austrittserklärung dokumentiert wird, solche Angaben enthalte, beruhe auf einem Fehler. Dieser Fehler sei entstanden, weil der Vordruck bereits im Vorgriff auf das Inkrafttreten einer früheren Fassung des Lebenspartnerschaftsgesetzes angepasst worden sei. Diese frühere Fassung sah vor, die Lebenpartnerschaft steuerlich der Ehe völlig gleichzusetzen. Das letztlich verabschiedete Gesetz sieht eine solche Gleichstellung jedoch nicht vor.

Das Oberlandesgericht habe die hessischen Amtsgerichte mit einer Rundverfügung angewiesen, von der Aufnahme von Daten über eine eingetragene Lebenspartnerschaft in die Kirchenaustrittserklärung abzusehen. Offensichtlich ist diese Rundverfügung nicht ausreichend von allen hessischen Amtsgerichten zur Kenntnis genommen worden. Ich habe daher, um Wiederholungsfälle zu vermeiden, das Oberlandesgericht gebeten, den falschen Vordruck "aus dem Verkehr" zu ziehen und durch einen neuen Vordruck zu ersetzen. Eine Antwort steht noch aus. In meinem nächsten Tätigkeitsbericht werde ich über den Ausgang der Angelegenheit berichten.

Den Betroffenen habe ich entsprechend informiert. Soweit er die kircheninterne Informationsübermittlung rügte, musste ich ihn an die zuständige Datenschutzbeauftragte der katholischen Kirche verweisen. Allerdings wäre die nicht unproblematische kircheninterne Informationsverarbeitung nicht möglich gewesen, wenn sich bereits die Mitteilung des Amtsgerichts auf das tatsächlich Erforderliche beschränkt hätte.

5.2 Polizei und Strafverfolgung

5.2.1 Prüfung der Datei "Gewalttäter Sport"

Vor Beginn der Fußballweltmeisterschaft 2006 habe ich beim Polizeipräsidium Frankfurt einen Teil des hessischen Datenbestandes der Datei "Gewalttäter Sport" überprüft. Die Prüfung führte nicht zu Beanstandungen.

Bei der Datei "Gewalttäter Sport" handelt es sich um eine sogenannte Verbunddatei, die je nach Bedarf sowohl den Polizeibehörden der Länder als auch denen des Bundes zur Verfügung steht und zu der sowohl von Bundes- wie auch von Landespolizeidienststellen Daten angeliefert werden. Die Datei wird seit dem Jahre 1994 geführt. Auf Bundesebene koordiniert eine "Zentrale Informationsstelle Sporteinsätze" (ZIS) die Sammlung, Bewertung und Steuerung der anlassbezogen übermittelten Informationen aus dem In- und Ausland. Die Aufgaben der ZIS sind dem Landeskriminalamt Nordrhein-Westfalen übertragen. Auf Länderebene stehen ihr jeweils eine "Landesinformationsstelle Sporteinsätze" (LIS) gegenüber, welche die Verteilung und Bewertung der Informationen landesintern steuert. Diese LIS ist in Hessen dem Polizeipräsidium Frankfurt zugeordnet. Sie wird unterstützt von so genannten szenenkundigen Beamten, die ihren Dienstsitz am Sitz von Bundesligamannschaften haben und sowohl mit den Fußballvereinen wie auch mit Fanclubs zusammenarbeiten. Sie sind über die eventuell vorhandene Gewaltbereitschaft von Einzelpersonen, Fangruppen und Fanclubs bestens informiert. In der Datei "Gewalttäter Sport" sind bundesweit ca. 6.000 bis 6.500 Personen gespeichert. Etwa 300 Datensätze stammen von hessischen Polizeibehörden; davon stammt etwa die Hälfte aus dem Zuständigkeitsbereich des Polizeipräsidiums Frankfurt am Main.
Rechtsgrundlage für die Führung der Datei ist heute § 7 Abs. 1, § 8 Abs. 1, 2, 4 und 5 und § 9 des BKAG. Rechtsgrundlage für die Datenanlieferung der Länder ist § 13 Abs. 1 BKAG. Rechtsgrundlage für die Datenübermittlung an die Länder und für das Bereithalten der Daten zum Abruf für die Landespolizeibehörden ist § 10 Abs. 1 und 7 BKAG.

§ 10 BKAG

(1) Das Bundeskriminalamt kann an andere Polizeien des Bundes und an Polizeien der Länder personenbezogene Daten übermitteln, soweit dies zur Erfüllung seiner Aufgaben oder der des Empfängers erforderlich ist.

(7) Die Einrichtung eines automatisierten Verfahrens für die Übermittlung personenbezogener Daten durch Abruf ist nach Maßgabe des § 10 Abs. 2 und 3 des Bundesdatenschutzgesetzes nur zur Erfüllung vollzugspolizeilicher Aufgaben mit Zustimmung des Bundesministeriums des Innern und der Innenministerien und Senatsinnenverwaltungen der Länder zulässig, soweit diese Form der Datenübermittlung unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist.

Nach § 34 des BKAG hat das BKA für jede bei ihm geführte Datei in einer Errichtungsanordnung Festlegungen u.a. zur Rechtsgrundlage, Bezeichnung und Zweck der Datei, des betroffenen Personenkreises, der zu speichernden Daten sowie Fristen zur Prüfung und Löschung der Daten zu treffen. Im Jahre 2005 wurde die Errichtungsanordnung angesichts der bevorstehenden Fußballweltmeisterschaft 2006 und im Hinblick auf das politische und gesellschaftliche Verlangen an die Sicherheitsbehörden, unter Beobachtung der Weltöffentlichkeit einen friedlichen Verlauf der Fußballweltmeisterschaft 2006 - auch in Nachbetrachtung der schweren Ausschreitungen vorangegangener Veranstaltungen - zu gewährleisten, geändert. So wurden z.B. die aufgezählten Straftaten, die Anlass zur Aufnahme in die Datei bieten und u.a. Gewalt-, Raub- und Diebstahlsdelikte umfassen, um die Delikte "Verwenden von Kennzeichen verfassungswidriger Organisationen (§ 86a StGB), Volksverhetzung (§ 130 StGB) und Beleidigung (§ 185 StGB)" erweitert.

Nach der Errichtungsanordnung ermöglicht die Datei das Gewinnen von Anhaltspunkten für das Ergreifen von sachgerechten und wirksamen Eingriffsmaßnahmen. Sie liefert der Polizei Erkenntnisse für organisatorische und taktische Maßnahmen. Sie dient der Verhinderung gewalttätiger Auseinandersetzungen und sonstiger Straftaten im Zusammenhang mit Sportveranstaltungen. Anlässe die zur Datenspeicherung führen - immer im Zusammenhang mit Sportveranstaltungen festgestellt - können z.B. sein:

- eingeleitete und abgeschlossene Ermittlungsverfahren sowie rechtskräftige Verurteilungen wegen bestimmter bereits erwähnter Straftaten.
- Personalienfeststellungen, Platzverweise und Ingewahrsamnahmen zur Verhinderung anlassbezogener Straftaten, wenn Tatsachen die Annahme rechtfertigen, dass die Betroffenen Straftaten von erheblicher Bedeutung begehen werden.

Bei der erstgenannten Fallgruppe erscheint das Anknüpfen an "rechtskräftig Verurteilte" oder zumindest an "Beschuldigte" bestimmter im Zusammenhang mit Sportveranstaltungen begangener Straftaten, als Speichervoraussetzung ausreichend. Stichprobenhaft habe ich von den etwa 50 betroffenen Personen 15 Betroffene ausgewählt und um Vorlage der Kriminalakten gebeten. Die Speichervoraussetzungen waren bei allen gegeben. Gegen jeden der Betroffenen war wegen eines der in der Errichtungsanordnung aufgeführten Delikte, vorwiegend wegen Gewalttaten, begangen im Zusammenhang mit Sportveranstaltungen, Ermittlungsverfahren eingeleitet oder abgeschlossen oder rechtskräftige Verurteilungen ergangen.

Ich habe mich nun der zweiten Fallgruppe zugewandt. Zwar müssen auch hier Tatsachen die Annahme rechtfertigen, dass die Betroffenen Straftaten "von erheblicher Bedeutung" begehen werden, doch sind die Straftaten, die im Zusammenhang mit Ausschreitungen bei Großveranstaltungen zu befürchten sind, immer "von erheblicher Bedeutung". Und "Tatsachen, die die Annahme rechtfertigen, dass solche Taten bevorstehen" sind bei Fußballgroßveranstaltungen - mehr oder weniger stark ausgeprägt - immer vorhanden oder latent gegeben. Andererseits haben Betroffene geklagt, sie seien zu Unrecht in die Datei aufgenommen worden. Sie wären rein zufällig und unbeabsichtigt in eine Gruppe von Hooligans geraten und mit ihnen als gewaltbereit eingestuft worden.

Bei den szenenkundigen Beamten des Polizeipräsidiums Frankfurt, Polizeidirektion Süd, habe ich nun die Datenschutzkontrolle auf diejenigen Betroffenen konzentriert, zu denen keine Kriminalakten existieren. Sie waren also nicht Beschuldigte oder Verurteilte bestimmter Straftaten. Einer der anderen in der Errichtungsanordnung genannten Anlässe musste ausschlaggebend für die Datenspeicherung in der Datei sein. Dabei stellt eine bloße Personalienfeststellung keinen ausreichenden Anlass dar, um den mit der Datenspeicherung in der Datei "Gewalttäter Sport" verbundenen Eingriff in das Recht auf informationelle Selbstbestimmung als rechtmäßig zu erachten. Es handelte sich um 102 Personen. Im Ergebnis habe ich bei keinem der Betroffenen die Datenspeicherung beanstandet. Bei den meisten Betroffenen waren Platzverweise oder Ingewahrsamnahmen Anlass der Datenspeicherung. Zu jedem Einzelnen konnten mir die szenenkundigen Beamten der Polizeidirektion Süd bezeichnen, aufgrund welcher allgemeinen polizeilichen Lagebeurteilung und bei welchem Fußballspiel die Polizei eingeschritten war und welche Rolle die betroffene Person dabei spielte. Zwar war es oft so, dass keine Straftaten vorlagen, aber festgehalten war, dass durch gegenseitige Provokationen von Fangruppen tätliche Auseinandersetzungen unmittelbar bevorstanden und durch den Platzverweis oder die Ingewahrsamnahme Straftaten verhindert wurden. Jedenfalls war bei keinem der Betroffenen ausschließlich eine Personalienfeststellung Anlass der Datenspeicherung. Zusammenfassend ist festzustellen, dass von hessischen Polizeibehörden keine leichtfertigen oder unverhältnismäßigen Speicherungen in der Datei "Gewalttäter Sport" festzustellen waren.

5.2.2 Auskunft über eigene Daten zur Weitergabe an private Sicherheitsdienste

Das Recht auf Auskunft über Datenspeicherungen zur eigenen Person gehört zu den elementaren Ausprägungen des Grundrechtes auf informationelle Selbstbestimmung. Wenn Arbeitgeber von Stellenbewerbern verlangen, ihrer Bewerbung eine von der Polizei ausgestellte Auskunft über eigene Daten beizufügen, stellt dies ein Missbrauch dieses Rechts dar.

Im Berichtszeitraum wurde folgendes datenschutzrechtliche Problem gleich von zwei Seiten an mich herangetragen:

Ein Einwohner aus dem Westerwald schilderte, er habe sich bei einem Frankfurter Sicherheitsdienst beworben. Das Unternehmen verlange von ihm, dass er seinen Bewerbungsunterlagen eine polizeiliche Selbstauskunft nach § 29 Abs. 1 HSOG, welche er beim HLKA beantragen möge, hinzufügen soll.

§ 29 Abs. 1 HSOG

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.

Dort sei ihm auf Nachfrage mitgeteilt worden, solche Anfragen würden nicht schriftlich beantwortet. Die Sicherheitsunternehmen würden auf diesem Wege Informationen erlangen, die ihnen nicht zustehen. Es handele sich um einen Missbrauch seines datenschutzrechtlichen Informationsanspruchs, dem die Behörde nicht Vorschub leisten will. Der Betroffene wandte sich daraufhin an mich.

Tatsächlich hatte sich schon einige Wochen vorher das HLKA mit mir in Verbindung gesetzt und mich über eine Verfahrensweise informiert, die einem Missbrauch des Auskunftsrechts begegnen sollte. Es gingen dort Auskunftsanträge ein, die offensichtlich nicht in Wahrnehmung des datenschutzrechtlichen Informationsanspruchs, sondern auf Betreiben eines Dritten, und zwar meist von einem gewerblichen Sicherheitsunternehmen gestellt wurden. Teilweise wurde das Drittinteresse offenbar, indem das Unternehmen selbst die formularmäßig aufbereiteten und in Form und Ausdruck identischen Auskunftsanträge päckchenweise dem HLKA zukommen ließ. Da die Anträge auch noch mit einer entsprechenden Einverständniserklärung versehen waren, sollten die Antworten gleich dem Unternehmen zurückgeschickt werden. An einem solch offensichtlichen Missbrauch des Auskunftsrechts wollte sich das HLKA verständlicherweise nicht beteiligen.

Andererseits hat das Verlangen der Sicherheitsunternehmen in § 34a der Gewerbeordnung durchaus einen rechtlichen Hintergrund. Danach darf ein Bewachungsunternehmer mit der Durchführung von Bewachungsaufgaben nur Personen beschäftigen, die u.a. die erforderliche Zuverlässigkeit besitzen.

Wie diese Zuverlässigkeit zu prüfen ist, lässt die Gewerbeordnung offen. Pflichtwidrig würde ein Bewachungsunternehmer handeln, würde er die erforderliche Zuverlässigkeit einfach außer Acht lassen. Er benötigt also Anhaltspunkte, um die Zuverlässigkeit eines Bewerbers beurteilen zu können. Dabei hätte eine polizeiliche Selbstauskunft, aus der hervorgeht, dass über den Antragsteller keinerlei Datenspeicherung vorliegt, die Wirkung eines "Persilscheines". Nun können Personen, über die die Polizei in ihren Informationssystemen keine Daten gespeichert hat, sicherlich als ausreichend zuverlässig eingeschätzt werden; das Unternehmen könnte sich daher darauf berufen, dass es bei dieser Sachlage seiner Prüfpflicht Genüge getan hat. Doch diese Intention widerspricht den Vorstellungen des Gesetzgebers. Für die gewünschte Prüfung steht dem Unternehmer das Instrument zur Verfügung, sich ein sog. Führungszeugnis nach § 30 BZRG vorlegen zu lassen.

§ 30 Abs. 1 und 2 BZRG

(1) Jeder Person, die das 14. Lebensjahr vollendet hat, wird auf Antrag ein Zeugnis über den sie betreffenden Inhalt des Zentralregisters erteilt (Führungszeugnis). Hat der Betroffene einen gesetzlichen Vertreter, so ist auch dieser antragsberechtigt. Ist der Betroffene geschäftsunfähig, so ist nur sein gesetzlicher Vertreter antragsberechtigt.
(2) Der Antrag ist bei der Meldebehörde zu stellen.

Dieses Führungszeugnis unterscheidet sich erheblich von der Selbstauskunft der Polizei.

Zunächst ist es ausdrücklich für Drittinteressenten z.B. einen potentiellen Arbeitgeber geschaffen, für den die Unbescholtenheit seines Bewerbers wegen der Art der Tätigkeit von Bedeutung ist. In das Führungszeugnis werden im Wesentlichen alle strafrechtlichen Verurteilungen eingetragen. Hinzu kommen einige Entscheidungen von Verwaltungsbehörden, wie z.B. Passversagungen oder die Versagung waffenrechtlicher Erlaubnisse. Auch die Einstellung eines Strafverfahrens wegen Schuldunfähigkeit ist einzutragen. Aus Resozialisierungsgründen gibt es im Falle von nur einer Eintragung im Register eine Bagatellschwelle, z.B. für Verurteilungen, durch die auf Geldstrafe von nicht mehr als 90 Tagessätzen erkannt worden ist. Die Regelung (§ 32 BZRG) ist durch Verweise, Ausnahmen und Rückausnahmen recht kompliziert, doch sie ist enumerativ und für jedermann im Gesetz nachzulesen.

Es gibt im Bundeszentralregisterrecht neben den Vorschriften für das Führungszeugnis auch noch einen alle Eintragungen im Register umfassenden datenschutzrechtlichen Informationsanspruch (§ 42). Damit diese Selbstauskunft von den Betroffenen nicht als Leumundszeugnis oder sozusagen als erweitertes Führungszeugnis für dritte Interessenten verwendet werden kann, gibt es Vorkehrungen. So wird einem Anfrager diese Auskunft nur zur Einsicht vorgelegt - nicht zur Mitnahme. Sie kann auch nur persönlich entgegengenommen werden.

§ 42 Abs. 1 BZRG

Einer Person, die das 14. Lebensjahr vollendet hat, wird auf Antrag mitgeteilt, welche Eintragungen über sie im Register enthalten sind. § 30 Abs. 1 Satz 2, 3 gilt entsprechend. Erfolgt die Mitteilung nicht durch Einsichtnahme bei der Registerbehörde, so ist sie, wenn der Antragsteller im Geltungsbereich dieses Gesetzes wohnt, an ein von ihm benanntes Amtsgericht zu senden, bei dem er die Mitteilung persönlich einsehen kann. Befindet sich der Betroffene in amtlichem Gewahrsam einer Justizbehörde, so tritt die Anstaltsleitung an die Stelle des Amtsgerichts. Wohnt der Antragsteller außerhalb des Geltungsbereichs dieses Gesetzes, so ist die Mitteilung an eine von ihm benannte amtliche Vertretung der Bundesrepublik Deutschland zu senden, bei der er die Mitteilung persönlich einsehen kann. Nach Einsichtnahme ist die Mitteilung vom Amtsgericht, der Anstaltsleitung oder der amtlichen Vertretung der Bundesrepublik Deutschland zu vernichten.

Ganz anders die Speicherung personenbezogener Daten durch die Polizei: Sie ergeht gerade nicht, um eine Interessenlage Dritter zu erfüllen, sondern findet zur Aufgabenerfüllung der Polizei statt. Dabei steht neben der Gefahrenabwehr die vorbeugende Bekämpfung von Straftaten im Vordergrund. Sie hat präventiven, nicht repressiven Charakter. Künftige Straftaten sollen leichter aufgeklärt - noch besser - verhindert werden. Die Polizei speichert Daten nicht nur über Verurteilungen. Zwar muss sie ihre Daten löschen, wenn ein Verdacht entfallen ist (s. Ziff. 5.1.1). Doch die Bagatellschwelle orientiert sich in erster Linie nicht an Resozialisierungsaspekten, sondern an der Erforderlichkeit und der Verhältnismäßigkeit. So darf die Polizei auch Daten über Fälle speichern, die noch gar nicht abgeschlossen sind oder bei denen die Justiz, z.B. aus Gründen der Billigkeit, auf eine strafrechtliche Verurteilung verzichtete oder die sie gegen Zahlung einer Geldauflage einstellte. Selbstverständlich muss sie einen Betroffenen im Rahmen einer Selbstauskunft auch über solche Datenspeicherungen informieren. Doch dass der Betroffene im Rahmen einer Selbstauskunft gezwungen wird, seinem künftigen Arbeitgeber solche Informationen zu offenbaren, widerspricht dem datenschutzrechtlichen Grundgedanken, der dem Informationsrecht zugrunde liegt.

Das HLKA informierte mich, es wolle Anfrager, die offensichtlich eine fremdbestimmte Selbstauskunft beantragen, künftig darüber informieren, dass das Auskunftsrecht nach § 29 HSOG ausschließlich dem Betroffenen selbst vorbehalten ist. Weiterhin wolle es auf die zitierten Regelungen des BZRG hinweisen und entsprechend dem Rechtsgedanken in § 42 BZRG im Falle der Aufrechterhaltung des Auskunftsverlangens dem Anfrager anbieten, die Auskunft in einem Gespräch in einer Polizeidienststelle zu erläutern.

Ein Erfahrungsaustausch mit den anderen Landesdatenschutzbeauftragten und dem Bundesdatenschutzbeauftragten führte zu dem Ergebnis, dass das Problem sowohl bei den Bundesbehörden als auch in etwa der Hälfte der anderen Länder mehr oder weniger stark ausgeprägt vorkam. Dort wo es aufgetaucht ist, wurde ihm so oder ähnlich wie vom HLKA vorgesehen begegnet. Ich habe dem HLKA signalisiert, gegen das Verfahren vorläufig nichts einzuwenden. Übrig bleibt eine gewisse Unsicherheit, die einerseits beinhaltet, dass ein fremdbestimmtes Auskunftsverlangen nicht als ein solches erkannt wird. Andererseits könnte ein selbstbestimmtes Auskunftsverlangen fehlerhafterweise als fremdbestimmt eingeschätzt werden und der Betroffene sich bei der Geltendmachung seiner Datenschutzrechte gehindert betrachten. Zumindest Letzteres wurde seit Einführung des Verfahrens von niemandem angeführt.

5.2.3 Regelanfrage bei der Polizei vor ausländerrechtlichen Entscheidungen

Nur bei bestimmten Entscheidungen und bei Entscheidungen über Angehörige bestimmter Nationalitäten muss eine besondere Sicherheitsüberprüfung zum Zwecke der Terrorismusbekämpfung stattfinden. Eine generelle Anfrage der Ausländerbehörde bei der Polizei vor jeglicher ausländerrechtlichen Entscheidung ist nicht zulässig.
Ein Frankfurter Rechtsanwalt hatte bei einer Ausländerbehörde im Rhein-Main-Gebiet die Erteilung einer befristeten Aufenthaltserlaubnis für einen eritreischen Staatsangehörigen beantragt. Als er nach einiger Zeit nachfragte, wann mit der Erteilung zu rechnen sei, erklärte die Ausländerbehörde, eine Sicherheitsanfrage bei der Polizei sei noch nicht beantwortet. Der Anwalt meinte, eine solche Anfrage sei nur gerechtfertigt, wenn Anhaltspunkte dafür vorliegen, dass Sicherheitsinteressen der beantragten Erlaubnis entgegenstehen. Solche Anhaltspunkte lägen bei seinem Mandanten nicht vor. Er wandte sich an mich.

Tatsächlich wurde im Zuge des Terrorismusbekämpfungsgesetzes ein Verfahren eingeführt, wonach die Ausländerbehörden bei Angehörigen bestimmter Nationalitäten vor der Erteilung von befristeten Aufenthaltsgenehmigungen unter anderem die

Polizei um eine Stellungnahme bittet (s. meinen 27. Tätigkeitsbericht, Ziff. 6.1). Rechtgrundlage des Verfahrens sind nach der Neuregelung des Ausländerrechts die §§ 5 Abs. 4 und 54 Nr. 5 und 5a des AufenthG.

§ 5 Abs. 4 AufenthG

Die Erteilung eines Aufenthaltstitels ist zu versagen, wenn einer der Ausweisungsgründe nach § 54 Nr. 5 oder 5 a vorliegt. Von Satz 1 können in begründeten Einzelfällen Ausnahmen zugelassen werden, wenn sich der Ausländer gegenüber den zuständigen Behörden offenbart und glaubhaft von seinem sicherheitsgefährdenden Handeln Abstand nimmt. Das Bundesministerium des Innern oder die von ihm bestimmte Stelle kann in begründeten Einzelfällen vor der Einreise des Ausländers für den Grenzübertritt und einen anschließenden Aufenthalt von bis zu sechs Monaten Ausnahmen von Satz 1 zulassen.

§ 54 AufenthG

Ein Ausländer wird in der Regel ausgewiesen, wenn
1. - 4. ….

5. Tatsachen die Schlussfolgerung rechtfertigen, dass er einer Vereinigung angehört oder angehört hat, die den Terrorismus unterstützt oder eine derartige Vereinigung unterstützt oder unterstützt hat; auf zurückliegende Mitgliedschaften oder Unterstützungshandlungen kann die Ausweisung nur gestützt werden, soweit diese eine gegenwärtige Gefährlichkeit begründen,

5a. er die freiheitlich demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland gefährdet oder sich bei der Verfolgung politischer Ziele an Gewalttätigkeiten beteiligt oder öffentlich zur Gewaltanwendung aufruft oder mit Gewaltanwendung droht.

Nach einem Erlass des HMDIS erfolgt diese Prüfung bei Anträgen auf unbefristete Aufenthaltsgenehmigungen bei allen Ausländern. Bei befristeten Aufenthaltsgenehmigungen gilt der Erlass nur bei bestimmten Staatsangehörigen. Eritreische Staatsangehörige gehören bei befristeten Anträgen nicht zum Kreise der Betroffenen.

Auf meine Nachfrage erklärte die Ausländerbehörde, sie kenne den Erlass zur Intensivierung der Terrorismusbekämpfung. Sie war aber der Ansicht, sie habe zwecks Prüfung der allgemeinen Genehmigungsvoraussetzungen in jedem Falle eine Anfrage unter anderem bei der Polizei zu tätigen.

Diese Haltung entbehrte einer Rechtsgrundlage. Dem allgemeinen Ansinnen der Ausländerbehörde ist Rechnung getragen durch die Befugnis, im Ausländerzentralregister eventuell gespeicherte Daten abzurufen. Für den ansonsten noch zu prüfenden "gesicherten Lebensunterhalt" muss der Ausländer selbst Nachweise erbringen. Evtl. anhängige Strafverfahren ergeben sich aus Strafanzeigen, Anklageschriften, Urteilen etc., die der Ausländerbehörde von der Polizei bzw. den Strafverfolgungsbehörden unaufgefordert zu übermitteln sind.

Ich schaltete die Aufsichtsbehörde ein. Das HMDIS wies die betreffende Ausländerbehörde darauf hin, dass eine Rechtsgrundlage für eine generelle Anfrage bei den Polizeibehörden nicht vorhanden ist und zu unterbleiben hat.

5.3 Verfassungsschutz

5.3.1 Entwurf für ein Sicherheitsüberprüfungsgesetz

Das Hessische Ministerium des Innern und für Sport hat im September 2006 einen Entwurf für ein Sicherheitsüberprüfungsgesetz vorgelegt, zu dem ich Stellung genommen haben.

In dem Gesetzentwurf werden die Voraussetzungen und das Verfahren zur Überprüfung von Personen geregelt, die von einer Behörde oder einer anderen öffentlichen Stelle mit einer sicherheitsempfindlichen Aufgabe betraut werden.

Bisher erfolgte die Überprüfung der betroffenen Personen ohne ausreichende Rechtsgrundlage. Es existierte lediglich eine Aufgabenzuweisung an den Verfassungsschutz in § 2 Abs. 5 VerfSchG.

§ 2 Abs. 5 VerfSchG

Das Landesamt für Verfassungsschutz wirkt auf Ersuchen der zuständigen Stellen mit

1. bei der Sicherheitsüberprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können.

Außerdem gibt es Richtlinien der Landesregierung aus dem Jahr 1962, die im Laufe der Jahre abgeändert wurden.

Bei der Sicherheitsüberprüfung handelt es sich um sehr weitgehende Eingriffe in das Recht auf informationelle Selbstbestimmung, beispielsweise werden auch Ehegatten oder Verwandte in die Überprüfung einbezogen. Ab einer bestimmten Ermächtigungsstufe werden nicht nur vom Betroffenen angegebene Referenzpersonen, sondern auch weitere Personen, von denen der Betroffene nichts weiß, vom Landesamt für Verfassungsschutz befragt.

Meine Amtsvorgänger und ich haben deshalb immer wieder darauf hingewiesen, dass es einer konkreten gesetzlichen Regelung für die Sicherheitsüberprüfung bedarf. Nachdem auf Bundesebene bereits 1994 eine gesetzliche Regelung erfolgte und die anderen Bundesländer nachzogen, ist Hessen jetzt das letzte Bundesland, das ein Gesetz erarbeitet.

Der nunmehr vorliegende Gesetzentwurf wird deshalb von mir grundsätzlich begrüßt.

Die Regelungen des hessischen Entwurfs sind weitgehend mit denjenigen des Sicherheitsüberprüfungsgesetzes auf Bundesebene aus dem Jahr 1994 identisch. Dies beruht darauf, dass bei der gegenseitigen Anerkennung von Sicherheitsüberprüfungen zwischen dem Bund und den Ländern oder den Ländern untereinander Probleme vermieden werden sollen.

In einigen Punkten weicht der Entwurf allerdings vom Bundesgesetz ab. Derzeit befinde ich mich noch in der Diskussion mit dem HMDIS.

5.4 Verkehrswesen

5.4.1 Missbräuchliche Nutzung von Daten der örtlichen Fahrzeugregister durch Bedienstete einer Ordnungsbehörde?

Durch automatisierte Protokollierung kann ein unzulässiger Zugriff auf Daten aufgedeckt werden. Bei Abfrageterminals ist aber zusätzlich organisatorisch sicherzustellen, dass erforderlichenfalls neben dem Nutzer des Terminals auch der Zweck der Abfrage und der Datenempfänger festgestellt werden kann.

Eine Bürgerin wandte sich im vergangenen Jahr an mich, nachdem sie ein anonymes Schreiben erhalten hatte, in dem ihr ein angeblich unnötiger Überholvorgang mit ihrem Pkw vorgeworfen wurde. In diesem Schreiben wurde neben dem Kfz-Kennzeichen und ihrer Anschrift auch ihr Geburtsdatum sowie die Namen und das Alter der Familienangehörigen genannt. Der anonyme Briefschreiber kündigte an, sich weitere Schritte gegen sie vorzubehalten. Die Petentin fühlte sich durch dieses Schreiben bedroht und fragte, wie der Absender oder die Absenderin an diese Informationen gelangen konnte.

Aufgrund der genutzten Daten (Kfz-Daten und Meldedaten) kam eine - unzulässige - Nutzung von Einwohnermeldedaten und Zulassungsdaten in Frage.

In Hessen erfolgt der automatisierte Abruf unter Angabe des Kfz-Kennzeichens auf die Daten der örtlichen Fahrzeugregister durch Ordnungsbehörden seit dem 1. Januar 1999 mittels eines von der KIV entwickelten Verfahrens (Transaktion AUGE = **Au**skunft **Ge**meinde).
Hierbei haben die örtlichen Ordnungsbehörden der kreisangehörigen Städte und Gemeinden einen Zugriff auf den Fahrzeug-Gesamtbestand der KIV in Hessen, allerdings nur, soweit es sich um die Verfolgung von Ordnungswidrigkeiten nach § 24 oder § 24a StVG handelt.

§ 24 StVG

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig einer Vorschrift einer auf Grund des § 6 Abs. 1 erlassenen Rechtsverordnung oder einer auf Grund einer solchen Rechtsverordnung ergangenen Anordnung zuwiderhandelt, soweit die Rechtsverordnung für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist. Die Verweisung ist nicht erforderlich, soweit die Vorschrift der Rechtsverordnung vor dem 1. Januar 1969 erlassen worden ist.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße geahndet werden.

§ 24a StVG

(1) Ordnungswidrig handelt, wer im Straßenverkehr ein Kraftfahrzeug führt, obwohl er 0,25 mg/l oder mehr Alkohol in der Atemluft oder 0,5 Promille oder mehr Alkohol im Blut oder eine Alkoholmenge im Körper hat, die zu einer solchen Atem- oder Blutalkoholkonzentration führt.

(2) Ordnungswidrig handelt auch, wer unter der Wirkung eines in der Anlage zu dieser Vorschrift genannten berauschenden Mittels im Straßenverkehr ein Kraftfahrzeug führt. Eine solche Wirkung liegt vor, wenn eine in dieser Anlage genannte Substanz im Blut nachgewiesen wird. Satz 1 gilt nicht, wenn die Substanz aus der bestimmungsgemäßen Einnahme eines für einen konkreten Krankheitsfall verschriebenen Arzneimittels herrührt.

(3) Ordnungswidrig handelt auch, wer die Tat fahrlässig begeht.

(4) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu eintausendfünfhundert Euro geahndet werden.

(5) Das Bundesministerium für Verkehr, Bau und Stadtentwicklung wird ermächtigt, durch Rechtsverordnung im Einvernehmen mit dem Bundesministerium für Gesundheit und dem Bundesministerium der Justiz mit Zustimmung des Bundesrates die Liste der berauschenden Mittel und Substanzen in der Anlage zu dieser Vorschrift zu ändern oder zu ergänzen, wenn dies nach wissenschaftlicher Erkenntnis im Hinblick auf die Sicherheit des Straßenverkehrs erforderlich ist.

Rechtsgrundlage für die Anwendung dieses Verfahrens ist § 36 Abs. 2 letzter Satz StVG i. V. m. § 26 Abs. 1 StVG. Die hier genannten Verwaltungsbehörden wurden in Hessen durch Verordnung vom 7. April 1992 (GVBl. I S. 134, verkündet

am 15. April 1992, 61-42/43) festgelegt. § 3 dieser Verordnung stellt fest, dass für die Verfolgung von Ordnungswidrigkeiten nach §§ 24 und 24a StVG einschließlich der Erteilung von Verwarnungen, der Erhebung von Verwarnungsgeldern, der Einstellung von Verfahren und der Kostenentscheidungen nach § 25a Abs. 2 StVG die Bürgermeister (Oberbürgermeister) als örtliche Ordnungsbehörden zuständig sind.

§ 36 Abs. 2 letzter Satz StVG
…
Satz 1 gilt entsprechend für den Abruf der örtlich zuständigen Polizeidienststellen der Länder und Verwaltungsbehörden im Sinne des § 26 Abs. 1 aus den jeweiligen örtlichen Fahrzeugregistern.

§ 26 Abs. 1 StVG

Bei Ordnungswidrigkeiten nach § 24, die im Straßenverkehr begangen werden, und bei Ordnungswidrigkeiten nach § 24a ist Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten die Behörde oder Dienststelle der Polizei, die von der Landesregierung durch Rechtsverordnung näher bestimmt wird. Die Landesregierung kann die Ermächtigung auf die zuständige oberste Landesbehörde übertragen.

Aufgrund meiner Nachforschungen konnte ich feststellen, dass zu dem Kfz-Kennzeichen der Petentin im genannten Zeitraum tatsächlich ein automatisierter Abruf mittels des Verfahrens AUGE stattgefunden hat, bei dem allerdings kein Ordnungswidrigkeitenverfahren eingeleitet wurde. Da jedem Terminal, von dem aus diese Anfragen möglich sind, eine sog. Identifikationsnummer zugeordnet ist, stand zweifelsfrei fest, von welchem Terminal in welcher Behörde die Abfrage durchgeführt wurde.

Da das anonyme Schreiben auch Angaben über Familienangehörige der Petentin enthielt, habe ich ebenfalls nachgeprüft, ob eine Anfrage auf die EWO-Datei der betroffenen Kommune erfolgt ist. Eine Auswertung der Protokollsätze seitens der KIV ergab jedoch keine Zugriffe auf die Datensätze der in Frage kommenden Personen in dem entsprechenden Zeitraum.

Aufgrund der von mir festgestellten Angaben habe ich daraufhin die betroffene Ordnungsbehörde mit dem Vorgang konfrontiert und um Stellungnahme gebeten.

Zur Sachverhaltsaufklärung hat der Behördenleiter umfangreiche interne Gespräche geführt und Nachforschungen veranlasst. Dabei wurde festgestellt, dass aufgrund der internen Organisationsstruktur der Behörde der Mitarbeiter, von dessen Terminal die Abfrage erfolgte, täglich mehrfach von Mitarbeiterinnen und Mitarbeitern seiner Arbeitsgruppe telefonisch gebeten wird, Halter von bestimmten Kraftfahrzeugen zu ermitteln, die beispielsweise ihr Fahrzeug extrem verkehrsbehindernd abgestellt haben. In diesen Fällen können die Mitarbeiterinnen und Mitarbeiter dann direkt Kontakt mit dem Fahrzeughalter aufnehmen, ohne dass dem Halter Abschleppkosten entstehen. Sowohl diese Halteranfragen als auch die Datenweitergabe an die anfragenden Mitarbeiterinnen und Mitarbeiter wurden in der Vergangenheit in der Behörde nicht schriftlich dokumentiert.

Der betreffende Mitarbeiter konnte sich zum Zeitpunkt der Befragung durch den Behördenleiter nicht mehr bewusst an eine Halterabfrage zu dem entsprechenden Kfz-Kennzeichen erinnern. Auch den in Frage kommenden Mitarbeiterinnen und Mitarbeiter seiner Arbeitsgruppe war das betreffende Kennzeichen im Zusammenhang mit der Halteranfrage unbekannt bzw. sie versicherten, dass sie den betreffenden Mitarbeiter nicht gebeten haben, ihnen den Halter dieses PKW mitzuteilen.

Nach diesen Aussagen, weil sowohl der Grund für die Halterabfrage als auch der Datenempfänger nicht schriftlich notiert worden sind, ließ sich nur noch feststellen, dass diese Abfrage tatsächlich erfolgt ist. Die Frage nach der rechtlichen Zulässigkeit und Verantwortlichkeit für die missbräuchliche Nutzung der Daten für das anonyme Schreiben musste offenbleiben.

Aufgrund dieses aktuellen Falles wurde in der betroffenen Kommune mit einer Bürgermeisterverfügung u.a. festgelegt, dass, soweit personenbezogene Daten durch Behördenmitarbeiter abgefragt und weitergegeben werden, dies ausschließlich bei Nachweis eines dienstlichen Grundes erfolgen darf. Diese Abfragen und Datenübermittlungen müssen zukünftig so dokumentiert werden, dass Abfragezweck, Datenumfang und Datenempfänger nachvollziehbar sind.

Unter Beachtung der nunmehr vorliegenden Verfügung des Behördenleiters wird in Zukunft eine Klärung derartiger Halterabfragen unter Vermeidung einer missbräuchlichen Nutzung möglich sein.

Ich behalte mir vor, die Einhaltung der Bürgermeisterverfügung vor Ort zu prüfen.

5.5 Schulen und Schulverwaltung

5.5.1 Angabe der privaten Telefonnummer von Lehrern gegenüber der Schulverwaltung

Hessische Lehrkräfte können darauf vertrauen, dass die Schule ihre private Telefonnummer nicht Dritten, etwa Eltern der betreuten Schüler, ohne ihre Zustimmung übermittelt.

Die datenschutzrechtliche Anfrage eines schulischen Datenschutzbeauftragten offenbarte folgenden Sachverhalt:
Im Rahmen der Einstellung einer verbeamteten Lehrkraft verlangte die Schulverwaltung von dieser u.a. die Angabe der privaten Telefonnummer. Die Lehrkraft verweigerte jedoch diese Bekanntgabe mit dem Hinweis, diese Nummer könnte von der Schulverwaltung u.a. an verschiedene Eltern weitergeleitet werden. Daraus entstünden jedoch oftmals unzumutbare

Belästigungen. Trotz der Zusicherung seitens der Schulverwaltung, eine solche Übermittlung erfolge keinesfalls ohne schriftliche Einwilligung, wurde zunächst die Verweigerung aufrechterhalten.

Die Prüfung der Rechtslage ergab folgende Feststellungen:
Grundsätzlich darf nach § 34 Abs. 1 HDSG die Schule nur die Daten der Lehrkräfte erheben und weiterverarbeiten, die sie u.a. für die Durchführung des Dienstverhältnisses benötigt.

§ 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.

Diese Vorschrift wird im Kontext der Schulverwaltung allerdings konkretisiert durch Anlage 2 der "Verordnung zur Verarbeitung personenbezogener Daten in Schulen".

Anlage 2

Daten von Lehrerinnen und Lehrern, die in der Schule für die in § 1 angegebenen Zwecke verarbeitet werden dürfen:

Abkürzung des Namens,
Name, Geburtsname, Vorname(n),
Geschlecht,
Anschrift,
Telefon,
Dienstverhältnis,
Lehramt,
Funktion innerhalb der Schule,
Lehrbefähigung (jeweils Fach und Art),
Unterrichtserlaubnis (Art und Ablauftermin),
Pflichtstundensoll/Regelpflichtstunden,
erteilter Unterricht (Wochenstunden, Fächer, Klassen/Kurse),
Mehrarbeit,
Unterricht an anderen Schulen (Schule, Schulform, Wochenstunden, Fächer, Klassen/Kurse),
Anrechnung dienstlicher Tätigkeiten (Wochenstunden, Grund),
Pflichtstundenermäßigung (Wochenstunden, Grund),
Sprechstunde (Tag, Zeit, Raum),
Freistellungen.

Der Zweck des Datums der privaten Telefonnummer liegt in den Besonderheiten des Schulbetriebes begründet: Vielfältige Situationen im Schulbetrieb, plötzlicher Unterrichtseinsatz, dringende fachliche und organisatorische Nachfragen erfordern oftmals eine umgehende Kontaktaufnahme über die private Telefonnummer der Lehrkräfte. Insoweit kann hier die Erforderlichkeit der Datenerhebung zweifellos angenommen werden. Die datenschutzrechtliche Erlaubnis der Schule, personenbezogene Daten zu verarbeiten, führt aber nicht zwangsweise auch zur Auskunftspflicht der Betroffenen. Diese muss sich ebenfalls aus einer Rechtsvorschrift ergeben. Im vorliegenden Fall ergibt sie sich aus § 83 Abs. 3 HSchulG.

§ 83 Abs. 3 HSchulG

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

Danach haben die Lehrkräfte der Schule die erforderlichen Angaben zu überlassen. Dazu zählt also auch die private Telefonnummer, selbst wenn sie von den Betroffenen als besonders sensibel angesehen wird und nicht in öffentlichen Registern verfügbar ist.

Die Befürchtungen der betroffenen Lehrkraft reichen nicht aus, eine Verweigerung zu rechtfertigen. Denn die Weitergabe dieser privaten Telefonnummer innerhalb der Schulverwaltung, insbesondere an andere Lehrkräfte oder an Eltern, unterliegt zunächst dem allgemeinen datenschutzrechtlichen Verbot. Die Weitergabe innerhalb der Schule wäre nur durch § 34 Abs. 1 HDSG zu rechtfertigen. Die normale Kommunikation zwischen den Lehrkräften einer Schule erfolgt grundsätzlich in der Schule in mündlicher oder schriftlicher Form (Postfach). Gleichwohl wird oftmals durch die Lehrkräfte selber eine Liste privater Telefonnummern erstellt und verteilt, die Eintragung in diese erfolgt allerdings freiwillig.
Bei der Weitergabe der Telefonnummer an Dritte, insbesondere Eltern, hätte die Schulverwaltung § 34 Abs. 2 HDSG zu beachten.

§ 34 Abs. 2 HDSG

Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert

oder der Betroffene eingewilligt hat. Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

Da selbst die Eltern der Schüler, die die betroffene Lehrkraft betreut, generell kein "rechtliches Interesse" an der privaten Telefonnummer nachweisen können, darf die Übermittlung nur erfolgen, wenn die Lehrkraft dem vorher schriftlich zugestimmt hat.
Nachdem die Schulverwaltung erklärt hat, dass eine Übermittlung der Telefonnummer nur mit schriftlicher Einwilligung erfolgt, also ausdrücklich die Einhaltung der Rechtslage zugesichert hat, durfte die Angabe der Telefonnummer nicht verweigert werden. Im Übrigen können Lehrkräfte sich auch grundsätzlich darauf verlassen, dass die Schulverwaltung diese rechtlichen Bedingungen beachtet.

5.5.2 Umfrage an Wiesbadener Schulen

Im Rahmen der Weiterentwicklung von Unterrichtsmaterialien durch das Institut für Qualitätsentwicklung wurden Lehrkräfte mittels Fragebögen über ihre Unterrichtsgestaltung befragt. Bei solchen Befragungen ist sicherzustellen, dass die Befragten über die datenschutzrechtlichen Bedingungen der Befragung rechtzeitig informiert werden.

Im Rahmen einer Beschwerde teilte mir eine Lehrerin folgenden Sachverhalt mit:
Das Institut für Qualitätsentwicklung betreut u.a. landesweite Projekte zur Evaluierung und Weiterentwicklung von Unterrichtsmaterialien in hessischen Schulen. In diesem Rahmen wurde es tätig beim Projekt SINUS, in dem es um die Weiterentwicklung der Unterrichtsmaterialien im Fach Mathematik und in naturwissenschaftlichen Fächern ging. Dazu übersandte es verschiedenen Wiesbadener Schulen einen mehrseitigen Fragebogen für die betroffenen Fach-Lehrkräfte. Die Schulen wurden gebeten, die Fragebögen an die betroffenen Fachlehrer auszuteilen mit der Aufforderung, die Fragebögen ausgefüllt über die Schulleitung wieder an das Institut für Qualitätsentwicklung zurückzuschicken. Im Lehrerfragebogen war auf die Freiwilligkeit der Angaben nicht hingewiesen. Auf der ersten Seite enthielt er unter anderem den Hinweis, die Angaben würden anonym behandelt, d.h. Rückschlüsse auf die Person würden nicht gezogen. Zur Person wurde allerdings auf der zweiten Seite des Fragebogens u.a. erfragt: Geschlecht, Alter und Jahre im Schuldienst. Die weiteren zahlreichen Fragen zu Einzelheiten der Gestaltung des Unterrichts der Lehrkraft sahen eine Bewertungsskala von 1 - 6 vor, die bei 1 eine deutlich negative eigene Bewertung bedeutete. So lautete eine Frage: "Im Unterricht erläutere ich die zu vermittelnden Themen und beantworte die Fragen der Schüler." Die sich beschwerende Lehrkraft teilte weiter mit, der Fragebogen sei ihr von der Schulleitung ohne weitere Informationen ausgehändigt worden mit dem Hinweis, ihn binnen drei Tagen ausgefüllt wieder abzugeben.

Meine anschließende Nachfrage beim Institut für Qualitätsentwicklung über die Organisation der Befragung ergab dann, dass in der Tat ein Informationsschreiben für die Schulleitungen und Lehrkräfte mit dem Hinweis auf die Freiwilligkeit und den Ablauf der Befragung nicht verteilt worden war und auch keine diesbezüglichen mündlichen Hinweise vorgesehen waren.

Meine datenschutzrechtliche Bewertung des Sachverhalts ergab zunächst die Feststellung, dass die Angaben zur Person der Lehrkraft auf der erwähnten ersten Seite des Fragebogens personenbezogene Daten enthalten i. S. v. § 2 Abs. 1 HDSG.

§ 2 Abs. 1 HDSG

Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Zwar sahen die Fragen keine Namen vor. Die Angaben zu Geschlecht, Alter und Jahre im Schuldienst der Lehrkraft ließen jedoch unschwer die Möglichkeit zu, die Identität der betroffenen Lehrkraft festzustellen, wenn ein Abgleich mit dem Datenbestand in den Personalakten in der Schule erfolgte. Eine Personenzuordnung wurde weiterhin erleichtert durch die Eingrenzung der Betroffenen auf die Funktion als Fachlehrer. Damit waren die Daten in den Fragebögen zumindest im Bereich der Schule personenbestimmbar. Eine Personenbeziehbarkeit beim Institut für Qualitätsentwicklung selbst war im Rahmen der Auswertung allerdings nicht mehr möglich.

Um einen Schutz der Fragebögen gegen die sicher nicht beabsichtigte, aber auch nicht ausschließbare Einsicht durch Dritte in der Schule, insbesondere die Schulleitung, zu gewährleisten und zur deutlichen rechtlichen Aufklärung der Lehrkraft über ihre Rechte beizutragen, teilte das Institut für Qualitätssicherung auf meiner Aufforderung hin den betroffenen Schulen und Lehrkräften unverzüglich mit: Die Teilnahme an der Befragung sei freiwillig, und in dem Ausfüllen des Fragebogens sei die nach § 7 Abs. 2 HDSG notwendige Einwilligungserklärung zur Verarbeitung der personenbezogenen Daten zu sehen. Der Fragebogen solle entweder im verschlossenen Umschlag bei der Schulleitung abgegeben oder direkt an das Institut für Qualitätsentwicklung gesandt werden. Zum Zeitpunkt dieses Rundschreibens war allerdings eine wesentliche Anzahl der Fragebögen eingesammelt.

§ 7 Abs. 2 HDSG

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sie muss sich im Falle einer Datenverarbeitung nach Abs. 4 ausdrücklich auch auf die dort genannten Daten beziehen. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und jederzeit mit Wirkung für die Zukunft widerrufen kann.

In einer anschließenden Besprechung des Falles im Institut für Qualitätsentwicklung wurden Wege besprochen, wie künftig solche Fehler in der Abwicklung von Befragungsaktionen an Schulen vermieden werden könnten. Es wurde mir zugesichert, künftig die Fragebögen um ein Informationsblatt zu ergänzen, indem alle nach § 7 Abs. 2 HDSG notwendigen Hinweise dokumentiert werden, sofern nicht auf anderem Wege der Personenbezug gänzlich ausgeschlossen werden kann.

5.5.3 Aushang von Listen mit Nachhilfeschülern in der Schule

Veröffentlichungen am Schwarzen Brett in der Schule können gravierende Folgen haben, auch wenn sie auf den ersten Blick den schlichten Zweck der schnellen Information verfolgen.

Im Rahmen einer Beschwerde wurde mir folgender Sachverhalt übermittelt: Ein hessisches Gymnasium hatte unterschiedliche schulinternen Nachhilfekurse organisiert, die von Oberstufen-Schülern gegen ein angemessenes Entgelt betreut wurden. Die Zusammensetzung der Kurse wurde den beteiligten Schülern mit Ort und Zeit per Aushang am Schwarzen Brett im Schulgebäude mitgeteilt. Damit konnten auch evtl. Änderungen in den Daten der Kurse unbürokratisch und schnell weitergeleitet werden.
Parallel dazu betreuten Lehrkräfte der Schule weitere Schüler mit der sogenannten LRS-Schwäche (Lese- und Rechtschreibschwäche) in Förderkursen. Auch die diesbezüglichen Kursdaten wurden mit Namen der betroffenen Schüler am Schwarzen Brett in der Schule ausgehängt.

Die datenschutzrechtliche Bewertung dieser beiden Varianten führte zu folgenden Ergebnissen:
Soweit die Schulverwaltung die Kurse organisierte und einteilte, stellte die Bekanntgabe der Kursdaten an die beteiligten Kursleiter und Kursteilnehmer keine Übermittlung dar i.S.v. § 2 Abs. 2 Nr. 3 HDSG dar.

§ 2 Abs. 2 Nr. 3 HDSG
…
Im Sinne der nachfolgenden Vorschriften ist
…
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die Daten verarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abruft,
…
Denn die Adressaten der Aushänge waren zunächst einmal die Betroffenen selber, die begrifflich nach § 2 Abs. 5 HDSG nicht Dritte sein konnten.

§ 2 Abs. 5 HDSG

Dritter ist jede Person oder Stelle außerhalb der Daten verarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie Daten im Auftrag verarbeiten.

Der Begriff Übermittlung setzt aber definitionsgemäß den Dritten als Empfänger voraus.

Die Aushänge konnten jedoch auch von Unbeteiligten gelesen werden, wie etwa anderen Schülern. Diese sind als Dritte i.S.v. § 2 Abs. 5 HDSG anzusehen, da sie nicht der Schulverwaltung angehören. Damit lag eine Übermittlung i.S.v. § 2 Abs. 2 Nr. 3 HDSG vor. Die Datenverarbeitung in Form der Übermittlung ist nach § 7 Abs. 1 HDSG nur zulässig, wenn sie auf einer Einwilligung beruht, oder eine Rechtsvorschrift sie erlaubt. Als Spezialvorschrift könnte dafür Anlage 6, Nr. 4 der "Verordnung zur Verarbeitung personenbezogener Daten in Schulen" in Betracht kommen.

Anlage 6 Nr. 4

Datenübermittlung an Personen und Stellen außerhalb des öffentlichen Bereichs

Eine Weitergabe personenbezogener Daten von Schülern oder Erziehungsberechtigten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist grundsätzlich nur mit dem Einverständnis der Betroffenen zulässig. In diesem Fall ist bei minderjährigen Schülern die Einwilligung der Erziehungsberechtigten erforderlich. Dies gilt auch für eine von ehemaligen Schülern gewünschte Übermittlung der Adressdaten von Mitschülern und ehemaligen Lehrerinnen und Lehrern.
Diese Bestimmung beinhaltet ferner, dass Auskünfte an Erziehungsberechtigte volljähriger Schüler über die Teilnahme am Unterricht oder über schulische Leistungen nur mit Zustimmung des Schülers erteilt werden dürfen.
Eine Ausnahme von dieser Bestimmung bilden die Fälle, in denen die Voraussetzungen des § 16 Abs. 1 HDSG erfüllt sind, d.h. ein berechtigtes Interesse an der Datenübermittlung begründet und belegt wird (z.B. privatrechtlicher Ersatzansprüche) und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der Betroffenen beeinträchtigt werden.
Eine Übermittlung von Daten der Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat (§ 34 Abs. 2 HDSG).

Auch diese Vorschrift verweist auf eine Einwilligung oder die Regelung zur Datenübermittlung außerhalb des öffentlichen Bereichs nach § 16 HDSG.

§ 16 HDSG

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist über §§ 11 und 13 hinaus zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(2) Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

Schüler, die von den Kursen nicht betroffen waren, können kein "berechtigtes Interesse" an den Informationen vorbringen. Es war zudem nicht auszuschließen, dass die Aushänge zu den Kursen, die von Oberstufen-Schülern betreut wurden, schutzwürdige Belange der am Kurs teilnehmenden Schüler beeinträchtigen konnten. Denn die Kursteilnahme offenbarte in dem jeweiligen Fach persönlichen Nachholbedarf.

Ein besonders gravierender Datenschutzverstoß war die Nennung der Schülernamen bei den LRS-Kursen. Denn die Lese- und Schreibschwäche kann im Einzelfall Krankheitswert haben und ist dann ein sensitives Datum nach § 7 Abs. 4 HDSG. Aber auch ohne Krankheitswert offenbart es ein besonders gravierendes Defizit, und die Übermittlung beeinträchtigt damit schutzwürdige Belange in besonderem Maße. Ich habe daher die Schulverwaltung aufgefordert, auf diese Aushänge künftig zu verzichten und andere Wege der Information zu wählen.

5.6 Forschung

5.6.1 Aufbau des Deutschen Hämophilieregisters

Beim Paul-Ehrlich-Institut wird das Deutsche Hämophilieregister aufgebaut. Das Datenschutzkonzept für das neue bundesweite Patientenregister ist mit den Datenschutzbeauftragten des Bundes und der Länder intensiv diskutiert und abgestimmt worden.

5.6.1.1 Hintergrund

Nach § 21 des Transfusionsgesetzes (TFG) haben die Träger von Spendeeinrichtungen, pharmazeutische Unternehmen und Einrichtungen der Krankenversorgung jährlich die Zahlen zu dem Umfang der Gewinnung von Blut und Blutbestandteilen, der Herstellung, des Imports und Exports und des Verbrauchs von Blutprodukten und Plasmaproteinen i.S.v. § 14 TFG sowie die Anzahl der behandlungsbedürftigen Personen mit angeborenen Hämostasestörungen der zuständigen Bundesoberbehörde zu melden. Zweck des § 21 TFG ist die Ermittlung der Versorgung mit Blutprodukten. Empfänger der Meldungen ist das Paul-Ehrlich-Institut (PEI) als zuständige selbstständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Gesundheit. Das PEI hat seit 1998 aufgrund der Meldungen der Ärzte einen anonymisierten Bericht zu erstellen, insbesondere über den Verbrauch von Gerinnungsfaktoren und die Zahl der damit behandelten Patienten. Die Datenbank wird jedoch als nicht geeignet angesehen als Basis einer fundierten wissenschaftlichen Auswertung, da die Daten nicht vollständig sind und Doppelmeldungen auch nicht ausgeschlossen werden können.

Seit mehreren Jahren wird der Aufbau eines Deutschen Hämophilieregisters (DHR) angestrebt (www.pei.de). Erfasst werden sollen Daten von Patienten mit Hämophilie A und B (ca. 6.000 bis 8.000 männliche Patienten in Deutschland), und von Patienten mit dem Willebrand-Syndrom, das zwar häufiger vorkommt, jedoch selten dauerhaft. Folgende Ziele werden mit dem Aufbau des Registers verfolgt:

- Wissenschaftliche Auswertung der Behandlungsdaten, insbesondere Verfolgung der Krankheitsverläufe über Jahre,
- Optimierung von Qualität und Wirtschaftlichkeit der Therapie,
- Unterstützung bei der Umsetzung des im TFG geforderten Qualitätssicherungssystems durch die die vollständige Erfassung der nach § 21 TFG zu meldenden Daten. Das PEI wird auf der Basis der Daten des DHR seine gesetzliche Aufgabe nach § 21 TFG erfüllen und dazu die hierfür erforderlichen Daten aus dem DHR entnehmen. Das Konzept des DHR soll es dem Arzt erleichtern, seiner Meldepflicht nachzukommen und es dem PEI erleichtern, seiner Berichtspflicht nachzukommen. Die bisherige Meldung an das PEI mit dem Meldebogen "Angaben zu Patienten mit angeborenen Hämostasestörungen" wird dann entfallen.

Unter Leitung des BMGS wurde in Gesprächen mit Hämophiliebehandlern, Patientenorganisationen und dem PEI vereinbart, dass das DHR bei dem PEI als unabhängige neutrale Stelle angesiedelt werden soll. Die Gesellschaft für Thrombose- und Hämostaseforschung e.V. (GTH), die Vertreter der Patientenorganisationen Deutsche Hämophiliegesellschaft zur Bekämpfung von Bluterkrankungen e.V. (DGH) und die Interessengemeinschaft Hämophiler e.V. (IGH) haben sich unter der Federführung des PEI zusammengeschlossen, um auf der Basis eines multilateralen Kooperationsvertrages ein DHR als Online-Datenbank zu erstellen und zu pflegen. Das Bundesministerium für Gesundheit hat das PEI mit Erlass vom 10. Dezember 2004 beauftragt, ein DHR aufzubauen und zu betreiben.

Die Vertragsparteien setzen einen Ausschuss ein, der über alle für das DHR, seinen rechtmäßigen Fortgang, seine Entwicklung und seine Perspektiven maßgeblichen Fragen beratschlagt, Beschlüsse fasst und Wahlen durchführt. Der Ausschuss setzt sich aus je zwei Vertretern jeder Vertragspartei zusammen. Es wird allerdings in dem Vertrag von einer "originären" Verantwortung des PEI für das Register ausgegangen. Aufgrund dieser originären Verantwortung und der dem PEI in § 21 TFG zugewiesenen Aufgaben verfügt das PEI in Belangen, die sich auf Verantwortungsbereiche, Kostentragungsaspekte und die Verpflichtung nach § 21 TFG auswirken können, über eine Letztentscheidungskompetenz im Sinne eines Vetorechts. Nach dem Vertrag hat das PEI auch die Verantwortung für die Installation gemäß dem beschlossenen Konzept, die

Einhaltung der Datensicherheitsanforderungen, Durchführung der erforderlichen Updates und die Wartung und ist verpflichtet, alle datenschutz- und datensicherheitsrelevanten Maßnahmen zu ergreifen und umzusetzen. Das PEI ist daher als verantwortliche Daten verarbeitende Stelle im Sinne der Datenschutzgesetze anzusehen.

Für den Aufbau dieses bundesweiten Registers mit Patientendaten ist ein detailliertes Datenschutzkonzept unerlässlich. Das Datenschutzkonzept des DHR wurde unter dem Vorsitz meiner Dienststelle im Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder intensiv diskutiert und 2006 abschließend mit allen Datenschutzbeauftragten abgestimmt. Eine zentrale Diskussionsgrundlage waren dabei auch die generischen Konzepte für medizinische Forschungsnetze, die die Telematikplattform für medizinische Forschungsnetze (TMF) in Abstimmung mit den Datenschutzbeauftragten des Bundes und der Länder entwickelt hat (Reng, Debold, Specker, Pommerening, Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin, Medizinisch Wissenschaftliche Verlagsgesellschaft, 2006; www.egms.de/pdf/journals/mibe/-2005-1/mibe000017.pdf; 29. Tätigkeitsbericht, Ziff. 9.2; 32. Tätigkeitsbericht, Ziff. 10.2).

5.6.1.2 Datenschutzrechtliche Rahmenbedingungen

In verschiedenen Bundesgesetzen (z.B. § 75 SBG X) und Landesgesetzen (z.B. § 12 Abs. 3 HKG i.V.m. § 33 HDSG) finden sich datenschutzrechtliche Regelungen zur Durchführung von Forschungsvorhaben mit personenbezogenen Daten. Diese Regelungen sind jedoch für den Aufbau auf Dauer angelegter Krankheitsregister bzw. auf Dauer angelegter einrichtungsübergreifender Forschungsnetze nicht anwendbar, sie beziehen sich ausschließlich auf zeitlich und inhaltlich begrenzte konkrete Forschungsvorhaben.

Für das Hämophilieregister gibt es keine datenschutzrechtliche gesetzliche Regelung. Außerhalb des spezialgesetzlich geregelten Bereichs sind grundsätzlich verschiedene Datenschutzkonzepte möglich: Datenverarbeitung auf der Grundlage von Einwilligungen der Betroffenen - mit oder ohne Zwischenschaltung eines Datentreuhänders - oder unter Verzicht auf die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen ohne Einwilligung der Betroffenen. Entscheidend für die konkrete Ausgestaltung des Konzepts ist zunächst die Frage, welche konkreten Ziele und Zwecke mit dem Register erreicht werden sollen.

5.6.1.3 Einzelheiten der Ausgestaltung des Deutschen Hämophilieregisters

5.6.1.3.1 Fachliche Vorgaben für die Ausgestaltung des Registers

Die Ausgestaltung eines Datenschutzkonzepts für ein Patientenregister hängt zunächst von medizinischen Fachfragen und Zielen und der Ausgangssituation in dem in Frage stehenden Bereich ab.

Bei der konkreten Ausgestaltung des Datenschutzkonzepts des DHR waren zusätzlich zu den unter 5.6.1 aufgeführten grundsätzlichen Zielen des DHR spezielle Vorgaben der Projektbeteiligten einzubeziehen:

- Erreichung einer möglichst großen Akzeptanz bei Behandlern und Patienten,
- keine zentrale Speicherung von Name, Geburtsdatum und Adresse der Patienten außerhalb der Praxis des behandelnden Arztes,
- Reidentifizierung des Patienten nur über den Behandler,
- Vermeidung von Doppelmeldungen und die korrekte Zuordnung der Meldungen zweier Behandler zu den Meldungen,
- Möglichkeit statistischer Auswertungen für Behandler,
- mit Zustimmung des behandelnden Arztes ein Offline-Zugriff der Krankenkassen auf Qualitätssicherungsdaten (Behandler, Anzahl Patienten der Krankenkasse),
- für alle Patienten, die nicht eine Speicherung ihrer Daten im DHR einwilligen, eine anonyme Sammelmeldung an das DHR.

Die Vorgaben der Projektbeteiligten enthielten damit bereits wesentliche Aspekte eines Datenschutzkonzepts; insbesondere auch für die Patientenorganisationen war die Sicherstellung des Schutzes der Patientendaten ein zentraler Punkt.

5.6.1.3.2 Umfang der Speicherung von personenbezogenen Patientendaten im Register

Von zentraler Bedeutung ist die Frage, ob und ggf. in welchem Umfang personenbezogene oder personenbeziehbare Daten in einem bundesweiten Patientenregister gespeichert werden sollen. Ein Register mit ausschließlich anonymisierten Patientendaten wurde in diesem Fall nicht als hinreichend angesehen für die Erreichung der o.a. Ziele und Vorgaben. Es wurde aber auch nicht als erforderlich bzw. auch nicht als erstrebenswert angesehen, in dem DHR Name, Geburtsdatum und Adresse der Patienten zu speichern. Für die kontinuierliche Erfassung und korrekte zeitliche und örtliche (um z.B. regionale Häufung von Erkrankungen feststellen zu können) Zuordnung der Behandlungsdaten und Krankheitsverläufe zu einem Patienten über Jahre hinweg wurde es als ausreichend und auch als erforderlich angesehen, dass im Register die von den Ärzten gemeldeten Daten dem Pseudonym des Patienten eindeutig zugeordnet werden können. Über ein für jeden Patienten gebildetes Pseudonym soll es möglich sein, die Daten innerhalb des DHR zusammenzufassen und damit eine zuverlässige Abbildung des Behandlungsverlaufs der Patienten als Voraussetzung der wissenschaftlichen Evaluation von Fragen wie der optimalen Behandlungsform und -dosierung oder den Risiken und der Behandlungsstrategie beim Auftreten von Inhibitoren zu ermöglichen.

Im Gegensatz zu vielen anderen Forschungsnetzen (s. z.B. das Kompetenznetz Parkinson, s. 32. Tätigkeitsbericht, Ziff. 10.2.1) soll es beim DHR in keinem Fall erforderlich sein, den Patienten anhand des Pseudonyms unter bestimmten Voraussetzungen außerhalb der Behandlungsinstitution wieder zu reidentifizieren.

Gespeichert werden im DHR sog. Profildaten und Behandlungsdaten. Profildaten (für die wissenschaftliche Auswertung und die Bildung von Patientengruppen) enthalten Angaben über das Geschlecht, Geburtsmonat, Geburtsjahr sowie die ersten beiden Ziffern der Postleitzahl der Adresse des Patienten. Behandlungsdaten enthalten diagnostische Daten (insbesondere Art der Erkrankung, Überträgereigenschaft etc.) und therapeutische Daten (Verbrauch von Gerinnungsfaktoren, Krankenhausaufenthalte - ohne konkrete Daten, angegeben die Dauer in Tagen pro Jahr - etc.).

Im DHR werden zu keinem Zeitpunkt Name, Geburtsdatum oder Adresse der Patienten verarbeitet. Der behandelnde Arzt übermittelt die aus der Versicherungsnummer und dem Institutionenkennzeichen der Krankenkasse gebildete so genannte Patientennummer an das DHR (im Rechtssinne an das PEI als verantwortliche Daten verarbeitende Stelle). Diese Patientennummer (p') ist - da die Möglichkeit einer Reidentifizierung des Patienten über diese Patientennummer nicht völlig ausgeschlossen ist - als personenbeziehbares Datum zu qualifizieren, das unter den Anwendungsbereich der Datenschutzgesetze fällt. Die Patientenummer wird allerdings nicht dauerhaft im DHR gespeichert. Nach der Übermittlung an das DHR wird die Patientennummer sofort in ein vom so genannten Intermediär (einer speziellen Software auf einem physisch getrennten Rechner innerhalb des DHR-Programmes) gebildetes Pseudonym (p'') umgewandelt, d.h. die Patientenummer wird nur während der Berechnung des Pseudonyms (temporär) im DHR gespeichert. Im Intermediär liegt die Patientenummer nur für wenige Millisekunden entschlüsselt vor. Das Pseudonym (p'') wird dem Register mitgeteilt. Es wird im DHR gespeichert und diesem werden die Profil- und Behandlungsdaten zugeordnet, die der behandelnde Arzt - wiederum über die Patientenummer und den Intermediär - an das DHR meldet. Die konkrete technische Ausgestaltung ist noch in der Diskussion, u.a. wird der Einsatz eines Rechners geprüft, der das Konzept einer sog. "Black-Box" umsetzt, d.h. der Betreiber kann technisch auf die dort gespeicherten Daten nicht zugreifen und erhält nur die pseudonymisierten Daten an einer definierten Schnittstelle.

Das DHR erhält daher nicht ausschließlich pseudonymisierte Daten, die vom PEI auf keinen Fall depseudonymisiert werden können. Im datenschutzrechtlichen Sinn verarbeitet das PEI - wenn auch strikt begrenzt und technisch abgeschottet und jeweils nur für einen kurzen Zeitraum - personenbeziehbare Daten, da sich die aus Versichertennummer und Krankenkasse gebildete Patientennummer (p') kurzfristig technisch im Zugriffsbereich des PEI befindet. Auf einem Rechner des PEI läuft die Umschlüsselung der Patientennummer, das Ergebnis ist das Pseudonym; d.h. der Intermediär hat vorher personenbeziehbare Daten, hinterher das Pseudonym, das PEI (insbesondere der Administrator) könnte mit einem gewissen Aufwand die Patientennummer dem Pseudonym zuordnen und speichern. An dieser Stelle weicht das Datenschutzkonzept des DHR als zentrale Datenschutzmaßnahme von den generischen Modellen der TMF ab: Bei den generischen Modellen der TMF wird eine Informationsverteilung und Aufgabenteilung empfohlen: Sofern das Pseudonym nicht vom behandelnden Arzt selbst erzeugt wird, ist die Stelle, die das Pseudonym erzeugt (i.d.R. eine rechtlich und personell getrennte sogenannte Vertrauensstelle), strikt getrennt von der Stelle, die die medizinischen Daten unter den Pseudonymen speichert. Datenschutz wird über so genannte informationelle Gewaltenteilung erreicht, die im Einzelfall unterschiedlich ausgestaltet wird. Beim DHR befindet sich alles in einer Stelle - aber einer öffentlichen Stelle, die neutral bezüglich der Behandlungsstrategien ist und weder den Behandlungsinstitutionen noch der Industrie nahesteht und vor diesem Hintergrund als vertrauenswürdig eingestuft wird für die vorgesehene Datenverarbeitung.

Da das PEI personenbeziehbare Patientendaten erhält, bedürfen die Datenübermittlungen der behandelnden Ärzte an das DHR einer Rechtsgrundlage. Als Rechtsgrundlage kommt - da keine gesetzliche Regelung für das DHR vorliegt - nur eine Einwilligung der Patienten in Betracht.

5.6.1.3.3 Einwilligungserklärung der Patienten

Für die Verarbeitung der Patientendaten im DHR wird die Einwilligung der Patienten eingeholt. Vor der Erteilung der Einwilligung werden die Patienten über das gesamte Verfahren mittels einer schriftlichen Patienteninformation konkret informiert.

Für den Umfang der Patienteninformation spielen rechtliche Vorgaben eine Rolle, aber auch Fragen der Akzeptanz. Für die Patienten wurde vom DHR eine ausführliche Patienteninformation erstellt, die insbesondere Informationen über die folgenden Punkte enthält:

- Verantwortliche Daten verarbeitende Stelle,
- Ziele des DHR,
- Zeitlich unbegrenzte Speicherung der Patientendaten,
- Zugriffsrechte auf das DHR,
- Zugangsbedingungen für Forscher,
- Freiwilligkeit der Teilnahme der Patienten am DHR,
- Recht des Patienten auf Widerruf und Verfahrensweise im Fall eines Widerrufs.

In der Einwilligungserklärung wird auf die Patienteninformation Bezug genommen. Mit der Einwilligung wird der behandelnde Arzt auch von seiner ärztlichen Schweigepflicht entbunden, soweit es für die Teilnahme des Patienten am DHR erforderlich ist.

5.6.1.3.4 Meldung und Einsicht durch die behandelnden Ärzte

Ärzte sind weiterhin nach § 21 TFG zur Meldung der Anzahl der von ihnen behandelten Patienten mit angeborenen Hämostasestörungen sowie dem Umfang der Anwendung von Blutprodukten bei diesen Patienten verpflichtet. Diese Meldun-

gen erfolgen kumulativ, sie sind anonymisiert und aggregiert. Die Ärzte sind nicht zur Teilnahme am Meldeverfahren zum DHR verpflichtet. Wenn Ärzte freiwillig am DHR teilnehmen wollen, erhalten sie eine Information über das DHR und unterschreiben eine Einwilligungserklärung in die Verarbeitung ihrer eigenen Daten. Danach erhalten sie vom DHR eine Zugangsberechtigung und eine Arbeitsanweisung zum genauen Umgang mit der Datenbank. Mit der Teilnahme am DHR erfüllen sie gleichzeitig ihre Meldepflicht nach § 21 TFG und eine gesonderte Meldung an das PEI ist nicht mehr erforderlich. Für Patienten, die ihre Einwilligung zur Teilnahme am DHR nicht geben, kann der Arzt die Meldung nach § 21 TFG gesammelt und anonymisiert in einer separaten Eingabemaske des DHR online durchführen.

Der als Teilnehmer registrierte Arzt kann nach Angabe seines Benutzernamens und seines Passwortes die Daten verschlüsselt über das Internet an das beim PEI geführte DHR übermitteln. Auf demselben Weg kann er sich die Daten seiner eigenen teilnehmenden Patienten ansehen, nicht jedoch die Daten eines anderen Arztes (auch nicht desselben Patienten) oder Daten von anderen Patienten. Die Ärzte - wie auch die anderen Benutzergruppen (Forscher, Mitarbeiter des DHR, Krankenkassen etc.) können ihr Passwort selbst ändern.

5.6.1.3.5 Nutzung der Daten

Beim DHR werden verschiedene Benutzergruppen definiert, z.B. Ärzte, Mitarbeiter des DHR und Forscher. Innerhalb der Benutzergruppen werden noch verschiedene Rollen (z.B. innerhalb der Benutzergruppe "Mitarbeiter des DHR" Administration, Forschungsexport und -freigabe) unterschieden und den Benutzergruppen und Rollen jeweils spezifische Zugriffs- und Verarbeitungsrechte zugeordnet.

Auch die Benutzergruppe "Krankenkasse" wird eingerichtet. Im Rahmen der Qualitätssicherungsmaßnahmen erhalten die Krankenkassen Zugriff auf die bei ihnen vorzulegenden Belege zur Meldung nach § 21 TFG der Behandler, soweit der Behandler der Einsichtnahme in diese Daten durch die Krankenkasse zugestimmt hat.

Statt des bisherigen Beleges zur Meldung nach § 21 TFG, den das PEI ausstellte, erhält der Behandler seine Belege zur Meldung nach § 21 TFG durch das DHR. Diese Belege sind im Rahmen der Qualitätssicherung bei der jeweiligen Krankenkasse vorzulegen und weisen nach, wie viele bei der Krankenkasse versicherte Patienten der Arzt im letzten Jahr behandelte. Um sich die Mühe des Ausdrucks und der Übersendung des Belegs an die Krankenkasse zu sparen, kann der Behandler der Krankenkasse Zugriff auf den für sie erstellten Beleg gewähren.

Forscher erhalten nie Zugriff auf den gesamten Datenbestand des DHR, sondern nur auf den jeweils erforderlichen Teildatenbestand. Der von ihnen für ein Forschungsvorhaben benötigte Teildatenbestand muss beantragt werden. Antragsberechtigt sind die Mitglieder des Ausschusses des DHR sowie Wissenschaftler, die sich mit Fragen im Zusammenhang mit Blutgerinnungsstörungen beschäftigen. Im Antrag muss das Studienvorhaben detailliert beschrieben, die benötigten Datenbestände dargestellt und der Datenschutz zugesichert werden. Der Ausschuss entscheidet darüber, ob dem Antrag auf Nutzung des pseudonymisierten Datenbestandes stattgegeben wird. Ein Direktzugriff auf das DHR ist in keinem Fall möglich. Der bewilligte Forschungsexport wird vom DHR erstellt, vor der Freigabe auf ein evtl. Reidentifizierungsrisiko überprüft und anschließend ggf. freigegeben. Nach Authentifizierung gegenüber dem Register können die Antragsteller sich ihre Forschungsdaten herunterladen. Die beantragten Daten werden stets ohne die Pseudonyme herausgegeben. Alle Anträge und alle Zugriffe auf die bereitgestellten Exportdateien werden protokolliert und dokumentiert.

5.6.2 Generisches Datenschutzkonzept für Biomaterialbanken

Die Telematikplattform für medizinische Forschungsnetze hat ein generisches Datenschutzkonzept für Biomaterialbanken entwickelt, in dem die rechtlichen Rahmenbedingungen für den Aufbau und Betrieb von Biomaterialbanken dargelegt werden. Das Konzept wurde mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmt und ist eine zentrale Diskussionsgrundlage für den künftigen Aufbau von Biomaterialbanken in Deutschland.

5.6.2.1 Begriff, Zwecke und Brisanz von Biomaterialbanken

Biomaterialbanken (BMB, auch "Biobanken" genannt) enthalten in der Regel sowohl Biomaterialien (wie z.B. Zellen, Gewebe, Blut, Organe oder Anteile solcher Substanzen wie etwa Serum oder DNA) wie auch - in unterschiedlichem Umfang - Daten der Personen, die solche Materialien spenden. Sie sind ein zentraler Bestandteil der modernen medizinischen Forschung, insbesondere der molekular orientierten medizinischen Forschung. Der Wert einer BMB für die Forschung hängt maßgeblich ab von der Anzahl und Qualität der Proben und dem Umfang der damit verknüpften Daten der Spendenden (z.B. Angaben über Krankheiten und Behandlungsverläufe der Spendenden und ihrer Angehörigen, genetische Daten, Daten über die familiäre und soziale Situation, den Arbeitsplatz, den Lebensstil, Umweltdaten wie etwa die Nähe des Wohnortes zu einem Kernkraftwerk etc.). Die besondere datenschutzrechtliche Brisanz des Themas ergibt sich insbesondere aus der Möglichkeit der Verwendung der Proben für vielfältige, nahezu unbegrenzte medizinische Fragestellungen und aus den z.T. umfangreichen gespeicherten Datensätzen über die spendenden Personen, aus denen detaillierte Persönlichkeitsprofile erkennbar werden können. Vor dem Hintergrund einer Veränderung der medizinischen Forschungsstrukturen hin zu einer Vernetzung werden auch zunehmend zentrale, d.h. institutionenübergreifende Biomaterialbanken geplant bzw. realisiert. Großprojekte wie z.B. die Gendatenbanken in Island, Estland und Großbritannien haben in der Öffentlichkeit ein Bewusstsein geweckt für die mit Biomaterialbanken verbundenen Chancen und auch für die datenschutzrechtlichen Probleme.

2001 hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder detailliert mit der Verarbeitung genetischer Daten befasst, u.a. auch mit den rechtlichen Voraussetzungen eines Aufbaus von Probensammlungen (30. Tätigkeitsbericht, Ziff. 27.14). In meinem 33. Tätigkeitsbericht (Ziff. 5.8.1) habe ich darauf aufmerksam gemacht, dass die Möglichkeiten, Blut- und Gewebeproben (insbesondere auch genetisch) zu analysieren, ständig zunehmen und vor diesem

Hintergrund die rechtlichen Rahmenbedingungen für die Gewinnung, Aufbewahrung und Verwendung von Blut- und Gewebeproben in Biomaterialbanken der Klärung bedürfen. In meinem 34. Tätigkeitsbericht (Ziff. 5.8.3) hatte ich als Beispiel für eine konkrete Abklärung dargelegt, dass der Vorstand des Universitätsklinikums Frankfurt auf der Grundlage meiner Beratung am 24. August 2005 Rahmenbedingungen für den Aufbau von Biobanken im Universitätsklinikum beschlossen hat. Bundesweit geht der Aufbau von Biobanken weiter. Das derzeit größte Projekt ist die im Rahmen des Nationalen Genomforschungsnetzes aufgebaute Biomaterialbank popgen (Populationsrepräsentative Bevölkerungsstichprobe und Krankheitskohorte, www.popgen.de; zum Datenschutzkonzept s. www.datenschutzzentrum.de/material/tb/tb28/kap04_6htm; Eller-Eberstein/-Gundermann/Krawczack/Schreiber/Wolf, Datenmanagement bei popgen, in: Informatik 2006, Band 1, S. 729 ff.) im Universitätsklinikum Schleswig-Holstein, für das noch ein förmliches Datenschutz-Audit geplant ist.

5.6.2.2 Ziel des Datenschutzkonzepts

Angesichts der Tatsache, dass

- derzeit nach wie vor erhebliche Rechtsunsicherheit bezüglich der Patienten- bzw. Spenderrechte besteht,
- Umfang und Zentralisierung von Biobanken zunehmen bei gleichzeitiger Aufhebung einer konkreten Zweckbindung i.S. einer inhaltlich begrenzten wissenschaftlichen Fragestellung,
- an dem Aufbau von Biomaterialbanken vielfach zahlreiche Institutionen in verschiedenen Rollen beteiligt sind und
- spezifische Fragen der Reidentifizierungsrisiken bei Proben und Daten in BMB auftreten

ist es von zentraler Bedeutung, dass die Telematikplattform für Medizinische Forschungsnetze (TMF; www.tmf-ev.de), die bereits in Abstimmung mit den Datenschutzbeauftragten Generische Lösungen für die Forschungsnetze in der Medizin entwickelt hat (Reng/Debold/Specker/Pommerening, Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin, MWV 2006), jetzt praxisgerechte Lösungsvorschläge für den datenschutzgerechten Aufbau und Betrieb von BMB entwickelt hat (Biomaterialbanken - Datenschutz und ethische Aspekte - Generische Konzepte und Realisierung, MWV 2007). Die wesentlichen datenschutzrechtlichen Fragen des Konzepts wurden unter dem Vorsitz meiner Dienststelle im Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder intensiv diskutiert und die überarbeitete Fassung mit den Datenschutzbeauftragten in den wesentlichen datenschutzrechtlichen Fragen abgestimmt. Das Konzept enthält darüber hinaus auch zahlreiche Aussagen zu zivilrechtlichen und strafrechtlichen Fragen sowie zu Fragen des Verwertungsrechts und Persönlichkeitsrechts.

Biomaterialbanken können je nach Anzahl der Proben, mit dem Aufbau der BMB verbundenen Forschungsthemen, der Dauer der Nutzung der Proben, dem Kreis der berechtigten Nutzer der Proben und dem Umfang der mit den Proben verbundenen Daten sehr unterschiedlich organisiert und ausgestaltet sein. Das Konzept der TMF gibt einen Überblick über zahlreiche Varianten und unterscheidet drei grundsätzliche Organisationsmodelle:

- Integration der Biomaterialbank in eine Klinik oder medizinische Einrichtung
- eigenständige BMB und
- BMB im Netz.

Damit ist klar, dass die im Konzept dargelegten Überlegungen und Grundmodelle und die Zusammenstellung rechtlicher, technisch-organisatorischer und praktischer Aspekte eine Diskussion über die konkrete Ausgestaltung von Einzelprojekten nicht ersetzen können. Sie sind aber eine äußerst hilfreiche Grundlage für die weitere Diskussion über die konkrete Ausgestaltung von Biomaterialbanken im Einzelfall.

Das Konzept bezieht sich in erster Linie auf künftig neu gewonnene Proben, und zwar sowohl auf Proben, die im alltäglichen Behandlungskontext gewonnen werden, wie auch auf Proben, die für die Aufnahme in eine BMB für die Forschung gewonnen werden.

5.6.2.3 Zentrale datenschutzrechtliche Aspekte des Konzepts

5.6.2.3.1 Grundsätzliche Überlegungen

Grundlegender datenschutzrechtlicher Ausgangspunkt der Datenschutzbeauftragten des Bundes und der Länder, der auch dem Konzept der TMF vorangestellt wird, ist der folgende: Je abstrakter und allgemeiner der Forschungszweck, die Aufbewahrungszeit und die Nutzungsberechtigten benannt sind, umso strengere Anforderungen sind sowohl an die diesbezügliche Information der Betroffenen und die Formulierung der Einwilligungserklärung als auch an die Sicherheit der Verfahren und die erforderlichen Regelungen zur Aufbewahrung und Nutzung der Proben zu stellen.

5.6.2.3.2 Trägerschaft der Biomaterialbanken

Dem Konzept zufolge eignen sich in der Wissenschaft typischerweise die Rechtsform eingetragener Verein, GmbH und privatrechtliche Stiftung besonders gut für eine BMB; dargelegt werden die jeweiligen Möglichkeiten, die Verantwortlichkeiten klar festzulegen. Aus datenschutzrechtlicher Sicht ist es ein zentrales Anliegen, klare Verantwortlichkeiten - insbesondere auch dauerhaft - für die Proben und Daten verbindlich festzulegen. So ist es zu begrüßen, dass das Konzept auch auf Probleme im Zusammenhang mit Insolvenz des Trägers einer BMB eingeht, wie sie in der Praxis auch schon aufgetreten sind. Wenn auch die Ausführungen zeigen, dass hier Fragen offenbleiben, wird hierdurch zumindest ein Problembewusstsein geschaffen, und die Lösung der Probleme liegt sowohl im Interesse der Forschung wie auch im Interesse des Datenschutzes der Probanden.

5.6.2.3.3 Anonymisierbarkeit von Proben/Unterschied zwischen Daten und Proben

Biomaterialien unterscheiden sich von medizinischen Daten insbesondere dadurch, dass
- sie umfangreiche, über die aktuellen bei ihrer Gewinnung vorhandenen Fragestellungen hinausgehende, insbesondere auch genetische Informationen enthalten und
- sie Informationen enthalten, über die sie den spendenden Personen – bei Vorhandensein geeigneter personenbezogener Vergleichsproben – eindeutig wieder zugeordnet werden können. Im Gegensatz zu medizinischen Daten ist es bei Biomaterialien auch nicht möglich, durch Vergröbern oder Weglassen von Teilinformationen einen solchen Bezug aufzuheben. Eine absolute Anonymisierung von Biomaterialien ist daher prinzipiell nicht möglich.

Vor diesem Hintergrund hat es mit den Datenschutzbeauftragten des Bundes und der Länder intensive Diskussionen über die Frage gegeben, ob Biomaterialien überhaupt anonymisiert werden können. Nach der Legaldefinition in § 3 Abs. 6 BDSG liegt eine (sog. faktische) Anonymisierung vor, wenn ein Personenbezug nur noch mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft hergestellt werden kann. Die Datenschutzbeauftragten des Bundes und der Länder sind übereingekommen, dass eine (faktische) Anonymisierung von Biomaterialien derzeit im Einzelfall grundsätzlich noch als möglich eingestuft werden kann. Entscheidend sind die konkreten Umstände der Gewinnung und Verwendung der Proben und Daten und das Ergebnis einer Risikoanalyse (z.B. die Möglichkeit des Zugangs zu einer personenbezogenen Vergleichsprobe der Spendenden für die Forschenden). Es ist der Verdienst des TMF-Konzepts, dass es auf diese zentrale Frage der Möglichkeit einer faktischen Anonymisierung von Proben detailliert eingeht und auch Problembewusstsein schafft, wenngleich die Ausführungen zur langfristigen Situation notwendigerweise fragmentarisch sein müssen.

Das TMF-Konzept schließt aus der Diskussion um die Unmöglichkeit einer absoluten Anonymisierung, dass
- die Herausgabe von Proben aus der BMB an Dritte nach Möglichkeit zu vermeiden ist,
- eine erforderliche Weitergabe von Proben nur unter striktem Verbot von Reidentifizierungsversuchen - gekoppelt mit hohen Vertragsstrafen - erfolgen darf,
- jede Weitergabe kontrolliert erfolgen muss und
- auch vor einer Veröffentlichung von Analysen und Forschungsergebnissen das Reidentifizierungsrisiko geprüft werden muss.

Offen ist aus der Sicht des Datenschutzes die Frage, wie - u.U. international - die Einhaltung der Vorgaben der Einwilligungserklärung bzw. der vertraglichen Regelungen effektiv überprüft werden können.

5.6.2.3.4 Anforderungen an Einwilligungserklärungen

Aus der Lagerung von Biomaterialien in BMB und der Nutzung der Materialien für die Forschung ergeben sich neue Fragen hinsichtlich der Patienten- bzw. Spenderinformation und der Ausgestaltung der Einwilligungserklärung, die im Konzept aufgegriffen und diskutiert werden, insbesondere Fragen der Reichweite der Einwilligungserklärung, Fragen nach einem evtl. Interesse der betroffenen Patienten oder spendenden Personen an Mitteilungen über erzielte Forschungsergebnisse, ärztlich begründeten Mitteilungspflichten des Forschenden, Fragen nach Eigentums- und Nutzungsübertragung bei Proben, Fragen nach den Folgen eines Widerrufs der Einwilligungserklärung und deren vielschichtige Verschränkung.

Von zentraler datenschutzrechtlicher Bedeutung ist die Frage der Reichweite der Einwilligungserklärung. Nach allgemeinem Datenschutzrecht setzt eine wirksame Einwilligungserklärung voraus, dass die betroffene Person weiß, in welchem Umfang und zu welchem Zweck ihre Daten verarbeitet werden sollen. Die Anforderungen an die Vollständigkeit und Präzision der Information können allerdings je nach Lebensbereich variieren. So ist es z.B. allgemein anerkannt, dass der Eigengesetzlichkeit der Forschung bei der Formulierung von Einwilligungserklärungen im Rahmen von epidemiologischen Studien Rechnung getragen werden muss. Bei BMB gestaltet sich die Frage der Information der betroffenen Personen und damit der Zweckbindung der Proben und Daten jedoch erheblich schwieriger. BMB sind vielfach angelegt als Pool zur Durchführung verschiedener Forschungsvorhaben, die zwar oft ein bestimmtes Indikationsgebiet zum Forschungsschwerpunkt haben, aber auch für Forschungsvorhaben genutzt werden sollen, die zum Zeitpunkt der Probengewinnung bzw. -einlagerung noch nicht absehbar sind. Die TMF legt - unter Berufung auf den Nationalen Ethikrat, der sich 2004 in seiner Stellungnahme zu "Biobanken für die Forschung" ebenfalls eingehend mit dieser Frage befasst hat (www.ethikrat.org) - dar, dass es für die Forschung möglich sein sollte, dass die spendenden Personen ganz allgemein in die Nutzung ihrer Proben und Daten für die medizinische Forschung einschließlich genetischer Forschung einwilligen, sofern ihnen hinreichend klargemacht wird, dass der Zweck der Verwendung der Probe offen ist, und zwar insbesondere hinsichtlich der inhaltlichen wissenschaftlichen Fragestellungen, der involvierten Forscher und des Zeitpunktes der Löschung bzw. Vernichtung der personenbezogenen Daten und Proben.

Dabei wird - wiederum entsprechend der Stellungnahme des Nationalen Ethikrates – hervorgehoben, dass das Recht der Biomaterial spendenden Person auf Widerruf ihrer Einwilligung unverzichtbar ist, auch bei jeder Weitergabe der Probe realisiert werden muss und der Offenheit der Verwendungszwecke der Proben Grenzen setzt. Darüber hinaus wird - ebenfalls in Anlehnung an den Nationalen Ethikrat - eine pauschale Einwilligung in die Weitergabe von personenbezogenen Proben und Daten an unbestimmte weitere Empfänger ausgeschlossen. Die Proben und Daten können anonymisiert oder pseudonymisiert weitergegeben werden; soweit erforderlich kann eine Verknüpfung mit personenbezogenen Daten über die BMB vorgenommen werden. Damit ist sichergestellt, dass die spendende Person ihre Entscheidungsrechte nicht vollständig aus der Hand gibt, sondern ihr bestimmte Handlungs- und Steuerungsmöglichkeiten bleiben.

In jedem Fall sollte sie über die Verfahrensweise nach einem evtl. Widerruf der Einwilligung informiert werden:

Was geschieht mit den Proben und Daten? Werden sie vernichtet bzw. gelöscht oder anonymisiert?
Es liegt auf der Hand, dass diese Frage sowohl für die Forschenden wie auch für die Betroffenen von erheblicher Bedeutung sein kann und daher - da rechtlich nicht zwingend vorgegeben -konkret vereinbart werden muss.

Angesprochen wird in dem Konzept auch die Frage, inwieweit Forschende im Einzelfall eine rechtliche und/oder ethische Pflicht haben, von sich aus die Biomaterial spendende Person zu informieren, wenn bestimmte Forschungsergebnisse für sie relevant sind, z.B. den Ausbruch einer Krankheit verhindern können. Die TMF geht davon aus, dass sowohl eine Mitteilungspflicht als auch ein Ausschluss von Mitteilungen vereinbart werden kann. Ergebnismitteilungen können aus datenschutzrechtlicher Sicht aber auch Risiken mit sich bringen: Wenn eine Ergebnismitteilung vereinbart wird, darf die Verfahrensweise bei der Ergebnismitteilung selbstverständlich nicht dazu führen, dass das bestehende Datenschutzkonzept (z.B. Trennung von Identitätsdaten und medizinischen Daten, Pseudonymisierung) nicht mehr eingehalten wird. Zu bedenken ist auch, dass Ergebnismitteilungen an die spendenden Personen für sie mit Nachteilen verbunden sein können, z.B. bei einem Abschluss von Versicherungsverträgen, bei dem die Betroffenen ihnen bekannte Gesundheitsrisiken offenbaren müssen. Unabhängig davon ist in jedem Fall der datenschutzrechtliche Auskunftsanspruch der Proben spendenden Person über die zu ihrer Person gespeicherten personenbezogenen Daten zu gewährleisten.

5.6.2.3.5 Technisch-organisatorische Datensicherheitsmaßnahmen

Als abzuwehrende Risiken werden im Konzept genannt

- der unbefugte Zugriff auf Informationen, die in der BMB gespeichert sind; ihm soll durch Zugangs- und Zugriffskontrolle begegnet werden, die im Detail nicht Gegenstand des Konzepts ist,
- der unbefugte Zugriff auf die Proben; ihm soll durch physischen Schutz der Proben begegnet werden, der ebenfalls im Detail nicht Gegenstand des Konzepts ist und der auch als weniger problematisch eingestuft wird, weil die Beschaffung einer Probe mit voller (genetischer) Information auf anderem Wege leicht ist (z.B. ein Haar),
- die unbefugte Reidentifikation eines Probanden unter Verwendung von berechtigt oder unberechtigt erlangten Informationen. Das Risiko einer unbefugten Reidentifikation eines Probanden steht im Zentrum der Darstellung. Ihm soll vor allem begegnet werden durch eine Trennung der Datenbestände und eine Trennung der Aufgaben der Datenverarbeitung (sog. "informationelle Gewaltenteilung"):

Im Grundmodell wird davon ausgegangen, dass die Proben und zumindest vier Datenarten zu unterscheiden und unter getrennter Verantwortung zu speichern sind (auf der Ebene der BMB, nicht der konkreten Projektebene):

- identifizierende Daten (IDAT),
- medizinische Daten (MDAT),
- Proben mit organisatorischen Angaben wie z.B. Herkunft, Datum (OrgDAT) und
- aus der Probe gewonnene Analysedaten (ProbDAT).

Für die Zuordnung dieser getrennten Teildatenbestände werden die Kennungen

- PID (eindeutiger Patientenidentifikator),
- PSB (Pseudonym, unter dem die MDAT gespeichert werden),
- LABID (Kennzeichnung einer Probe) und
- LABIDtrans

als Pseudonyme verwendet, die jeweils nur unter genau definierten Bedingungen miteinander verknüpfbar sind.

Eine verteilte Speicherung von Informationen und Aufgabenwahrnehmung ist allerdings nur dann zielführend, wenn mit dieser Verteilung auch eine entsprechende rechtlich differenzierte Verantwortlichkeit einhergeht. Diese Frage wird im Konzept eingehend diskutiert. Bei der Konstruktion der Verteilung der Datenbestände und Aufgaben und der zu unterscheidenden Verantwortlichkeiten und Zugriffmöglichkeiten wird eine Prüfung von Aufwand und Verhältnismäßigkeit empfohlen. Je leichter aus den Daten ein Rückschluss auf die Person gezogen werden kann, desto eher wird eine getrennte Datenhaltung als notwendig angesehen. Im Einzelfall soll daher auch z.B. von der Forderung nach getrennter Speicherung des Teildatenbestandes abgewichen werden können. Für alle BMB wird es aber als zwingend angesehen, dass die personenbezogene Patientenliste räumlich und technisch getrennt von den Forschungsdaten gespeichert ist und die Verantwortlichen auch einer getrennten disziplinarischen Verantwortung unterworfen sind. Es wird davon ausgegangen, dass die Führung der Patientenliste zumindest einer von der restlichen Datenbank getrennten disziplinarischen Verantwortung unterliegen muss, da sie als Ort des Identitätsmanagements besonders schutzbedürftig ist. Wann die Aufgabe der Führung der Patientenliste durch einen externen Datentreuhänder, d.h. einen besonders vertrauenswürdigen Dritten (z.B. Notar), wahrgenommen werden muss, wird offengelassen. Diese Notwendigkeit ist lt. Konzept in jedem Einzelfall zu prüfen. Es wird empfohlen, dass zumindest eine separate Einrichtung die Patientenliste führt. Diese Fragen der Separierung von Datenbeständen und Aufgaben und die entsprechend differenzierte Zuordnung von Verantwortlichkeiten werden künftig bei der datenschutzrechtlichen Bewertung von Konzepten für den Aufbau und Betrieb von Biomaterialbanken eine zentrale Rolle spielen.

Diskutiert werden im Konzept zahlreiche Optionen der Ausgestaltung und Realisierung von getrennter Speicherung und Verantwortlichkeit jeweils für die unterschiedlichen Modellvarianten:

- BMB in einer Klinik oder medizinischen Einrichtung,
- eigenständige BMB und
- BMB in einem Forschungsnetz.

Ein Direktzugriff von Forschern auf die zentrale Datenbank wird nur dann als vertretbar angesehen, wenn das Risiko einer Reidentifizierung der spendenden Person durch die gespeicherten Daten als sehr gering eingeschätzt wird. Als Regelfall wird der Export von Daten genannt, und zwar lediglich der Export der im Einzelfall erforderlichen Daten. Ist ein hohes Reidentifizierungspotenzial aus dem Gesamtbestand nicht auszuschließen, so muss für die Herausgabe von Daten außerdem ein zweites Pseudonym PSN erzeugt werden. Bei jedem Export muss dieses unterschiedlich sein, damit keine externen Datenbestände aufgebaut werden können, die über einen kritischen Informationsbestand verfügen.

5.6.2.3.6 Eigentumsverhältnisse und Nutzungsrecht

Das Konzept legt bei Behandlungs- und Forschungsproben jeweils in unterschiedlicher Weise zu berücksichtigende eigentumsrechtliche, sachenrechtliche und persönlichkeitsrechtliche Aspekte dar und kommt zu der Empfehlung, dass für künftig aufzubauende BMB "für alle Proben die Bedingungen der Nutzung und Weitergabe genau festzulegen" sind. Auch hier treffen sich Interessen der Forschung und des Datenschutzes. Alle rechtlichen Aspekte müssen zu einem Gesamtkonzept zusammengefügt werden.

5.6.3 Datenschutz bei der Arzneimittelprüfung

Bei der Arzneimittelprüfung verbleiben die personenbezogenen medizinischen Daten der an der Studie teilnehmenden Personen beim Prüfarzt. Andere an der Arzneimittelprüfung beteiligte Stellen dürfen grundsätzlich nur pseudonymisierte Daten erhalten. Kontrovers diskutiert wird gegenwärtig, wie die Pseudonymisierung auszugestalten ist.

Die Wirksamkeits- und Verträglichkeitsprüfung neuer Arzneimittel erfolgt in kontrollierten klinischen Studien. Die Verfahrensweise ist insbesondere im Arzneimittelgesetz (AMG) detailliert geregelt. In den letzten Jahren wurde das Arzneimittelgesetz infolge neuer EU-Regelungen mehrfach geändert, u.a. auch in Punkten, die datenschutzrechtliche Fragen betrafen. Die neuen EU-Regelungen betrafen insbesondere den Schutz der an der Studie teilnehmenden Personen sowie das Verfahren zur Bewertung der klinischen Prüfung durch die Ethikkommission und zur Genehmigung durch die zuständige Bundesoberbehörde. Wesentliche Änderungen der §§ 40 bis 42 AMG, die den Schutz des Menschen bei klinischen Prüfungen beinhalten, wurden erforderlich.

Klinische Studien werden stets auf der Grundlage einer schriftlichen Einwilligung der an der Studie teilnehmenden Personen durchgeführt. Im Rahmen einer Studie werden umfangreiche sensitive medizinische Daten über die an der Studie teilnehmenden Personen erhoben. An dem Verfahren der Arzneimittelprüfung sind eine Reihe von Personen bzw. Stellen in unterschiedlichen Funktionen beteiligt, insbesondere

- der Prüfarzt, der für die Durchführung der klinischen Prüfung verantwortlich ist,
- der Sponsor, d.h. eine Person, eine Firma, eine Institution oder eine Organisation, die die Verantwortung für die Initiierung, das Management und/oder die Finanzierung einer klinischen Prüfung übernimmt (zumeist forschende Pharmafirmen), der die Prüfberichte des Prüfarztes und die Meldungen über unerwünschte Ereignisse erhält,
- das Bundesinstitut für Arzneimittel und Medizinprodukte, das Mitteilungen über unerwünschte Arzneimittelwirkungen erhält und an die europäische Datenbank weitergibt.

Es benötigen jedoch keinesfalls alle involvierten Stellen die **personenbezogenen** Daten der an der Studie teilnehmenden Personen. Letztere haben vielmehr ein Recht darauf, dass ihre persönlichen medizinischen Daten nicht unnötig über zahlreiche Stellen im In- und Ausland verbreitet werden. Aus datenschutzrechtlicher Sicht sind daher die zentralen Fragen,

- wer außer dem Prüfarzt welche Daten der an der Studie teilnehmenden Personen erhält und
- wie die an der Studie teilnehmenden Personen über die Datenflüsse informiert werden.

Im AMG sind zu diesen Fragen nunmehr detaillierte Regelungen enthalten. In § 40 AMG sind die Voraussetzungen der Durchführung einer klinischen Prüfung detailliert festgelegt. Zu den Voraussetzungen zählt auch, dass die an der Studie teilnehmenden Personen über Zweck und Umfang der Erhebung und Verwendung personenbezogener Daten, insbesondere von Gesundheitsdaten, informiert worden sind und schriftlich eingewilligt haben. Sie sind nach § 40 Abs. 2a Nr. 1 insbesondere darüber zu informieren, dass die erhobenen Daten soweit erforderlich

- zur Einsichtnahme durch die Überwachungsbehörde oder Beauftragte des Sponsors zur Überprüfung der ordnungsgemäßen Durchführung der klinischen Prüfung bereitgehalten werden (Nr. 1a),
- pseudonymisiert an den Sponsor oder eine von ihm beauftragte Stelle zum Zwecke der wissenschaftlichen Auswertung weitergegeben werden (Nr. 1b),
- im Falle eines Antrags auf Zulassung pseudonymisiert an den Antragsteller und die für die Zulassung zuständige Behörde weitergegeben werden (Nr. 1c) und
- im Falle unerwünschter Ereignisse des zu prüfenden Arzneimittels pseudonymisiert an den Sponsor und die zuständige Bundesoberbehörde sowie von dieser an die Europäische Datenbank weitergegeben werden (Nr. 1d).

Damit ist eindeutig geregelt, dass der Sponsor, die Zulassungsbehörde und die zuständige Bundesoberbehörde sowie die Europäische Datenbank keine personenbezogenen Daten der an der Studie teilnehmenden Personen erhalten dürfen. Die konkrete Form der Übermittlung der jeweiligen Daten an die genannten Stellen wird jedoch kontrovers diskutiert. Die Praxis ist offensichtlich derzeit nicht einheitlich. Teilweise werden auch Berichte bzw. Meldungen mit den medizinischen Angaben und den Initialen, dem Geschlecht und dem vollständigen Geburtsdatum der an der Studie teilnehmenden Personen weitergegeben.

Die Art und Weise der Pseudonymisierung ist im AMG nicht konkret vorgeschrieben. Es gelten daher die allgemeinen datenschutzrechtlichen Vorgaben. Pseudonymisierung ist ein Rechtsbegriff. Ebenso wie beim Anonymisieren ist es das Ziel des Pseudonymisierens, den Personenbezug auszuschließen. Beim Pseudonymisieren bleibt jedoch eine Zuordnungsregel, nach der der Kenner dieser Regel den Personenbezug herstellen kann. Im Übrigen ist wie bei der Anonymisierung auch bei der Pseudonymisierung zu prüfen, ob die Informationen (für Dritte ohne Zuordnungsregel) nicht mehr oder mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (vgl. z.B. § 3 Abs. 6 BDSG). Enthalten z.B. Berichte des Prüfarztes an den Sponsor über Verträglichkeit, Wirkung und Nebenwirkungen bei den einzelnen an der Studie teilnehmenden Personen, klinische Prüfberichte oder Meldungen über unerwünschte Ereignisse die Initialen, das Geschlecht und das vollständige Geburtsdatum einer an der Studie teilnehmenden Person, so können deutschlandweit zwar keineswegs alle an der Studie teilnehmenden Personen identifiziert werden, aber es können beispielsweise an der Studie teilnehmende Personen mit ungewöhnlicheren Namen oder auch mit einem ungewöhnlichen Alter mit etwas Aufwand und etwa unter Zuhilfenahme von Telefonbüchern, Meldedaten o. Ä. identifiziert werden. Auch wenn ein regionaler Bezug vorhanden ist, vereinfacht das die Identifizierung. Außerdem können die meisten Dateien in Deutschland über die Initialen erschlossen werden.

Betrachtungen zur Möglichkeit einer Reidentifizierung bei der Nutzung von Initialen und Geburtsdatum als Pseudonym

Die Kenntnis der Initialen und des genauen Geburtsdatums einer Person reicht in vielen Konstellationen nicht aus, eine Person zu identifizieren. Aber die Wahrscheinlichkeit ist doch größer, als sie im ersten Augenblick erscheint.

Das genaue Geburtsdatum ist bereits sehr aussagekräftig. Man stelle sich für jedes Geburtsdatum ein Kästchen vor und für jede Person, deren Zuordnung man wissen will eine Kugel. Wenn man eine Kugel entnimmt, kann man dann auf die Person schließen, die der Kugel zugeordnet ist?
Wenn das komplette Geburtsdatum bekannt ist, stehen für jedes Jahr 365 (bzw. 366) "Kästchen" zur Verfügung. Da der Mensch über 100 Jahre alt werden kann, gibt es auch Kästchen für das Jahr 1900 in denen sich noch eine oder mehrere Kugeln befinden. Die Lebenserwartung beträgt in Deutschland etwa 80 Jahre, was für ca. 30.000 (80 Jahre mal 365 Tage) verschiedene Geburtstage steht. Im Durchschnitt sind daher, wenn man für jeden Bewohner eine Kugel in sein "Geburtstagskästchen" legt, in jedem Kästchen etwa 2.750 Kugeln (80.000.000 Einwohner verteilt auf 30.000 Kästchen). Je länger das Geburtsdatum zurückliegt, also je älter die Personen sind, umso weniger "Kugeln" gibt es im Kästchen und umso einfacher kann ich auf die Person schließen. Zu alten Personen gibt es dann oft nur noch eine Kugel im "Kästchen" und man kann sogar mit dem "Pseudonym" Geburtstag eine Person identifizieren.

Wenn die Initialen bekannt sind, gibt es eine weitere Information. Für jede Person sind dann bildlich gesprochen auf der Kugel die Initialen vermerkt. Für häufige Initialen hilft das nicht weiter. Eine Person zu identifizieren ist immer noch schwierig oder unmöglich. Das Bild ändert sich aber, wenn eine Person einen sehr seltenen Anfangsbuchstaben beim Vor- oder Nachnamen hat. Einen Nachnamen mit Y oder Q haben weniger als eine von 500 Personen. Zusammen mit dem Vornamen sind diese Initialen nur bei etwa einer von 10.000 Personen gegeben: in dem Beispiel hätte nur jede 10.000ste Kugel diese Initialen. Da sogar bei einem bundesweiten Register durchschnittlich nur 2.750 Kugeln in einem "Kästchen" sind, ist bei diesen Nachnamen (bzw. Vornamen) die Wahrscheinlichkeit groß, eine Person identifizieren zu können.
Wenn es noch eine regionale Zuordnung gibt, reduziert sich die Zahl der zu berücksichtigenden Einwohner. Handelt es sich um das Rhein-Main-Gebiet mit 3.000.000 Einwohnern, so sind im Schnitt 100 Kugeln in einem "Kästchen". Eine Identifizierung ist daher mit großer Sicherheit möglich. Dies gilt dann auch für Nachnamen mit seltenen Initialen wie z.B. I, U, V oder Z.

Aus diesem Grund ist es möglich, eine Person in vielen Fällen zu identifizieren, wenn die Initialen und das Geburtsdatum vorliegen.

Die Verwendung von Initialen und Geburtsdatum wird daher von den Datenschutzbeauftragten des Bundes und der Länder nicht als hinreichende Pseudonymisierung angesehen. Im Übrigen ist die Frage, welche Angaben in den Prüfberichten und in den Meldungen über die an der Studie teilnehmenden Personen tatsächlich erforderlich sind, damit sie korrekt zugeordnet werden können und die Arzneimittelsicherheit gewährleistet ist, derzeit noch offen. Von den forschenden Pharmafirmen werden hierzu auch voneinander abweichende Stellungnahmen abgegeben. Die Fragen sind unter dem Vorsitz meiner Dienststelle im Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder intensiv diskutiert worden. Die Diskussion muss 2007 fortgesetzt werden. Geplant ist auch ein Gespräch der Datenschutzbeauftragten mit dem Bundesinstitut für Arzneimittel und Medizinprodukte.

5.7 Gesundheitswesen

5.7.1 Einführung des flächendeckenden Mammographie-Screenings

In diesem Jahr wurde auch in Hessen mit dem Aufbau der Infrastruktur für das flächendeckende qualitätsgesicherte Mammographie-Screening begonnen. Mit meiner Beratung wurde die Rechtsgrundlage für die Übermittlung der Meldedaten an die neue Zentrale Einladungsstelle in der Meldedatenübermittlungsverordnung geschaffen. Eine Prüfung der Zentralen Einladungsstelle ergab, dass die Daten der Frauen, die nicht teilnehmen möchten, korrekt gelöscht werden.

5.7.1.1 Einleitung

Mit dem Ziel der Absenkung der Brustkrebssterblichkeit bei Frauen zwischen 50 und 70 Jahren wurden seit 1998 in Deutschland zunächst Modellprojekte zum qualitätsgesicherten Mammographie-Screening beschlossen und eingeführt. Gegenstand der Modellprojekte war die Erprobung von Strukturen, innerhalb deren künftig qualitätsgesichertes Mammographie-Screening in Deutschland flächendeckend durchgeführt werden kann. Während der Durchführung der Modellprojekte forderten der Bundesrat (BRDrucks. 372/01 und 1031/01), der Bundestag (BTDrucks. 14/6453 und 14/9122, Plenarprotokoll 14/246, TOP 31a, S. 24940) und die Gesundheitsministerkonferenz (75. Sitzung am 20./21. Juni 2002, TOP 8.2) 2002 die Bundesregierung auf, für die baldmögliche Einführung eines flächendeckenden qualitätsgesicherten Brustkrebs-Früherkennungsprogramms in allen Bundesländern auf der Grundlage der europäischen Leitlinien in Deutschland zu sorgen. Das Bundesministerium für Gesundheit und Soziales bat Ende 2002 den Bundesausschuss für Ärzte und Krankenkassen, Richtlinien zur Einführung des Mammographie-Screenings zu entwerfen. Eine entsprechende Änderung der Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Früherkennung von Krebserkrankungen (Krebsfrüherkennungs-Richtlinien) ist 2003 erfolgt. Der Gemeinsame Bundesausschuss der Ärzte und Krankenkassen änderte mit Beschluss vom 23. März 2003 die Brustkrebsfrüherkennungs-Richtlinien dahingehend, dass jede Frau in Deutschland vom 50. bis 69. Lebensjahr an alle zwei Jahre einen Anspruch auf eine Mammographie hat. Alle Frauen dieses Alters sollen routinemäßig über ein Einladungssystem auf der Grundlage amtlicher Meldedaten zum Mammographie-Screening eingeladen werden. In den Richtlinien sind auch wesentliche Details der Organisationsstruktur des flächendeckenden Screenings in den Ländern festgelegt.

Ein zentraler Aspekt des Projekts war von Anfang an das Anliegen, **jeder** Frau in der betroffenen Altersgruppe das Mammographie-Screening anzubieten, unabhängig von der Frage, ob die Frau in der gesetzlichen Krankenversicherung versichert ist. Die Frauen sollen turnusgemäß, persönlich und schriftlich zur Teilnahme eingeladen werden. Um dies zu ermöglichen, sollen die Meldeämter den einladenden Stellen die hierfür erforderlichen Datensätze der Frauen in der betroffenen Altersgruppe übermitteln. Die Teilnahme am Mammographie-Screening ist selbstverständlich freiwillig. Die Richtlinien sehen vor, dass die Daten derjenigen Frauen, die am Mammographie-Screening nicht teilnehmen wollen, in der einladenden Stelle gelöscht werden.

Sowohl bei den Modellprojekten als auch bei der flächendeckenden Einführung waren auch eine Reihe von datenschutzrechtlichen Fragen zur Verarbeitung der Daten der betroffenen Frauen zu klären. Dies erfolgte in enger Abstimmung mit dem Regierungspräsidium Darmstadt, das für die Verarbeitung der Daten in den Screening-Einheiten zuständig ist.

5.7.1.2 Vom Modellprojekt zum flächendeckenden Screening in Hessen

In meinem 30. Tätigkeitsbericht, Ziff. 11.1 hatte ich darüber berichtet, dass in Wiesbaden und im Rheingau-Taunus-Kreis (wie auch in Bremen und in der Region Weser-Ems) Modellprojekte zur Einführung einer qualitätsgesicherten Brustkrebsfrüherkennung mittels Mammographie-Screening durchgeführt werden. Aufgrund meiner Forderung wurde ein überarbeitetes Datenschutzkonzept von den Projektbeteiligten vorgelegt. Abschließend wurde insbesondere geklärt, dass

- die Übermittlung der Meldedaten aller Frauen im Alter von 49 bis 69 Jahren mit Hauptwohnsitz in Wiesbaden oder dem Rheingau-Taunus-Kreis auf der Grundlage des § 34 Abs. 3 und 4 HMG erfolgen kann:
  Eine Gruppenauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner darf nach dieser Vorschrift erteilt werden, wenn sie im öffentlichen Interesse ist.

§ 34 Abs. 3 HMG

Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohnerinnen und Einwohner (Gruppenauskunft) darf nur erteilt werden, soweit sie im öffentlichen Interesse liegt. Für die Zusammensetzung der Personengruppe dürfen die folgenden Daten herangezogen werden:

Tag der Geburt,

1. Geschlecht,
2. Staatsangehörigkeiten,
3. Anschriften,
4. Tag des Ein- und Auszugs,
5. Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht,
6. erwerbstätig/nicht erwerbstätig und
7. Verknüpfungen zu Familienangehörigen (Ehegatten, Kinder, Eltern).

Mitgeteilt werden dürfen außer der Tatsache der Zugehörigkeit zu der Gruppe folgende Daten:

1. Vor- und Familiennamen,
2. Doktorgrad,
3. Alter,
4. Geschlecht,
5. Staatsangehörigkeiten,
6. Anschriften und

7. gesetzliche Vertreterin/gesetzlicher Vertreter oder Betreuerin oder Betreuer.

Für das Projekt zur Verbesserung der Qualität von Mammographie-Untersuchungen wurde ein öffentliches Interesse bejaht. Die Vorschrift bezieht sich allerdings auf Einzelfälle. Mit der Ablösung der zeitlich und örtlich begrenzten Modellprojekte durch eine dauerhafte flächendeckende Durchführung des Screenings ist eine regelmäßige Datenübermittlung von den Meldeämtern an die Zentrale Stelle notwendig. Bereits im Jahr 2004 wurde daher von meiner Dienststelle klargestellt, dass eine regelmäßige Datenübermittlung für das Mammographie-Screening nur mit einer entsprechenden neuen Rechtsgrundlage zulässig ist.

- die Daten derjenigen Frauen, die eine Teilnahme an dem Projekt explizit gegenüber dem Projektträger ablehnen oder zum Einladungstermin nicht erscheinen und auch auf einen weiteren Terminvorschlag nicht reagieren, in der Datenbank des Projektsträgers gelöscht werden.

Seit dem 31. März 2006 ist das Modellprojekt in Hessen beendet, und seit dem 1. April 2006 wurde mit dem flächendeckenden Mammographie-Screening begonnen (detaillierte Informationen zum Sachstand bundesweit, zu den Vorschriften und weiteren Einzelheiten s. unter www.kooperationsgemeinschaft-mammographie.de).

5.7.1.3 Aufbau des flächendeckenden Screenings in Hessen

An der Durchführung des flächendeckenden Screenings in Hessen sind entsprechend den Vorgaben in den Richtlinien verschiedene Institutionen/Personen beteiligt:

- Sechs Screening-Einheiten, in denen das Screening durchgeführt wird. Eine Screening-Einheit besteht aus einer oder mehreren Mammographie-Einheiten zur Erstellung der Mammographie-Aufnahmen sowie einer oder mehrerer Einheiten zur ambulanten Abklärungsdiagnostik. Screening-Einheiten werden von maximal zwei programmverantwortlichen Vertragsärzten geleistet, die für die Organisation der Mammographien sowie der Abklärungsdiagnostik verantwortlich sind.
- Die - bei der KV-Hessen angesiedelte - Zentrale Stelle, die die Daten der in Frage kommenden Frauen von den Meldeämtern erhält und die Frauen zu einem konkreten Termin in die für sie jeweils nächstgelegene Screening-Einheit einlädt.
- Zwei Referenzzentren in Wiesbaden und Marburg, die die Fortbildung und Betreuung der beteiligten Ärzte gewährleisten und medizinische und technische Qualitätssicherung sowie die Auswertung des Programms sicherstellen.

Das Screening wird auf Bundesebene begleitet durch eine Kooperationsgemeinschaft, die durch sog. regionale Referenzzentren vor Ort präsent ist. Träger der Kooperationsgemeinschaft sind die Spitzenverbände der Krankenkassen und die Kassenärztliche Bundesvereinigung.

Eine Rechtsgrundlage für regelmäßige Datenübermittlungen wurde mit § 18 MeldDÜVO vom 6. Juli 2006 geschaffen. Der Inhalt der Neuregelung wurde mit meiner Dienststelle abgestimmt. Der neue § 18 der MeldDÜVO sieht vor, dass die Meldebehörden der Kassenärztlichen Vereinigung Hessen auf deren Antrag zum Zwecke der Früherkennung von Brustkrebs durch Mammographie-Screening den Namen, Doktorgrad, Tag und Ort der Geburt und Anschrift höchstens vierteljährlich übermitteln dürfen.

§ 18 MeldDÜVO

Die Meldebehörde übermittelt der Kassenärztlichen Vereinigung Hessen auf deren Antrag zum Zwecke der Früherkennung von Brustkrebs durch Mammographie-Screening höchstens vierteljährlich soweit erforderlich folgende Daten aller Frauen im Alter zwischen 50 und 69 Jahren, um sie zur vorsorglichen Untersuchung einzuladen:

1. Familienname (jetziger Name mit Namensbestandteilen)	0101 bis 0106,
2. Geburtsname mit Namensbestandteilen	0201 und 0202,
3. Vornamen	0301 und 0302,
4. Doktorgrad	0401
5. Tag und Ort der Geburt	0601 bis 0603,
6. gegenwärtige Anschrift	1201 bis 1211

5.7.1.4 Löschung der Daten der Frauen, die am Screening nicht teilnehmen wollen

Bei meiner Überprüfung des Verfahrens standen 2006 die Rechte der Frauen im Vordergrund, die nicht am Screening teilnehmen wollen.

In den Einladungsschreiben werden die Frauen darüber informiert, dass ihre von den Meldeämtern an die Zentrale Stelle übermittelten Daten - entsprechend den Regelungen in den Krebsfrüherkennungs-Richtlinien - gelöscht werden, wenn sie explizit erklären, dass sie am Screening nicht teilnehmen möchten oder auf die Einladung und ein erneutes Anschreiben nicht reagieren. Die Verfahrensabläufe habe ich in der Zentralen Stelle gemeinsam mit dem Regierungspräsidium Darmstadt überprüft und wie folgt vorgefunden.

5.7.1.4.1 Datenbankstruktur

Die für Einladungen benötigten Daten werden in zwei Datenbanktabellen als Listen gespeichert. Es gibt die Liste der Teilnehmerinnen und die Liste mit den Meldedaten (Meldeliste). Die Einträge dieser beiden Listen sind über die Screening-ID

(SID) miteinander verbunden; die SID wird mittels einer Hashfunktion aus dem Geburtsnamen, Geburtsort und Geburtsdatum gebildet.

In der Teilnehmerinnenliste sind neben der SID vor allem der Status und das Sperre-Datum gespeichert; nicht gespeichert sind der Name und die Adresse. Der Status besagt beispielsweise, ob eine Einladung erfolgt ist oder die Teilnahme verweigert wurde. Das Sperre-Datum legt fest, wann frühestens wieder eine Untersuchung erfolgen darf und daher eine Einladung versandt werden soll.

In der Meldeliste ist wiederum die SID gespeichert. Zusätzlich sind Geburtsname, Geburtsort, Geburtstag sowie Vorname, Nachname und die aktuelle Anschrift gespeichert, die für das Anschreiben benötigt werden.

5.7.1.4.2 Ablauf der Übernahme von Meldedaten und Löschung der Daten

Wenn eine Kommune Meldedaten an die Zentrale Stelle übermittelt, sollen diese in die Meldeliste übernommen werden, soweit sie für anstehende Untersuchungen benötigt werden. Dazu erfolgt für jede gemeldete Frau ein Abgleich mit dem Sperre-Datum aus der Teilnehmerinnenliste. Für den Abgleich wird aus den Meldedaten die SID gebildet und mit diesem Wert in der Teilnehmerinnenliste gesucht.

Wenn es in der Teilnehmerinnenliste keinen Eintrag mit dieser SID gibt, wird er angelegt und in der Meldeliste der Datensatz gespeichert. Das kann der Fall sein, wenn eine Frau 50 Jahre alt geworden ist und daher zum ersten Mal an dem Screening teilnehmen kann. Gibt es einen Eintrag in der Teilnehmerinnenliste, wird das Sperre-Datum mit dem Lieferdatum verglichen. Ist das Sperre-Datum erreicht oder bereits verstrichen, werden die Meldedaten übernommen. Gibt es einen Eintrag und das Sperre-Datum liegt in der Zukunft, werden keine Daten zu der Frau in der Meldeliste gespeichert. Sie wird beim Screening für die gelieferten Meldedaten nicht berücksichtigt.

Nach der Übernahme wird abhängig von den Untersuchungskapazitäten der Screening-Einheiten ein Einladungstermin ermittelt und ein Einladungsschreiben erstellt. Der Status wird in der Teilnehmerinnenliste auf "eingeladen" gesetzt.

Auf die Einladung reagieren die Teilnehmerinnen sehr unterschiedlich.

- Es gibt Frauen, die sich melden und mitteilen, dass sie nicht mehr behelligt werden wollen. In diesem Fall wird das Sperre-Datum im Teilnehmerinnendatensatz auf den 31. Dezember 9999 gesetzt. Der Status wird auf "verweigert" gesetzt. Der Datensatz in der Meldeliste wird gelöscht. Ab diesem Zeitpunkt werden die Meldedaten nicht mehr in die Meldeliste übernommen. Es wird zukünftig keine Einladung mehr verschickt. Zurzeit findet eine politische Diskussion statt, ob dieser Fall nicht ausgeschlossen werden soll. Es soll möglich werden, dass sich die betroffene Frau später wieder anders entscheidet und am Screening teilnimmt. Eine Lösung wäre es, die Sperre zeitlich zu befristen.
- Andere Frauen sagen, dass sie derzeit nicht teilnehmen wollen. Das Sperre-Datum in der Teilnehmerinnenliste wird auf einen Zeitpunkt in zwei Jahren gesetzt und der Status auf "abgesagt" gesetzt. Der Datensatz in der Meldeliste wird gelöscht.
- Es gibt Frauen, die bereits in Behandlung sind. Das Sperre-Datum in der Teilnehmerinnenliste wird auf den 31. Dezember 9999 gesetzt und der Datensatz in der Meldeliste wird gelöscht.
- Die Frau meldet sich, damit der Termin verschoben wird. Es wird nur der Einladungstermin geändert und der Terminplan der Screening-Einheit geändert.
- Die Frau meldet sich nicht. In diesem Fall wird davon ausgegangen, dass die Frau teilnimmt.

Bis 15 Tage nach dem (Erst-)Einladungstermin wird gewartet, ob die Screening-Einheit die Teilnahme meldet. Medizinische Daten erhält die Zentrale Stelle nicht.

- Wenn die Screening-Einheit die Teilnahme meldet, wird das Sperre-Datum auf den Teilnahmemonat plus zwei Jahre gesetzt und der Status auf "teilgenommen" gesetzt. Der Datensatz in der Meldeliste wird gelöscht.
- Meldet die Screening-Einheit keine Teilnahme, wird ein Erinnerungsschreiben mit einem neuen Termin verschickt. Der Status wird auf "erinnert" gesetzt.

  Es können nun die gleichen Möglichkeiten eintreten wie bei der Ersteinladung.

  Wie bei der Ersteinladung wird abgewartet, ob es in den 15 Tagen nach dem Termin eine Teilnahmebestätigung durch die Screening-Einheit gibt.
- Wenn die Screening-Einheit die Teilnahme bestätigt, wird das Sperre-Datum auf den Teilnahmemonat plus zwei Jahre gesetzt und der Status auf "teilgenommen" gesetzt. Der Datensatz in der Meldeliste wird gelöscht.
- Hat die Frau auch auf das zweite Schreiben nicht reagiert und ist nicht zur Untersuchung gekommen, wird das Sperre-Datum um zwei Jahre erhöht. Der Status wird auf "ErinnerungErfolglos" gesetzt und der Datensatz in der Meldeliste wird gelöscht.

Ich habe geprüft, ob entsprechend der Beschreibung die Datensätze mit den Meldedaten nicht vorhanden bzw. gelöscht waren. Bei der Prüfung konnte ich feststellen, dass nur dann Meldedaten gespeichert waren, wenn sie auf Grund der Abläufe für eine Teilnahme benötigt wurden.

2007 werde ich noch weitere Aspekte des Verfahrens überprüfen.

5.7.2 Verwendung von Pflegedokumentationen bei der Durchführung von Qualitätsprüfungen in Pflegeeinrichtungen

Zur Frage der Heranziehung von Pflegedokumentationen für die Aufklärung und Weiterverfolgung von Falschabrechnungen und Abrechnungsbetrug habe ich zahlreiche Anfragen und Beschwerden erhalten. Soweit zwingend erforderlich dürfen Pflegedokumentationen auch für diese Zwecke verwendet werden. Die Verfahrensweise muss klar festgelegt und die Kenntnisnahme der sensitiven Daten strikt begrenzt werden.

Bei der Pflegedokumentation, die in den Pflegeeinrichtungen geführt wird, handelt es sich um eine personenbezogene Unterlage, die regelmäßig sehr detaillierte, sehr persönliche und überwiegend medizinische Informationen über die Betroffenen enthält und daher besonders schutzwürdig ist. Sie darf daher grundsätzlich nur für den Zweck der Pflege verwendet werden.
Die mir zugegangenen Anfragen und Beschwerden betreffen die Durchführung von Qualitätsprüfungen in Pflegeeinrichtungen.

5.7.2.1 Qualitätsprüfung und Abrechnungsprüfung

Die Durchführung von Qualitätsprüfungen ist in den §§ 112 ff. SGB XI geregelt. Nach § 112 Abs. 3 haben die Pflegeeinrichtungen auf Verlangen der Landesverbände dem Medizinischen Dienst der Krankenversicherung (MDK) oder den von den Landesverbänden bestellten Sachverständigen die Prüfung der erbrachten Leistungen und deren Qualität durch Einzelprüfungen, Stichproben und vergleichende Prüfungen zu ermöglichen. **Die Prüfungen sind** auf die Qualität, die Versorgungsabläufe und die Ergebnisse der in § 112 Abs. 2 SGB XI genannten Leistungen sowie **auf deren Abrechnung zu erstrecken**. Soweit ein zugelassener Pflegedienst auch häusliche Krankenpflege nach § 37 SGB V erbringt, gelten diese Regelungen entsprechend.

§ 112 Abs. 3 SBG XI

Die Pflegeeinrichtungen haben auf Verlangen der Landesverbände der Pflegekassen dem Medizinischen Dienst der Krankenversicherung oder den von den Landesverbänden bestellten Sachverständigen die Prüfung der erbrachten Leistungen und deren Qualität durch Einzelprüfungen, Stichproben und vergleichende Prüfungen zu ermöglichen. Die Prüfungen sind auf die Qualität, die Versorgungsabläufe und die Ergebnisse der in Abs. 2 genannten Leistungen sowie auf deren Abrechnung zu erstrecken, soweit ein zugelassener Pflegedienst auch Leistungen nach § 37 des Fünften Buches erbringt, gelten die Sätze 1 und 2 entsprechend.

Nach § 114 Abs. 1 SBG XI sind der MDK oder die von den Landesverbänden der Pflegekassen bestellten Sachverständigen in Wahrnehmung ihres Prüfauftrags nach § 112 Abs. 3 SBG XI berechtigt und verpflichtet, an Ort und Stelle zu überprüfen, ob die ambulanten oder stationären zugelassenen Pflegeeinrichtungen die vorgeschriebenen Leistungs- und Qualitätsanforderungen weiterhin erfüllen. Nach § 114 Abs. 6 SBG XI sind auf Verlangen Vertreter der betroffenen Pflegekassen oder ihrer Verbände an den Prüfungen zu beteiligen.

5.7.2.2 Verwendung der Pflegedokumentation für Abrechnungsprüfungen

Es ist unstreitig, dass die Pflegedokumentation Gegenstand der Qualitätsprüfung ist. Nach meiner Auffassung bestehen auch keine Bedenken gegen eine Einsichtnahme in die Pflegedokumentation durch den Vertreter der betroffenen Pflegekasse oder der Verbände der Pflegekassen, sofern diese an einer Prüfung vor Ort nach § 114 Abs. 1 bis 3 SBG XI beteiligt werden, um die **vom Gesetzgeber vorgeschriebene** Abrechnungsprüfung durchzuführen. Dies entspricht dem Wortlaut des Gesetzes. Die Abrechnungsprüfung ist vom Gesetzgeber gezielt als Bestandteil der Qualitätsprüfung festgelegt worden, damit Falschabrechnung und Abrechnungsbetrug festgestellt und verfolgt werden können.

In Hessen werden seit einiger Zeit regelmäßig Qualitätsprüfungen in Pflegeeinrichtungen durchgeführt, an denen jeweils der MDK, die Heimaufsicht sowie ein Vertreter der betroffenen Pflegekasse oder des Verbandes der Pflegekasse teilnehmen. Es handelt sich nach den mir vorliegenden Informationen ausschließlich um **anlassbezogene** Qualitätsprüfungen, nicht um routinemäßige Qualitätsprüfungen. Entsprechend den o. a. Grundsätzen habe ich keine Bedenken dagegen, dass sich die Qualitätsprüfung wie gesetzlich vorgesehen auch auf die Abrechnungen erstreckt und der Vertreter der betroffenen Pflegekasse oder des Verbandes der Pflegekassen in diesem Zusammenhang in die Pflegedokumentation Einsicht nimmt und evtl. Abrechnungsauffälligkeiten z.B. durch Vergleich der Pflegedokumentation mit den Rechnungen feststellt, also z.B. überprüft, ob eine abgerechnete Leistung tatsächlich erbracht wurde.

Vom Gesetzgeber nicht explizit geregelt ist die weitere Verfahrensweise, wenn im Rahmen einer Qualitätsprüfung Anhaltspunkte für Falschabrechnungen oder Abrechnungsbetrug ersichtlich werden.

Soweit im Rahmen einer solchen anlassbezogenen Qualitätsprüfung nach § 112 SBG XI **konkrete Anhaltspunkte** für einen Abrechnungsbetrug festgestellt werden und **die weitere Aufklärung des Sachverhalts sowie eine Beweissicherung ausschließlich unter Zuhilfenahme der Pflegedokumentation durchgeführt werden kann**, habe ich keine Bedenken dagegen, dass die Pflegedokumentation **im jeweils erforderlichen Umfang** kopiert und von dem Vertreter der betroffenen Pflegekassen für diese Zwecke mitgenommen wird. Die Originaldokumentation ist umgehend zurückzugeben.

Die Pflegedokumentation beinhaltet umfangreiche, sensitive persönliche Daten des Betroffenen. Nach der gesetzlichen Regelung ist die Pflegedokumentation keine Abrechnungsunterlage i. S. d. § 105 SBG XI. Es besteht daher auch keine rechtliche Grundlage, die eine routinemäßige Weitergabe der Pflegedokumentation an die Pflegekasse erlauben würde. Da jedoch im **Einzelfall** eine Einsichtnahme in die Pflegedokumentation durch den Vertreter der betroffenen Pflegekasse oder des Verbandes zur Abrechnungsprüfung zulässig ist und sich im Rahmen der Prüfung vor Ort konkrete Anhaltspunkte für einen Abrechnungsbetrug ergeben können, kann es nicht das Ziel der gesetzlichen Regelung sein, eine weitere Durchführung der

Abrechnungsprüfung **einschließlich** der notwendigen Beweissicherung unmöglich zu machen. Die Durchführung der Abrechnungsprüfung muss abgeschlossen werden können mit der Konsequenz, dass Verfehlungen im Zusammenhang mit der Abrechnung ggf. zivilrechtlich und/oder strafrechtlich verfolgt werden. Wie die AOK Hessen mehrfach mir gegenüber schriftlich und mündlich dargelegt hat, ist eine abschließende Klärung des Sachverhalts und eine Beweissicherung vor Ort nicht immer möglich.

5.7.2.3 Vorgaben für den weiteren Umgang mit den Pflegedokumentationen bei der Pflegekasse

Von dieser Position unberührt bleibt die Feststellung, dass die Pflegedokumentation keine Abrechnungsunterlage i. S. d. § 105 SBG XI darstellt. Dies hat zur Folge, dass die Verwendung der Pflegedokumentation durch den Vertreter der Pflegekasse nur zweckgebunden für die konkrete Überprüfung der Anhaltspunkte für Falschabrechnung und/oder Abrechnungsbetrug zulässig ist und durch geeignete technische und organisatorische Maßnahmen sicherzustellen ist, dass die Unterlage vernichtet wird, soweit bzw. sobald sie für die korrekte Überprüfung nicht mehr benötigt wird.

5.7.2.4 Maßnahmen der AOK Hessen zum datenschutzgerechten Umgang der Pflegedokumentationen

Von den Mitarbeitern meiner Dienststelle wurde zusammen mit der AOK zunächst ein Arbeitsablauf konzipiert, der detailgenau das Verfahren beschreibt, das zur temporären Speicherung der Unterlagen bei der zuständigen Ermittlungsgruppe der AOK führt. Der Arbeitsablauf wird jedem zuständigen Mitarbeiter ausgehändigt und ist bindend. Zusätzlich ist das mehrseitige Papier im hausinternen Intranet der AOK publiziert. Es enthält zunächst einige grundsätzliche rechtliche Anmerkungen, die ich bereits unter der Ziff. 5.7.2.1 dargelegt habe.

5.7.2.4.1 Kopie der Pflegedokumentation – Übergabe- und Rückgabeprotokoll

Ausschließlich dann, wenn im Rahmen einer Qualitätsprüfung bei den stichprobenhaften Abrechnungsprüfungen Auffälligkeiten festgestellt werden, kann das die Kopie der Unterlage rechtfertigen. Die Originalunterlagen werden soweit erforderlich durch den Prüfer mitgenommen. Hierüber wird ein Protokoll gefertigt, in dem wesentliche organisatorische Inhalte wie z.B. Name des Pflegedienstes, Name des Patienten sowie der inhaltliche Umfang der ausgehändigten Unterlagen festgehalten wird. Beide Parteien unterschreiben das Papier. Von der zentralen Ermittlungsgruppe der AOK werden anschließend die Kopien gefertigt.
Ebenfalls protokolliert und quittiert wird die Rückgabe der Unterlagen an den Pflegedienst. Dies erfolgt persönlich durch Mitarbeiter der AOK.

5.7.2.4.2 Eintrag in eine Datentabelle

Um zu jedem Zeitpunkt den Aufbewahrungsort der Dokumentationen nachvollziehen zu können, werden die Inhalte des Übergabeprotokolls in eine Tabelle eingetragen. So kann ad hoc festgestellt werden, ob sich die gesuchte Akte z.B. im Archiv, in der laufenden Bearbeitung oder bei der Staatsanwaltschaft befindet oder ob die Vernichtung erfolgte, weil es eine Einigung mit dem Pflegedienst gegeben hatte bzw. offene Forderungen der Pflegekasse beglichen wurden.
Zusätzlich führt die AOK eine "Gesamttabelle", die über das gesamte Kalenderjahr hinweg einen Überblick über sämtliche überprüfte Unterlagen vermittelt.

5.7.2.4.3 Auswertung

Die Auswertung erfolgt grundsätzlich bei der Ermittlungsgruppe der AOK, die in Rüdesheim angesiedelt ist. Neben den zuständigen Prüfern der AOK haben sonst keine weiteren Personen Zugriff auf die Unterlagen. Die Auswertung erfolgt manuell. Eine elektronische Erfassung der Unterlagen wird nicht vorgenommen.

5.7.2.4.4 Lagerung der Unterlagen

Nach Abschluss ggf. erfolgter Gespräche über finanzielle Rückforderungen mit dem Pflegedienst bzw. bis zum vollständigen Ausgleich zurückgeforderter Beträge werden die Unterlagen nebst Prüf- und Auswertungsberichten im Archiv in Rüdesheim aufbewahrt. Zugang zum Archiv haben ausschließlich befugte Mitarbeiter des zuständigen Fachbereichs der Pflegekasse der AOK.
Um jederzeit die Revisionsfähigkeit der gelagerten Unterlagen sicherstellen zu können, wird eine Archiv-Liste geführt, in der auch längerfristige Einlagerungen (z.B. im Zusammenhang mit Gerichtsverfahren) protokolliert werden.

5.7.2.4.5 Vernichtung der Unterlagen

Grundsätzlich sind die kopierten Unterlagen zum frühestmöglichen Zeitpunkt zu vernichten. Dies kann dann sein, wenn sich

a) der Verdachtsfall nicht erhärtet,

b) versehentliche Abrechnungsfehler geklärt und Rückforderungen akzeptiert sowie tatsächlich ausgeglichen sind oder

c) etwaige gerichtliche Auseinandersetzungen im Zusammenhang mit Betrugsfällen einen Abschluss gefunden haben.

Der Ort und Zeitpunkt der Vernichtung wird protokolliert und dem betroffenen Pflegedienst zur Kenntnis gegeben.

Die ebenso eindeutigen wie detaillierten Regelungen zum Umgang mit kopierten Pflegedokumentationen durch die Pflegekasse sind nicht nur im Interesse des Kostenträgers, sondern berücksichtigen ebenso die berechtigten Interessen sowohl der Pflegebedürftigen selbst als auch der Pflegedienste.

5.7.3 Kopflausbefall von Kindern - ein Fall für das Gesundheitsamt

Bei Kopflausbefall schreibt das Infektionsschutzgesetz eine namentliche Meldung betroffener Kinder an das zuständige Gesundheitsamt vor. Die Behörde kann nach Ansicht des Sozialministeriums aber keine weiteren Maßnahmen treffen, weil es keine Regelungen zur weiteren Verwendung der Personendaten gibt. Damit entsteht ein "Datenfriedhof" in den Ämtern, dessen Sinnhaftigkeit bezweifelt werden muss.

5.7.3.1 Personenbezogene Meldung von Kopflausfällen nach dem Infektionsschutzgesetz

Auch im abgelaufenen Berichtszeitraum habe ich mich aufgrund von Beschwerden mit der Datenübermittlung personenbezogener Daten an das Gesundheitsamt befasst. Im konkreten Fall ging es um die Frage, ob und wenn ja, welche Daten Kindertagesstätten im Zusammenhang mit dem Auftreten von Kopflausbefall zu melden haben. Nach §§ 33, 34 des Gesetzes zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz - IfSG) vom 20. Juli 2000 (BGBl. I S. 1045), zuletzt geändert durch Art. 57 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407) ist die Leitung der Gemeinschaftseinrichtung verpflichtet, das zuständige Gesundheitsamt unverzüglich zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen.

§ 33 IfSG

Gemeinschaftseinrichtungen im Sinne dieses Gesetzes sind Einrichtungen, in denen überwiegend Säuglinge, Kinder oder Jugendliche betreut werden, insbesondere Kinderkrippen, Kindergärten, Kindertagesstätten, Kinderhorte, Schulen oder sonstige Ausbildungseinrichtungen, Heime, Ferienlager und ähnliche Einrichtungen.

§ 34 Abs. 1 IfSG

Personen, die …verlaust sind, dürfen in den in § 33 genannten Gemeinschaftseinrichtungen keine Lehr-, Erziehungs-, Pflege-, Aufsichts- oder sonstige Tätigkeiten ausüben.…Satz 1 gilt entsprechend für die in der Gemeinschaftseinrichtung Betreuten mit der Maßgabe, dass sie die dem Betrieb der Gemeinschaftseinrichtung dienenden Räume nicht betreten, Einrichtungen der Gemeinschaftseinrichtung nicht benutzen und an Veranstaltungen der Gemeinschaftseinrichtung nicht teilnehmen.

§ 34 Abs. 5 IfSG

Wenn einer der in den Absätzen 1, 2 oder 3 genannten Tatbestände bei den in Absatz 1 genannten Personen auftritt, so haben diese Personen oder in den Fällen des Absatzes 4 der Sorgeinhaber der Gemeinschaftseinrichtung hiervon unverzüglich Mitteilung zu machen.

§ 34 Abs. 6 IfSG

Werden Tatsachen bekannt, die das Vorliegen einer der in den Absätzen 1, 2 oder 3 aufgeführten Tatbestände annehmen lassen, so hat die Leitung der Gemeinschaftseinrichtung das zuständige Gesundheitsamt unverzüglich zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen…

5.7.3.2 Befugnisse des Gesundheitsamtes

Nach Rechtsauffassung des Hessischen Sozialministeriums, die in einem "IfSG-Leitfaden" für Kinderbetreuungsstätten und Schulen in Hessen dokumentiert ist, kommt neben einem Besuchsverbot nach § 17 IfSG nur die Anordnung der Entwesung der mit Läusen und Nissen verunreinigten Räume und Gegenstände durch das zuständige Gesundheitsamt in Betracht. Für andere, weiterführende Maßnahmen enthalte das IfSG keine Rechtsgrundlage.

5.7.3.3 Was macht das Gesundheitsamt mit den personenbezogenen Daten der Kinder?

Festzustellen bleibt, dass es für die personenbezogene Datenübermittlung an das Gesundheitsamt eine klare gesetzliche Regelung im § 34 Abs. 6 IfSG gibt. Die Konsequenzen aus der Meldung des Kopflausbefalls, die nunmehr - entgegen den alten Regelungen des Bundesseuchengesetzes - mit personenbezogenen Angaben an das Gesundheitsamt zu erfolgen hat, sind jedoch unklar. Folgt man der im "Leitfaden" dargelegten Ansicht des Sozialministeriums, dass die Gesundheitsämter keine weiteren Maßnahmen ergreifen können, also nicht im Wege z.B. einer Beratung oder Kontrolle bei den Betroffenen vorstellig werden dürfen, muss die Sinnhaftigkeit der Datenübermittlung insgesamt hinterfragt werden.

Ebenfalls unklar sind die Speicherfristen für derartige Meldungen. Die zulässige Übermittlung führt zunächst einmal zu einer - ebenfalls zulässigen - Speicherung der Daten. Deren Dauer ist nicht im IfSG geregelt, denn es enthält keine Aufbewahrungs- bzw. Speicherfrist für die personenbezogenen Daten der Kinder und Eltern. Dies kann aber nicht zur Konsequenz haben, dass die Daten über einen unbestimmten Zeitraum hinweg gespeichert bleiben. Einer unbefristeten Speicherung stehen die allgemeinen Regelungen des HDSG entgegen, wonach die Erforderlichkeit der Datenspeicherung den Zeitpunkt der Löschung bestimmt. Sind die Daten also nach der Übermittlung zur rechtmäßigen Aufgabenerfüllung nicht mehr erforderlich, müssen sie gelöscht werden.

§ 19 Abs. 3 HDSG

Personenbezogene Daten sind unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 weiterverarbeitet wer-

den dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer aufgrund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Wenn nach der Übermittlung entsprechend der Aussage des Sozialministeriums keine weiteren Maßnahmen des Gesundheitsamtes erfolgen dürfen, weil es dafür keine Rechtsgrundlage im IfSG gibt, ist eine Aufbewahrung der Daten nicht erforderlich. Die personenbezogenen Daten wären folglich zu löschen. Auch das stellt den Sinn der Datenübermittlung an sich in Frage.

5.7.3.4 Weitere Vorgehensweise

Es erscheint deshalb erforderlich, neben der besonderen Befugnisnorm zur personenbezogenen Übermittlung der Daten betroffener Kinder klare Regelungen zu treffen, in welcher Weise diese Daten durch das Gesundheitsamt verwendet werden sollen. Das bloße Speichern der Informationen lässt Zweifel an der Erforderlichkeit hierfür aufkommen. Eine sinnvolle Regelung setzt voraus, dass die speichernde Stelle, also das Gesundheitsamt, die Daten zur Aufgabenerfüllung tatsächlich benötigt. Deshalb sollten ggf. konkrete Maßnahmen, zu denen das Gesundheitsamt befugt ist, festgelegt werden. In diesem Zusammenhang ist auch die Speicherdauer der Daten zu beurteilen und es sind dazu entsprechende Regelungen zu treffen.

Soll das Gesundheitsamt nicht weiter tätig werden, muss sowohl die Datenübermittlung als auch die Zulässigkeit einer Speicherung grundsätzlich in Frage gestellt werden.

Um möglichen Missverständnissen vorzubeugen: eine effektive Bekämpfung des sich derzeit in der Ausbreitung befindlichen Kopflausbefalls, insbesondere in Kindertagesstätten, soll nicht in Frage gestellt werden. Zur Diskussion steht jedoch eine eindeutige und nachvollziehbare gesetzliche Regelung, welche sowohl den Interessen der Betroffenen als auch der für die Bekämpfung zuständigen Behörde Rechnung trägt. Deshalb habe ich das Sozialministerium eingeschaltet und um eine Stellungnahme zu dieser Problematik gebeten.

5.7.4 Übermittlung von Versichertendaten durch die AOK Hessen an Versand-Apotheken

Die Übermittlung von Versichertendaten der AOK Hessen mit medizinischen Inhalten an Versand-Apotheken war wegen der fehlenden bzw. unvollständigen Einwilligung der Versicherten in die Datenübermittlung unzulässig.

5.7.4.1 Service für die Versicherten

Durch eine Beschwerde des Hessischen Apotheker-Verbandes bin ich auf die Verfahrensweise der AOK aufmerksam geworden. Die AOK Hessen hatte durch die zielgerichtete Auswertung ihres Versicherungsbestandes Versicherte ermittelt, die an Diabetes Mellitus erkrankt sind. Unter Verwendung eines Gesprächsleitfadens informierten zunächst Beschäftigte des eigenen Call-Centers, schließlich eine eigene Mitarbeitergruppe innerhalb der Fachabteilung diese Versicherten über Möglichkeiten einer preiswerten medizinischen Versorgung. Insbesondere wurde auf mögliche finanzielle Vorteile bei der Bestellung von medizinischen Produkten bei Versand-Apotheken hingewiesen. Zum Schluss wurden Versicherte nach ihrem Einverständnis zur Übermittlung der Adresse an die Versand-Apotheken gefragt und ein entsprechender Vermerk in den elektronisch zur Verfügung gestellten Versichertendatensatz eingestellt. Diese Datensätze wurden hernach geprüft und die Daten der Versicherten, die einer Übermittlung ihrer Adresse zugestimmt hatten, in einer gesonderten Tabelle hinterlegt.

5.7.4.2 Nicht nur Adressdaten wurden übermittelt

Die Einholung der mündlichen Einwilligung in eine Datenübermittlung war in diesem Fall zunächst unproblematisch. Durch die zur Verfügung gestellten Informationen, die sich aus einem Gesprächsleitfaden ergaben, den die eingesetzten Mitarbeiter der AOK benutzten, war der Versicherte hinreichend über die Art und den Inhalt der zu seiner Person vorgesehenen Datenübermittlung an die Apotheken aufgeklärt. Allerdings unterlief der AOK dabei ein Fehler: Neben den reinen Adressdaten der damit einverstandenen Versicherten wurde zudem die Diabetiker-Eigenschaft an die Versand-Apotheken übermittelt. Das war in dieser Form mit den Betroffenen nicht abgestimmt. Hinzu kam, dass es sich in diesem Kontext um die Übermittlung medizinischer Daten handelte, mithin um sensitive Daten, für die ein hohes Datenschutzniveau einzuhalten ist.

5.7.4.3 Auch das Verfahren der Datenübermittlung war mangelhaft

Die AOK übermittelte die in einer "Excel-Datei" zusammengespielten Daten der Versicherten (also Name und Anschrift) an Versand-Apotheken, die mit ihr einen Vertrag abgeschlossen hatten. Die Übermittlung der Excel-Datei erfolgte als Anhang zu einer E-Mail. Zusätzlich wurde der Apotheke telefonisch mitgeteilt, dass es sich um Diabetiker handelt, damit den Versicherten spezielle Informationen und Angebote übermittelt werden konnten.

Eine Verschlüsselung der auf elektronischem Weg übermittelten Informationen erfolgte nicht. Da eine E-Mail ohne großen technischen Aufwand von Unbefugten eingesehen werden kann, auf ihrem Weg vom Sender zum Empfänger nicht nachvollziehbare elektronische Strecken bis zum Server des Empfängers zurücklegt und dabei technisch auch eine Zwischenspeicherung auf anderen Servern nicht ausgeschlossen werden kann, muss eine nach dem derzeitigen Stand der Technik verfügbare Verschlüsselungssoftware eingesetzt werden. Eine E-Mail ist klassisch vergleichbar einer Postkarte, deren Inhalte grundsätzlich von jedem, der diese Karte in die Hand bekommt, zur Kenntnis genommen werden kann. Der nicht verschlüsselte Anhang der E-Mail-Sendungen der AOK an die Versand-Apotheken konnte demnach also auch von Unbefugten potenziell geöffnet und gelesen werden.

5.7.4.4 Beschwerde des Apotheker-Verbandes und Maßnahmen des HDSB

Die Beschwerde des Hessischen Apotheker-Verbandes hat mich auf die problematische Verfahrensweise der AOK aufmerksam gemacht. Ein Mitarbeiter meiner Dienststelle hat daraufhin unverzüglich die zuständige Stelle der AOK in Eschborn aufgesucht und den Sachverhalt recherchiert.
Aus datenschutzrechtlicher Sicht bestehen grundsätzlich keine Bedenken dagegen, dass die AOK aufgrund einer Einwilligung ihren Versicherten die Möglichkeit einer preiswerten medizinischen Versorgung eröffnet. Soweit hiermit eine Übermittlung personenbezogener Versichertendaten verbunden ist, sollte jedoch von der AOK eine strikt auf die von den Versicherten gewünschten Zwecke begrenzte Verwendung der Daten durch den Empfänger sichergestellt werden.

In dem Vertrag mit den Versand-Apotheken war zwar eine zweckgebundene Verwendung der Daten, aber nicht deren unverzügliche Löschung nach dem Versand der Informationsschreiben geregelt. Nach der Bewertung des Sachverhaltes hatte ich die AOK aufgefordert sicherzustellen, dass

- eine schriftliche Bestätigung der Apotheken über die Löschung der von Mitte Januar bis Mitte März übermitteln Daten erfolgt,
- weitere Informationen und eine Stellungnahme zu der bisherigen Verfahrensweise erfolgt,
- die Verschlüsselung der Mails bzw. der Anhänge sichergestellt wird,
- der Gesprächsleitfaden um die Frage ergänzt wird, ob der Versicherte mit der Übermittlung der Diabetiker-Eigenschaft einverstanden ist und
- vor der Fortsetzung des Projekts ein angemessenes Datenschutzkonzept für dessen weitere Durchführung vorgelegt wird.

5.7.4.5 Maßnahmen der AOK Hessen

Die AOK hat unverzüglich reagiert und die von mir unter der Ziff. 5.7.4.4 geforderten Maßnahmen umgesetzt. Der Gesprächsleitfaden wurde ergänzt und die Übermittlung durch kennwortgeschützte, komprimierte Dateien sichergestellt. Die Löschung der Adressdaten wurde schriftlich bestätigt. Da die Umsetzung der Maßnahmen unmittelbar realisiert wurde, habe ich von einer förmlichen Beanstandung abgesehen.

5.8 Sozialwesen

5.8.1 Kindeswohl und Datenschutz

Der spezielle kinder- und jugendhilferechtliche Datenschutz hat eine die Förderung des Kindeswohls unterstützende Funktion.

Ein Kreisjugendamt hat um Informationen gebeten, welche Rolle der Datenschutz einnimmt, wenn das Kreisjugendamt, insbesondere auch in Kooperation mit anderen Stellen, zugunsten des Kindeswohls tätig sein will.

Was das Kindeswohl betrifft, ist Ausgangspunkt Art. 6 Abs. 2 Satz 1 GG; diese Vorschrift vertraut das Kindeswohl primär den Eltern an.

Bei der Pflege und Erziehung der Kinder kann es zu Defiziten kommen, wenn die Eltern ihrer verfassungsrechtlichen Pflicht nur unzureichend nachkommen. Deshalb hat der Staat im Hinblick auf das Kindeswohl die sog. "Wächterfunktion", die in Art. 6 Abs. 2 Satz 2 GG verankert ist.

Art. 6 Abs. 2 GG

Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gemeinschaft.

Das Kindeswohl zu sichern ist das Hauptanliegen des Kinder- und Jugendhilfegesetzes (KJHG, SBG VIII). Diesem Ziel dienen auch die spezifischen Datenschutzvorschriften des SGB VIII (§§ 61 ff.). Datenverarbeitung zugunsten des Kindeswohls ist grundsätzlich zulässig. Werden im Rahmen des Kindeswohlschutzes Daten der Eltern verarbeitet, ist deren Recht auf informationelle Selbstbestimmung betroffen, das Verfassungsrang hat (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG). Auch insoweit geht es also um Datenschutz, und es kann hier zu Konflikten mit dem Kindeswohl kommen. Priorität hat unter Beachtung der "praktischen Konkordanz" in diesem Zusammenhang das Kindeswohl, was sich sehr deutlich in § 8a SGB VIII widerspiegelt.

§ 8a SGB VIII

(1) Werden dem Jugendamt gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen bekannt, so hat es das Gefährdungsrisiko im Zusammenwirken mehrerer Fachkräfte abzuschätzen. Dabei sind die Personensorgeberechtigten sowie das Kind oder der Jugendliche einzubeziehen, soweit hierdurch der wirksame Schutz des Kindes oder des Jugendlichen nicht infrage gestellt wird. Hält das Jugendamt zur Abwendung der Gefährdung die Gewährung von Hilfen für geeignet und notwendig, so hat es diese den Personensorgeberechtigten oder den Erziehungsberechtigten anzubieten.

(2) In Vereinbarungen mit den Trägern von Einrichtungen und Diensten, die Leistungen nach diesem Buch erbringen, ist sicherzustellen, dass deren Fachkräfte den Schutzauftrag nach Abs. 1 in entsprechender Weise wahrnehmen und bei der Abschätzung des Gefährdungsrisikos eine insoweit erfahrene Fachkraft hinzuziehen. Insbesondere ist die Verpflichtung aufzunehmen, dass die Fachkräfte bei den Personensorgeberechtigten oder den Erziehungsberechtigten auf die Inanspruch-

nahme von Hilfen hinwirken, wenn sie diese für erforderlich halten, und das Jugendamt informieren, falls die angenommenen Hilfen nicht ausreichend erscheinen, um die Gefährdung abzuwenden.

(3) Hält das Jugendamt das Tätigwerden des Familiengerichts für erforderlich, so hat es das Gericht anzurufen; dies gilt auch, wenn die Personensorgeberechtigten oder die Erziehungsberechtigten nicht bereit oder in der Lage sind, bei der Abschätzung des Gefährdungsrisikos mitzuwirken. Besteht eine dringende Gefahr und kann die Entscheidung des Gerichts nicht abgewartet werden, so ist das Jugendamt verpflichtet, das Kind oder den Jugendlichen in Obhut zu nehmen.

(4) Soweit zur Abwendung der Gefährdung das Tätigwerden anderer Leistungsträger, der Einrichtungen der Gesundheitshilfe oder der Polizei notwendig ist, hat das Jugendamt auf die Inanspruchnahme durch die Personensorgeberechtigten oder die Erziehungsberechtigten hinzuwirken. Ist ein sofortiges Tätigwerden erforderlich und wirken die Personensorgeberechtigten oder die Erziehungsberechtigten nicht mit, so schaltet das Jugendamt die anderen zur Abwendung der Gefährdung zuständigen Stellen selbst ein.

§ 8a SGB VIII betont also den Vorrang des Kindeswohls, selbst wenn das zur Beeinträchtigung der Elternrechte führt.

Ich habe das Kreisjugendamt in diesem Sinne beraten.

5.8.2 Auskunftsanspruch von Unfallversicherungsträgern gegenüber Ärzten

Unfallversicherungsträger haben keinen Anspruch auf Übersendung krankenhausärztlicher Entlassungsberichte, soweit gesetzlich nur ein Auskunftsanspruch vorgesehen ist.

Zwischen einem Unfallversicherungsträger und einem Krankenhaus gab es eine heftige Kontroverse darüber, ob die in § 203 SGB VII (Gesetzliche Unfallversicherung) geregelte Auskunftspflicht von Ärzten so weit reichen kann, dass dem Unfallversicherungsträger der krankenhausärztliche Entlassungsbericht zu übersenden ist. Mir wurde die Angelegenheit zur datenschutzrechtlichen Würdigung vorgelegt.

In § 203 SGB VII ist ausdrücklich nur eine Auskunftspflicht von Ärzten gegenüber Unfallversicherungsträgern normiert.

§ 203 Abs. 1 SBG VII

Ärzte … sind verpflichtet, dem Unfallversicherungsträger auf Verlangen Auskunft über die Behandlung, den Zustand sowie über Erkrankungen und frühere Erkrankungen des Versicherten zu erteilen, soweit dies für die Heilbehandlung und die Erbringung sonstiger Leistungen erforderlich ist. Der Unfallversicherungsträger soll Auskunftsverlangen zur Feststellung des Versicherungsfalls auf solche Erkrankungen oder auf solche Bereiche von Erkrankungen beschränken, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können.

Mit dem vom Unfallversicherungsträger gegebenen Hinweis auf den in § 20 SBG X angeordneten Untersuchungsgrundsatz lässt sich die in § 203 SBG VII nur verfügte Auskunftspflicht nicht zu einer Herausgabepflicht des krankenhausärztlichen Entlassungsberichts "verdichten". Denn rechtssystematisch gilt, dass die spezielle Norm der generellen vorgeht. Das bedeutet hier: Der allgemeine sozialverwaltungsverfahrensrechtliche Untersuchungsgrundsatz tritt hinsichtlich des Informationsflusses zwischen Ärzten und Unfallversicherungsträgern hinter den speziellen § 203 SBG VII zurück, der eben nur eine Auskunftspflicht und keine Pflicht zur Herausgabe des Entlassungsberichts anordnet.

Verweigert somit der Unfallversicherungsträger gegenüber dem Versicherten den Erlass eines begünstigenden Verwaltungsaktes schon allein deshalb, weil der krankenhausärztliche Entlassungsbericht nicht übersendet wird, dann ist dieses Verwaltungshandeln des Unfallversicherungsträgers rechtswidrig. Rechtmäßig ist allein das Anfordern der erforderlichen Informationen, und genau hierauf bezieht sich die in § 203 SBG VII verfügte ärztliche Auskunftspflicht.

Kommt es zu einer sozialgerichtlichen Auseinandersetzung, hat das Sozialgericht zu überprüfen, ob ärztlicherseits der Auskunftspflicht nach § 203 SBG VII Genüge getan wurde. Falls es in der sozialgerichtlichen Praxis vorkommen sollte, den Entlassungsbericht zum Gegenstand des Rechtsstreits zu machen, wäre das mit § 203 SBG VII kaum zu vereinbaren. Jedenfalls würde eine solche sozialgerichtliche Praxis es nicht rechtfertigen, wenn der Unfallversicherungsträger schon im vorprozessualen Stadium unter Verstoß gegen § 203 SBG VII auf der Übersendung des Entlassungsberichts besteht. Die Rechtmäßigkeit einer solchen Verwaltungspraxis lässt sich auch nicht daraus herleiten, dass eine andere Verfahrensweise, also die Erteilung von Auskünften nach § 203 SBG VII, dem Unfallversicherungsträger "bisher völlig fremd" war.

Ich habe das Krankenhaus über die Rechtslage informiert und den Unfallversicherungsträger gebeten, seine Praxis zukünftig an § 203 SBG VII auszurichten.

5.8.3 Übermittlung von Sozialdaten zu Zwecken der Durchführung eines Disziplinarverfahrens

Ohne Einwilligung des Betroffenen ist es nicht zulässig, Sozialdaten zu Zwecken der Durchführung eines Disziplinarverfahrens zu übermitteln.

Im Rahmen eines Disziplinarverfahrens nach der Hessischen Disziplinarordnung forderte der Untersuchungsführer die Übermittlung von Sozialdaten von der Deutschen Rentenversicherung - Hessen -, was diese ablehnte. Daraufhin erbat der Untersuchungsführer von mir Rechtsauskunft zu der Frage, ob er kraft des Disziplinarrechts die Übermittlung von Sozialdaten des Betroffenen beanspruchen kann.

Zwar schreibt § 17 HDO, auf den der Untersuchungsführer hinwies, vor, dass alle Gerichte und Verwaltungsbehörden in Disziplinarsachen dem Untersuchungsführer Rechts- und Amtshilfe zu leisten haben.

In den allgemeinen Vorschriften zum Sozialdatenschutz wird jedoch geregelt, dass im Verhältnis zum Sozialdatenschutz die Regelungen zur Amtshilfe nachrangig sind (§ 37 Satz 3 SBG I), § 67d SBG X, der sich speziell mit den Übermittlungsgrundsätzen bei Sozialdaten befasst, ordnet die ausschließliche Maßgeblichkeit des Sozialrechts bei der Übermittlung von Sozialdaten an.

§ 67d Abs. 1 SGB X

Eine Übermittlung von Sozialdaten ist nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt.

Die Durchsicht der §§ 68 ff. SBG X, insbesondere auch des § 71 SBG X, der die Übermittlung für die Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse betrifft, und des § 73 SBG X, der die Übermittlung für die Durchführung eines Strafverfahrens zulässt, hat jedoch das Resultat, dass eine Übermittlung zu Zwecken der Durchführung eines Disziplinarverfahrens gesetzlich gerade nicht vorgesehen ist. Dies hat zur Konsequenz, dass eine Übermittlung nur dann zulässig wäre, wenn der Betroffene vorher eingewilligt hat (§ 67d Abs. 1 SBG X).

Über diese Rechtslage habe ich den Untersuchungsführer informiert. Mittlerweile ist unter Aufhebung der HDO das Hessische Disziplinargesetz (HDG) vom 21. Juli 2006 in Kraft getreten (GVBl. I S. 394). An der Vorrangigkeit des Sozialdatenschutzrechts hat sich freilich nichts geändert.

5.9 Personalwesen

5.9.1 Datenschutzrechtliche Begleitung der Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung

Auch in diesem Jahr lag ein Schwerpunkt meiner Arbeit in der Begleitung der Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung und dabei in erster Linie bei der Beurteilung der rechtlichen Zulässigkeit von Änderungsanträgen zur Anpassung der Software an die Bedingungen der Landesverwaltung. Außerdem habe ich eine nicht geringe Anzahl von Konzepten zur Weiterentwicklung datenschutzrechtlich bewertet und die Entwickler beraten.

Die im Rahmen der NVS durchgeführten organisatorischen Änderungen in der Landesverwaltung und die gleichzeitige Einführung der Personalverwaltungssoftware SAP R/3 HR erfordert es, die Software immer wieder anzupassen. Je mehr Dienststellen ihre Personaldaten in das System eingepflegt haben, desto mehr Auswirkungen, auch in datenschutzrechtlicher Hinsicht, hatte jede beantragte Änderung. Ebenso waren auch die zu begutachtenden konzeptionellen Weiterentwicklungen zunehmend umfangreicher.

5.9.1.1 Prüfung und Beratung in konzeptionellen Fragen

Ich möchte an dieser Stelle nur einige der von mir datenschutzrechtlich bewerteten und geprüften Konzepte anführen. Über deren Inhalt kann ich nicht konkreter und ausführlicher berichten, weil die teilweise sehr technischen und komplexen Fragestellungen im Rahmen dieses Tätigkeitsberichts nicht so dargestellt werden können, dass sie ohne detaillierte Kenntnisse der verwaltungstechnischen Erfordernisse und der technischen Rahmenbedingungen der Software SAP R/3 HR allgemeinverständlich sind.

Im Einzelnen wurden mir folgende Konzepte vorgelegt:

- Konzept für die SAP-Veranstaltungsmanagement-Korrespondenz

Es war die Frage zu klären, inwieweit den Mitarbeiterinnen und Mitarbeitern im Veranstaltungsmanagement in datenschutzrechtlich zulässiger Weise eine Download-Berechtigung gegeben werden kann.
Mit einer Download-Berechtigung kann praktisch jede Standardauswertung im SAP R/3 HR-System auf den PC des Berechtigten heruntergeladen und dort - auch für andere Zwecke - weiterverarbeitet werden. Deshalb ist die Vergabe dieser Berechtigung im Hinblick auf ihre Erforderlichkeit für die Aufgabenstellung kritisch zu prüfen. Aus Datenschutzsicht sind solche Berechtigungen restriktiv zu handhaben.
Nach dem Konzept können die Mitarbeiterinnen und Mitarbeiter im Veranstaltungsmanagement nur sehr eingeschränkt auf die Daten der Mitarbeiterinnen und Mitarbeiter der hessischen Landesverwaltung zugreifen. Die Download-Berechtigung benötigen sie zur Erfüllung ihrer Aufgaben, um Anwesenheitslisten aus dem System herunterzuladen und aufgrund kurzfristiger Änderungen des Teilnehmerkreises zu bearbeiten. Außerdem müssen Word-Briefe, die im System als Standardbriefe hinterlegt sind, geändert und angepasst werden. Vor dem Hintergrund dieser Aufgabenstellung habe ich dem Konzept zugestimmt.

- Berechtigungsfeinkonzept für die Sachbearbeitersuche

Es war die Frage zu klären, ob und auf welche Einzeldaten im SAP-System, unter Berücksichtigung der besonderen Zugriffsbeschränkungen auf die Daten der Bediensteten des Landesamtes für Verfassungsschutz und der Polizei, die Mitarbeiterinnen und Mitarbeiter der Telefonzentrale der Hessischen Bezügestelle (HBS) zugreifen dürfen, um Anrufer direkt an die für sie in der HBS zuständigen Bediensteten weitervermitteln zu können. Ebenso sind diese Daten für die direkte Weiterleitung der eingehenden Post an die jeweils für die Sachbearbeitung zuständigen Bediensteten notwendig.

Die Sachbearbeitersuche wurde nach meiner Beratung so eingerichtet, dass die Mitarbeiterinnen und Mitarbeiter der Telefonzentrale und der Posteingangsstelle der HBS nur den Vornamen und den Nachnamen der im SAP-System gespeicherten Bediensteten der Landesverwaltung und den für sie zuständigen Sachbearbeiter der HBS einsehen können.
Die zur Suche des jeweiligen Datensatzes notwendigen Merkmale wurden in Absprache mit mir auf das unbedingt notwendige Maß reduziert. Somit wurde sichergestellt, dass in der Telefonzentrale und der Posteingangsstelle der HBS keine Auswertungen über alle Bediensteten von bestimmten Behörden erstellt werden können.
Es kann nur direkt über die Personalnummer oder über die Feldkombinationen Name, Vorname oder Name, Geburtsdatum gesucht werden, so dass davon ausgegangen werden kann, dass nur der gesuchte Datensatz direkt angezeigt wird.

- Konzeption für den Einsatz des Verfahrens IZEMA

IZEMA ist das bei der hessischen Polizei eingesetzte Zeitmanagementsystem zur Erstellung der Schicht- und Arbeitszeitplanung. Das System erfasst und verarbeitet die An- und Abwesenheitsdaten der Bediensteten und übergibt die abrechnungsrelevanten Zeiten über eine entsprechende Schnittstelle in das Abrechnungsverfahren im SAP-System.

Das Konzept wurde in Zusammenarbeit mit mir dahingehend angepasst, dass nur die Daten gespeichert und verarbeitet werden, die zur Erstellung der Schicht- und Arbeitszeitpläne sowie der Erfassung der An- und Abwesenheitsdaten tatsächlich notwendig sind.
Weiterhin wurden umfangreiche Änderungen im Berechtigungskonzept vorgenommen, sodass sichergestellt ist, dass nur die Bediensteten selbst bzw. die für die Erstellung der Schicht- und Arbeitszeitpläne zuständigen Mitarbeiterinnen und Mitarbeiter der jeweiligen Polizeidienststellen auf die Daten zugreifen können.
Ebenso wurden die Auswertungsmöglichkeiten auf den zur Aufgabenerfüllung konkret notwendigen Umfang reduziert.

- Konzept für die Pensionsrückstellungen

Im SAP-System werden die für die Berechnung der Pensionsrückstellung relevanten Daten der Beamtinnen und Beamten sowie die erforderlichen Daten der Angehörigen ausgewertet und dem Hessischen Competence Center (HCC) zur Berechnung der Pensionsrückstellungen übermittelt.

Hier war insbesondere die Frage zu klären, welche Daten von Angehörigen der Beamtinnen und Beamten zur Berechnung der Pensionsrückstellung konkret notwendig sind und somit an das HCC übermittelt werden dürfen.
Strittig war die Frage, ob das Geburtsdatum der Angehörigen vollständig zur Berechnung der Pensionsrückstellung notwendig ist.
Da sowohl die beauftragte Wirtschaftsprüfungsgesellschaft als auch der Hessische Rechnungshof dies als notwendig gefordert hatten, habe ich der Übermittlung des vollständigen Geburtsdatums zugestimmt.

- Konzept für die Altersteilzeitrückstellungen

Es werden die notwendigen Daten der Bediensteten, für die eine im Rechnungswesen zu verbuchende Rückstellung für die Altersteilzeit getätigt werden muss, ausgewertet.
Ich habe das Konzept geprüft und konnte diesem ohne Änderungen zustimmen.

- Konzept "Zentraler Zugriff"

Mit diesem Konzept soll die Problematik des Zugriffs auf Personaldaten von Bediensteten nachgeordneter Behörden datenschutzgerecht gelöst werden. Über diese Problemstellung hatte ich in meinem 34. Tätigkeitsbericht (Ziff. 5.10.2.4) berichtet.

Das Thema hat mich auch in diesem Jahr intensiv beschäftigt. Die Ausprägung des sog. "Merkmals Z" im SAP-System war sehr arbeitsaufwändig. Die notwendigen Anpassungen in den Zuständigkeitsanordnungen der einzelnen Ressorts waren teilweise so unterschiedlich, dass sich die Umsetzung und die Beurteilung der sich daraus ergebenden Konsequenzen für die Hinterlegungen in den Berechtigungen als äußerst schwierig erwiesen.

Das "Merkmal Z" wurde ab der Staffel 06/2006 im System "scharf geschaltet". Die Ressortinteressenvertreter haben mich gebeten, für eine Übergangsphase zunächst in ausgesuchten Behörden die konkreten Auswirkungen auf den Dienstbetrieb testen zu können. Dem habe ich, verbunden mit der Auflage, mir die Ergebnisse der Tests mitzuteilen, zugestimmt. Dies wurde mir fest zugesagt.

Obwohl ich ständig mit dieser Thematik befasst war, habe ich bis zum Redaktionsschluss dieses Berichts keine Mitteilungen erhalten, welche Ressorts das "Merkmal Z" konsequent im System hinterlegt haben und wie konkret weiter verfahren wird, bzw. was das Ergebnis der Tests war.

Leider muss ich in diesem Fall feststellen, dass die Absprachen, die ich im Projektausschuss mit Ressortinteressenvertretern treffe, nicht eingehalten werden. Dies ist um so schwerwiegender, als gerade die Einführung des "Merkmals Z" neben der Erstellung des Berechtigungskonzepts zur Sicherstellung der datenschutzrechtlichen Anforderungen dient, dass nur die Personen und diese auch nur soweit auf Personaldaten zugreifen dürfen, wie dies zur Erfüllung ihrer Aufgaben erforderlich ist. Sollte diese Anforderung beim Einsatz SAP R/3 HR nicht konsequent umgesetzt werden, muss ich dies beanstanden.

Ich werde deshalb eine Auswertung aller Datensätze im SAP R/3 HR-System verlangen und im Einzelnen prüfen, ob die Festlegungen der neuen Zuständigkeitsanordnungen in den jeweiligen Ressorts rechtmäßig im SAP-System hinterlegt worden sind.

5.9.1.2 Freie Auswahl von SAP-Druckern

Von einer hessischen Dienststelle wurde mir eine Druckausgabe einer Jahresentgeltbescheinigung einer Bediensteten übergeben, die bei dieser Behörde nie beschäftigt war. Ich habe diese Angelegenheit sofort überprüft und festgestellt, dass von einer Bediensteten der HBS bei der Druckausgabe ein "falscher" Drucker angesteuert worden war. Dies war möglich, weil das SAP-System so eingestellt war, dass jedem Mitarbeiter der Landesverwaltung alle im SAP-System angeschlossenen Drucker zur freien Auswahl angeboten wurden.

Dieser Sachverhalt wurde in Zusammenarbeit mit der HZD und dem HCC umgehend analysiert. Das System wurde dahingehend geändert, dass jetzt nur noch die Drucker der jeweiligen Dienststellen angesteuert werden können. Somit wird konsequent verhindert, dass Druckausgaben mit hochsensiblen Abrechnungsdaten in "fremden" Dienstellen ausgedruckt werden können.

5.9.1.3 Zugriff auf Einzelabrechnungsergebnisse

Im Rahmen meiner Prüftätigkeiten habe ich festgestellt, dass die Personalkostenhochrechner von vorgesetzten Dienststellen nicht nur die "Hochrechnungsdaten" für ihren Zuständigkeitsbereich erhalten, sondern ihnen auch automatisch alle zugrunde liegenden Einzelabrechnungsergebnisse aller Mitarbeiter des nachgeordneten Bereichs übermittelt werden.

Dies ist unzulässig, weil diese Daten nicht zur Erfüllung der Aufgaben eines Personalkostenhochrechners einer übergeordneten Dienstelle notwendig sind.

Das Programm ermittelt automatisch die Personalkosten für alle im Zuständigkeitsbereich der Personalkostenhochrechner liegenden Dienststellen und deren Personal. Die Verantwortung für die Richtigkeit dieser Daten liegt eindeutig bei der Personaladministration vor Ort und bei der HBS. Eine Überprüfung der Einzelabrechnungsergebnisse durch die Personalkostenhochrechner der vorgesetzten Dienststellen halte ich nicht nur für nicht erforderlich, sondern auch für faktisch unmöglich.
Den Personalkostenhochrechnern müsste in jedem Einzelfall bekannt sein, welche Person mit welcher Vergütungsgruppe und mit welchem Arbeitszeitanteil auf der jeweiligen Stelle geführt wird. Weiterhin müssten die persönlichen Verhältnisse der Bediensteten (Familienstand, Kinderzahl usw.) konkret bekannt sein.

Dies kann nur durch die jeweils Personal führenden Dienstellen, bei denen es jeweils verantwortliche Personalkostenhochrechner gibt, analysiert und verantwortet werden. Dort werden die notwendigen Überprüfungen eigenverantwortlich vorgenommen, so dass die Personalkostenhochrechnungsergebnisse in den vorgesetzten Dienststellen nicht noch einmal personenbezogen überprüft werden müssen.

Dies wurde mir durch mehrere Personalkostenhochrechner von vorgesetzten Dienststellen bestätigt, denen die Einzelabrechnungsergebnisse zwar zur Verfügung gestellt werden, die sie aber nicht nutzen.

Ich werde diese Angelegenheit durch weitere Prüfungen vor Ort weiter untersuchen und gegebenenfalls eine Änderung des Verfahrens der Personalkostenhochrechnung verlangen.

5.9.1.4 Releasewechsel HR in der Hessischen Landesverwaltung

Seit September d. J. bin ich konkret in das Projekt Releasewechsel HR eingebunden und werde dort bis zur Umsetzung beratend mitarbeiten.

5.9.1.5 Fazit und Ausblick

Die Zusammenarbeit mit den aus der Landesverwaltung beteiligten Stellen war immer vertrauensvoll und offen. Eine Ausnahme stellt, wie oben beschrieben, die Umsetzung des "Merkmals Z" dar.

Ich werde auch im nächsten Jahr das SAP-System vor Ort prüfen um sicherzustellen, dass die datenschutzrechtlichen Rahmenbedingungen, so wie von mir geprüft und begutachtet, eingehalten werden.

5.10 Finanzwesen

5.10.1 Kontendatenabrufersuchen nach §§ 93 Abs. 7 und 8, 93b AO

Überprüfungen von Kontendatenabrufersuchen hessischer Finanzbehörden bei den Kreditinstituten haben Mängel vor allem in einer rechtsschutzfähigen Dokumentation der Erforderlichkeit sowie bei der Information der Betroffenen ergeben. Unter dem Vorsitz meiner Dienststelle wurde im Arbeitskreis Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder ein Muster- und Maßnahme-Formular entwickelt und dem Bundesministerium für Finanzen zur Verfügung gestellt, das helfen soll, diese Mängel vor Ort abzustellen.

5.10.2 Rechtliche Grundlagen

Seit 1. April 2005 können Finanzbehörden zu eigenen Zwecken (§ 93 Abs. 7 AO) oder auf Ersuchen von anderen Behörden und Gerichten, die in ihrer Zuständigkeit Gesetze anwenden, die an Begriffe des Einkommensteuergesetzes anknüpfen (§ 93 Abs. 8 AO), über das Bundeszentralamt für Steuern (BZSt) Daten aus den von den Kreditinstituten nach § 24c Abs. 1 KWG zu führenden Dateien automatisiert abrufen, § 93b AO.

Diese von den Banken seit dem 1. April 2003 in besonderen Dateien zum Abruf bereitgestellten Daten dienten ursprünglich der Bekämpfung illegaler Finanzaktionen im Bereich Terrorismus und organisierter Kriminalität und wurden nach den Attentaten vom 11. September 2001 eingeführt. Die Verantwortung für die Zulässigkeit des Abrufs auch durch die Finanzverwaltung trägt die Finanzbehörde (im Fall des Abs. 7) sowie die ersuchende Stelle (im Fall des Abs. 8). Das BZSt darf lediglich prüfen, ob das Ersuchen plausibel ist.

§ 93 Abs. 7 und Abs. 8 AO

(7) Die Finanzbehörde kann bei den Kreditinstituten über das Bundeszentralamt für Steuern einzelne Daten aus den nach § 93b Abs. 1 zu führenden Dateien abrufen, wenn dies zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht.

(8) Knüpft ein anderes Gesetz an Begriffe des Einkommensteuergesetzes an, soll die Finanzbehörde auf Ersuchen der für die Anwendung des anderen Gesetzes zuständigen Behörde oder eines Gerichtes über das Bundeszentralamt für Steuern bei den Kreditinstituten einzelne Daten aus den nach § 93b Abs. 1 zu führenden Dateien abrufen und der ersuchenden Behörde oder dem ersuchenden Gericht mitteilen, wenn in dem Ersuchen versichert wurde, dass eigene Ermittlungen nicht zum Ziele geführt haben oder keinen Erfolg versprechen.

§ 93b AO

(1) Kreditinstitute haben die nach § 24c Abs. 1 des Kreditwesengesetzes zu führende Datei auch für Abrufe nach § 93 Abs. 7 und 8 zu führen.

(2) Das Bundeszentralamt für Steuern darf auf Ersuchen der für die Besteuerung zuständigen Finanzbehörden bei den Kreditinstituten einzelne Daten aus den nach Absatz 1 zu führenden Dateien im automatisierten Verfahren abrufen und sie an die ersuchende Finanzbehörde übermitteln.

(3) Die Verantwortung für die Zulässigkeit des Datenabrufs und der Datenübermittlung trägt in den Fällen des § 93 Abs. 7 die ersuchende Finanzbehörde, in den Fällen des § 93 Abs. 8 die ersuchende Behörde oder das ersuchende Gericht.

(4) § 24c Abs. 1 Satz 2 bis 6, Abs. 4 bis 8 des Kreditwesengesetzes gilt entsprechend.

Die Rechtmäßigkeit eines Kontendatenabrufs kann vom zuständigen Gericht im Rahmen der Überprüfung des Steuer- bzw. Leistungsbescheids oder eines anderen Verwaltungsakts zu dessen Vorbereitung der Kontendatenabruf vorgenommen wurde oder isoliert im Wege der Leistungs- oder (Fortsetzungs-)Feststellungsklage überprüft werden. Da der Gesetzestext keine näheren Angaben zur Durchführung eines Kontendatenabrufersuchens macht, hat das Bundesministerium für Finanzen (BMF) in einem umfangreichen Anwendungserlass zu § 93 Abs. 7 und 8 AO detaillierte Ausführungsvorschriften vorgegeben. Unter Berücksichtigung dieser Konkretisierungen wurde ein einstweiliges Anordnungsverfahren gegen das Inkrafttreten der Normen zum Kontendatenabrufverfahren vor dem Bundesverfassungsgericht zurückgewiesen (BVerfG, Beschluss vom 22. März 2005 - BvR 2357/04, 1 BvQ 2/05). Die Entscheidung zur der Hauptsache über die Verfassungswidrigkeit der zugrunde liegenden Regelungen, insbesondere zu deren Normenklarheit und Verhältnismäßigkeit (s. dazu Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 2. November 2004), steht noch aus.

Derzeit bilden daher die §§ 93 Abs. 7 und 8, 93b AO zusammen mit dem Anwendungserlass (AEAO) zu § 93 AO die rechtliche Grundlage für die bundesweite Durchführung des Verfahrens.

In Hessen wurden von April 2005 bis Juni 2006 laut Auskunft des Hessischen Finanzministeriums insgesamt 1.107 Kontendatenabrufersuchen durchgeführt. Noch ist das Verfahren nicht die Regel, die Tendenz aber steigend. Die Finanzverwaltung hat (Word-)Formulare im Intranet zur Verfügung gestellt, mit denen ein Kontodatenabrufersuchen vom Mitarbeiter des Finanzamtes aktenkundig gemacht werden soll. Zukünftig ist beabsichtigt, das Abrufverfahren zu automatisieren. Zum Zeitpunkt der Prüfungen war das Verfahren noch papiergebunden und wurde auf dem Postweg abgewickelt.

In Hessen wurde der Anwendungserlass des BMF durch Rundverfügung der OFD Frankfurt für den Dienstgebrauch aufbereitet und an die Finanzämter weitergegeben. In allen geprüften Finanzämtern wurden die betroffenen Mitarbeiter in Dienstbesprechungen und mit Hausverfügungen über die anzuwendenden Grundlagen und die Verfahrensweise informiert. Dies sind im Wesentlichen:

I. Bei Kontendatenabrufersuchen der Finanzämter für das Besteuerungsverfahren (§ 97 Abs. 7 AO):

1.
Ein Kontendatenabruf zu eigenen Zwecken der Finanzbehörde nach § 93 Abs. 7 AO soll im gesamten Besteuerungsverfahren des Anwendungsbereichs der Abgabeordnung erfolgen können; auch im Haftungs-, Festsetzungs-, Erhebungs-, Rechtsbehelfs- und Vollstreckungsverfahren.

2.
Nach § 93 Abs. 7 AO kann die Finanzbehörde im Einzelfall folgende Bestandsdaten (Kontenstammdaten) zu Konten- und Depotverbindungen über das BZSt abrufen:

- die Nummer eines Kontos, das der Verpflichtung zur Legitimationsprüfung im Sinne des § 154 Abs. 2 Satz 1 AO unterliegt, oder eines Depots,
- den Tag der Errichtung und den Tag der Auflösung des Kontos oder Depots,

- den Namen sowie bei natürlichen Personen den Tag der Geburt, des Inhabers und eines Verfügungsberechtigten sowie
- den Namen und die Anschrift eines abweichend wirtschaftlich Berechtigten (§ 8 Abs. 1 Geldwäschegesetz).

Kontenbewegungen und Kontenstände können auf diesem Weg nicht ermittelt werden. Dies kann aber im Einzelfall im Verlauf der Sachbearbeitung nach § 93 Abs. 1 AO erfolgen.

3.
Ein Kontendatenabruf steht im Ermessen der Finanzbehörde und darf nur anlassbezogen und zielgerichtet erfolgen. Er muss als Pflichtangabe entweder den Namen und das Geburtsdatum einer natürlichen Person bzw. den Namen einer Personenvereinigung oder juristischen Person enthalten. Bei der Ausübung des Ermessens sind die Grundsätze der Gleichmäßigkeit der Besteuerung, der Verhältnismäßigkeit der Mittel, der Erforderlichkeit, der Zumutbarkeit, der Billigkeit und von Treu und Glauben sowie das Willkürverbot und das Übermaßverbot zu beachten.

4.
Die Erforderlichkeit ist im Einzelfall durch eine Prognose zu ermitteln, dass z.B. aufgrund konkreter Momente oder allgemeiner Erfahrungen ein Kontendatenabruf angezeigt ist.

5.
Die Finanzbehörde soll zunächst der betroffenen Person Gelegenheit geben, Auskunft über ihre Konten und Depots zu erteilen, es sei denn, der Ermittlungszweck würde gefährdet oder eine Aufklärung durch die betroffene Person ist nicht zu erwarten. Hierbei soll auch bereits darauf hingewiesen werden, dass die Finanzbehörde einen Kontendatenabruf durchführen kann, wenn die Sachaufklärung durch Betroffene nicht zum Ziel führt. Wurde von einem Auskunftsverlangen abgesehen, ist die betroffene Person nachträglich über die Durchführung des Kontendatenabrufs zu informieren.

6.
Wurden neue Konten oder Depots festgestellt, ist die betroffene Person über das Ergebnis zu informieren und darauf hinzuweisen, dass die Finanzbehörde das betroffene Kreditinstitut nach § 93 Abs. 1 AO um Auskunft ersuchen kann, wenn ihre Zweifel durch die Auskunft der betroffenen Person nicht ausgeräumt werden. Allerdings kann sich die Finanzbehörde auch unmittelbar an das Kreditinstitut wenden, wenn durch eine vorhergehende Information der betroffenen Person der Ermittlungszweck gefährdet werden würde oder sich aus den Umständen des Einzelfalls ergibt, dass eine Aufklärung durch sie selbst nicht zu erwarten ist. In diesen Fällen ist sie jedoch nachträglich zu informieren. In Vollstreckungsfällen wird die Information im Benachrichtigungsschreiben über die erfolgte Pfändungsmaßnahme aufgenommen.

7.
Wurden die Angaben der betroffenen Person bestätigt, ist diese gleichwohl über die Durchführung des Kontendatenabrufs zu informieren. Dies soll i. d. R. durch einen Hinweis im Steuerbescheid erfolgen.

8.
Die jeweiligen Bediensteten, die Auskunft für den Fortgang der von ihnen bearbeiteten Akten benötigen, führen im internen Verfahrensablauf den Abruf durch. Der Abruf erfolgt mittels eines bundeseinheitlichen Vordrucks. Das Zeichnungsrecht obliegt der Hauptsachgebietsleitung AO (HSGL AO). Die Verfügung des Ersuchens ist zu den Akten zu nehmen. Eine Zweitschrift ist der Hauptsachbearbeitung AO (HSB AO) für statistische Zwecke zuzusenden. Das Original ist auf dem Postweg an das BZSt weiterzuleiten.

II. Bei Kontendatenabrufersuchen der Finanzämter auf Ersuchen anderer Behörden und Gerichte (§ 93 Abs. 8 AO):

1.
Ein Kontendatenabrufersuchen auf Ersuchen einer anderen Behörde, nach § 93 Abs. 8 AO kann die Finanzbehörde durchführen, wenn die andere Behörde im Rahmen ihrer Zuständigkeit ein Gesetz oder eine Rechtsverordnung anwendet, die an Begriffe des Einkommensteuergesetzes anknüpft; dieses sind z.B. "Einkommen", "Einkünfte" oder inhaltsgleiche Begriffe. Das für die Besteuerung der betroffenen Person zuständige Finanzamt ist auch zuständiges Finanzamt für den Kontendatenabruf auf Ersuchen. Innerhalb des Finanzamtes ist die Zuständigkeit im Sachgebiet der HSGL AO zu zentralisieren. Die ersuchende Behörde hat ebenfalls einen bundeseinheitlichen Vordruck zu nutzen. Eine Durchschrift des Ersuchens ist beim Finanzamt in der zentral zuständigen Stelle (HSGL AO) aufzubewahren.

2.
Ein Kontendatenabruf kommt nur in folgenden Fällen in Betracht:

- im Rahmen der Sozialhilfe: Bestimmung der zu berücksichtigenden Einkommen (auch Einkünfte aus Kapitalvermögen) bei der Berechnung von Sozialhilfe;
- im Rahmen der Sozialversicherungen: Bestimmung des Gesamteinkommens i. S. d. Einkommensteuerrechts (§ 16 SGB IV);
- bei der sozialen Wohnraumförderung: Bestimmung des maßgebenden Gesamteinkommens (Summe der positiven Einkünfte);
- bei der Ausbildungsförderung und Aufstiegsförderung: Bestimmung des maßgebenden Einkommens (Summe der positiven Einkünfte);
- bei der Gewährung von Wohngeld: Bestimmung des maßgebenden Gesamteinkommens (Summe der positiven Einkünfte);
- bei der Gewährung von Erziehungsgeld: Bestimmung des maßgebenden Einkommens (nicht um Verluste in einzelnen Einkommensarten zu vermindernde Summe der positiven Einkünfte);

- bei Leistungen zur Unterhaltssicherung: Anrechnung etwaiger Einkünfte bei einem Wehrpflichtigen.

In anderen Fällen ist ein Kontendatenabruf nach § 93 Abs. 8 AO nicht möglich. Bei der Bemessung des Arbeitslosengeldes II ist der Begriff des Einkommens abweichend vom Einkommensteuergesetz definiert, somit liegt kein "Anknüpfen" an Begriffe des EStG und keine Anwendungsmöglichkeit vor.

3.
Der Kontendatenabruf muss zur Klärung des Sachverhaltes unmittelbar geeignet, erforderlich und verhältnismäßig sein. Auch hier genügt eine Prognoseentscheidung der ersuchenden Stelle aufgrund konkreter Momente oder allgemeiner Erfahrungen. Ein Kontodatenabruf ist dann nicht erforderlich, wenn es zur Aufklärung des Sachverhaltes ein ebenso geeignetes, aber für die betroffene Person weniger belastendes Beweismittel gibt. Diese Entscheidung obliegt aber nicht der Finanzbehörde, sondern der ersuchenden Stelle. Sie trägt die Verantwortung für die Zulässigkeit des Datenabrufs und der Datenübermittlung.

4.
Im Ersuchen der anderen Behörde ist daher die Rechtsgrundlage anzugeben und zu versichern, dass eigene Ermittlungen nicht zum Ziel geführt haben. Die Finanzbehörde überprüft die Plausibilität der Angaben. Sie prüft insbesondere, ob die Angaben zur Rechtsgrundlage des Ersuchens nachvollziehbar sind und versichert wurde, dass eigene Ermittlungen nicht zu Ziel geführt haben oder keinen Erfolg versprechen. Zudem sind die Identität und die Authentizität der ersuchenden Behörde oder des ersuchenden Gerichts in geeigneter Weise zu prüfen. Im Beanstandungsfall ist das Ersuchen zurückzugeben.

5.
Die Finanzbehörde erhält das Ergebnis des Ersuchens vom BZSt in einem verschlossenen Briefumschlag und leitet diesen an die ersuchende Stelle weiter. Sie nimmt inhaltlich vom Ergebnis keine Kenntnis und vermerkt die Weiterleitung auf der Aktenausfertigung des Ersuchens.

6.
Die Information der betroffenen Person über die erfolgte Abfrage ist Aufgabe der ersuchenden Stelle. Sie richtet sich nach den im Einzelfall jeweils anzuwendenden gesetzlichen Regelungen, die regelmäßig eine Information für den Fall vorsehen, dass Daten nicht bei der betroffenen Person selbst erhoben werden (§ 67a Abs. 5 Satz 1 SGB X) oder aus dem jeweils geltenden Datenschutzgesetz.

5.10.3 Prüfergebnisse

In der Zeit von April 2005 bis Juni 2006 - die statistischen Werte werden quartalsweise festgestellt - wurden insgesamt von 35 hessischen Finanzämtern 1.092 Kontendatenabrufersuchen nach § 93 Abs. 7 AO und 15 Kontendatenabrufersuchen für andere Behörden/Gerichte nach § 93 Abs. 8 AO gestellt. Die Antwortzeiten des BZSt betrugen zwischen i. d. R. einer und vier Wochen.

Ich habe bei vier Finanzämtern, die laut Statistik eine höhere Anzahl von Abrufen zu eigenen Zwecken und auch einige der wenigen Abrufe auf Ersuchen anderer Behörden gestellt haben, 42 Kontendatenabrufe nach § 93 Abs. 7 AO und 5 Kontendatenabrufe nach § 93 Abs. 8 AO stichenprobenartig ausgewählt und geprüft.

Der Schwerpunkt meiner Prüfung lag auf folgenden Fragen:

1. Wie ist das Verfahren vor Ort organisiert?
2. In welchem Stadium des Besteuerungsverfahrens wurde die Anfrage jeweils durchgeführt?
3. Wurde zuvor eine Auskunft der betroffenen Person eingeholt?
4. Ob und wie wurde die Erforderlichkeitsprüfung durchgeführt und dokumentiert?
5. Wann und wie wurden die Betroffenen über den Kontendatenabruf informiert?
6. Wie "erfolgreich" war der Abruf?

Zu 1: Wie ist das Verfahren vor Ort organisiert?

Bei allen Stichproben entsprach der organisatorische Ablauf in den einzelnen Finanzämtern zunächst den Vorgaben und war im Wesentlichen gleich ausgestaltet:
Sowohl in den Fällen des § 93 Abs. 7 AO als auch im Bereich des § 93 Abs. 8 AO wurde der vorgesehene bundeseinheitliche Vordruck benutzt.
In den Fällen des § 93 Abs. 7 AO wurde der Vordruck in dreifacher Ausführung von dem oder der sachbearbeitenden Bediensteten ausgefüllt und zur Zeichnung an den HSGL AO gegeben. Von dort ging eine Durchschrift HSB AO zur Führung der Statistik, eine weitere verblieb bei HSGL AO. Das Original der Anfrage erhielt der oder die sachbearbeitende Bedienstete zur Anfrage an das BZSt und Ablage für die Akte. Die Antwort des BZSt ging direkt an die sachbearbeitende Person.
In Fällen des § 93 Abs. 8 AO wurde vermerkt, dass die Antworten des BZSt in verschlossenem Umschlag an die ersuchende Behörde weitergeleitet wurden.

Verbesserungswürdig waren allerdings einzelne Umsetzungsdetails. So waren z.B. bei einem Finanzamt im Statistikordner auch Kopien der Antworten des BZSt von erfolgreichen Ersuchen nach § 93 Abs. 7 AO abgeheftet, um die Erfolge zu dokumentieren. Diese Unterlagen sind für die Statistik nicht erforderlich und deshalb zu entfernen. Für die Statistik werden nur die kumulierten Ergebnisse (festgesetzte Mehrsteuern oder gezahlte Mehrsteuern) benötigt. In einem anderen Fall wurden die Ersuchen nach § 93 Abs. 8 AO nicht wie vorgesehen zentral beim HSGL AO abgelegt, sondern der jeweiligen Steuerakte hinzugefügt. Auch das wurde mittlerweile abgestellt.

Zu 2: In welchem Stadium des Besteuerungsverfahrens wurde das Ersuchen durchgeführt?

Es fiel auf, dass ca. 85 % der Kontendatenersuchen von Beschäftigten im Vollstreckungsbereich, weitere ca. 13 % im Bereich der Betriebsprüfung und die wenigsten Fälle (ca. 2%) im Bereich der Veranlagung gestellt wurden. Dies scheint ein bundesweiter Trend zu sein, denn das Ergebnis entspricht auch den Feststellungen der Datenschutzbeauftragten der anderen Bundesländer, soweit dort ähnliche Prüfungen durchgeführt wurden. Dies entspricht aber nicht der ursprünglichen Intention bei Einführung des Verfahrens, wonach die Notwendigkeit des Kontendatenabrufverfahrens mit der Möglichkeit zur Entdeckung hinterzogener Kapitalerträge begründet wurde.

Zu 3: Wurde zuvor eine Auskunft des Betroffenen eingeholt?

In den meisten Fällen waren ebenfalls keine Vermerke erkennbar, die dokumentierten, dass ein vorangegangenes Auskunftsersuchen oder eine Anhörung der betroffenen Person i. S. d. § 93 AO durchgeführt wurde. Zum Teil ergaben sich Hinweise beim intensiveren Aktenstudium, dass die Steuerpflichtigen nach Konten gefragt wurden. Ohne einen solchen Hinweis konnte aus den Akten nicht entnommen werden, ob bzw. aus welchen Gründen eine Anhörung unterblieb.

Zu 4: Ob und wie wurde die Erforderlichkeitsprüfung durchgeführt und dokumentiert?

Willkürliche und datenschutzrechtlich bedenkliche Routineabfragen habe ich nicht festgestellt. In einem Finanzamt waren Vermerke zur Erforderlichkeit eines Ersuchens angeordnet, dort war der Ablauf des Kontendatenabrufverfahrens nachvollziehbar und transparent.

Ansonsten war die Durchführung einer vorgeschalteten Erforderlichkeitsprüfung im Einzelfall nicht immer sofort erkennbar, nach Durchsicht der Akte bestanden aber jeweils keine Zweifel, dass der Kontendatenabruf erforderlich war. Es fehlte jedoch fast durchgängig an einer geeigneten Dokumentation. Im Bereich der Vollstreckungsverfahren haben einige Finanzämter die Durchführung eines Ersuchens per se für erforderlich gehalten, wenn der rückständige Steuerbetrag mindestens 25.000 € betrug. Gleichwohl war auch in diesen Fällen die Erforderlichkeit im Einzelfall vorhanden, da dort bereits sämtliche bekannten Vollstreckungsmöglichkeiten ausgeschöpft waren und der Steuerschuldner oder die Steuerschuldnerin erkennbar nicht mitwirkte.
Gerade in Bezug auf die Dokumentation der Ermessensentscheidung waren unterschiedliche Anordnungen getroffen. In einem Fall wurden bei der Vorlage zur Zeichnung durch den HSGL AO die Akten beigefügt, in einem anderen Fall wurde lediglich überwacht, ob bestimmte Sachgebiete überproportional Kontendatenabrufersuchen einleiten. In diesen Fällen war dann auch nicht auf den ersten Blick erkennbar, wie es zu der Entscheidung gekommen ist. Bei intensiver Durchsicht der Akte wurde dann zwar das Ergebnis bestätigt, die exakten Gründe im Einzelfall waren aber letztendlich nicht dokumentiert.

In einem weiteren Amt waren nur die Veranlagungsbezirke und die Betriebsprüfer angewiesen, die Ermessensentscheidung für ein Kontendatenabrufersuchen zu dokumentieren, da im Vollstreckungsbereich von einer offenkundigen Erforderlichkeit ausgegangen werden sollte. Zum Teil wurden die Erwägungen die zum Ersuchen führten, in Aktenvermerken festgehalten oder in Gesprächsnotizen z.B. mit dem Steuerberater der Betroffenen erwähnt. Eine übersichtliche Nachvollziehbarkeit konnte insbesondere in solchen Akten festgestellt werden, die ein sog. Aktenvorblatt enthielten, auf dem alle wesentlichen Schritte der Aktenbearbeitung vermerkt waren. Allerdings enthielten die Akten auch bei dieser Verfahrensweise nicht immer eine summarische Dokumentation über die Erforderlichkeitsprüfung und Prognoseentscheidung. Im Hinblick auf die Nachvollziehbarkeit der Entscheidung bei einem Bearbeiterwechsel oder der Nachprüfung der Zulässigkeit durch das Gericht ist eine nachvollziehbare (summarische) und transparente Dokumentation der Begründung in jedem Fall erforderlich.

In den Fällen des § 93 Abs. 8 AO kamen die Ersuchen sämtlich von Kreisbehörden, die im Rahmen der Gewährung von Sozialhilfe tätig wurden. Die anfragende Behörde hatte die Rechtsgrundlagen benannt und versichert, dass eigene Ermittlungen nicht zum Ziel geführt haben. Diese Angaben waren (durch Handzeichen gekennzeichnet) vom jeweiligen HSGL AO abgezeichnet worden. In einem Fall wurde das Ergebnis der vom Finanzamt kurz zuvor zufälligerweise zu eigenen Zwecken veranlassten Abfrage an das ersuchende Sozialamt weitergeleitet. Dies entsprach zwar nicht dem Zweck, konnte aber aufgrund der näheren Umstände in diesem Einzelfall so gelöst werden.

Zu 5: Wie "erfolgreich" war der Abruf?

Die tatsächlichen Erfolge eines durchgeführten Kontendatenabrufs waren ebenfalls sehr unterschiedlich. Es gab einzelne, wenige erfolgreiche Fälle, in denen z.B. in einem Besteuerungsverfahren zusätzlich 22.000 € Steuer festgesetzt oder in einem Vollstreckungsverfahren zusätzlich 9.300 € vollstreckt werden konnten. Es gab einige Fälle, in denen zwar "neue" Konten offengelegt wurden, diese aber trotzdem mangels Masse nicht belastet werden konnten. Ein Erfolg des Abrufs war jedoch aus den übrigen Akten nicht zu entnehmen. Eine aussagekräftige Gesamt-Erfolgsstatistik liegt mir nicht vor. Die Mitarbeiter der Finanzämter hatten sich jedenfalls größere Erkenntnisse erhofft.

Über die Erfolge der Abfragen nach § 93 Abs. 8 AO war zutreffend in den Akten der Finanzämter nichts festgehalten worden. Derartige Ergebnisse dürfen sich nur in den Akten der ersuchenden Behörde befinden.

Zu 6: Wann und wie wurden die Betroffenen über den Kontendatenabruf informiert?

Bei den meisten Kontendatenabfragen war nicht auf Anhieb erkennbar, ob und wie eine Information der Betroffenen stattgefunden hat. In einzelnen Fällen konnte aus kurzen Gesprächsnotizen, die aber unabhängig von der Bearbeitung des Kontendatenabrufersuchens an anderer Stelle gefertigt waren, Hinweise entnommen werden, dass z.B. die Steuerberatung in einem

Telefonat informiert wurde oder der oder die Steuerpflichtige selbst in einem Gespräch über den Ablauf der Betriebsprüfung auf die allgemeine Möglichkeit aufmerksam gemacht wurde.

Allerdings waren viele Verfahren auch noch nicht abgeschlossen und daher eine zeitlich zusammenhängende Information durchaus noch möglich. Eine organisatorische Kontrolle, wonach eine Information der betroffenen Person zu einem geeigneten Zeitpunkt durchgeführt werden soll, war in keinem der geprüften Finanzämter vorhanden.

Lediglich bei Kontendatenabrufersuchen in Vollstreckungsverfahren wurde von der OFD zwischenzeitlich in das Schreiben an die Person des Steuerschuldners, mit dem sie über die Pfändungsmaßnahme informiert wird, auch formularmäßig der Hinweis aufgenommen, dass die Maßnahme auf den Informationen eines Kontendatenabrufs beruhen. Eine Information der Betroffenen über die Erkenntnis ggf. neuer, von ihnen nicht angegebener Konten, habe ich in keinem der geprüften Fälle feststellen können. Auch diese Feststellungen entsprachen den Erfahrungen der datenschutzrechtlichen Stichprobenprüfungen in den anderen Bundesländern.

5.10.4 Bewertung

Zusammenfassend ist festzustellen, dass das Verfahren derzeit insbesondere im Steuerfestsetzungs- und Steuererhebungsverfahren zurückhaltend eingesetzt wird. Das Verfahren hat sich in erster Linie weg vom Steuererhebungsverfahren hin zu einem Werkzeug der Vollstreckung rückständiger Steuerforderungen entwickelt. Dies liegt m. E. daran, dass das Verfahren noch papiergebunden abläuft, die Rücklaufzeiten zu langwierig sind und die Ergebnisse nicht den erhofften Erfolg brachten. Dem Grunde nach wird das Verfahren zwar nach Erforderlichkeitsgesichtspunkten eingesetzt. Allerdings lässt die Dokumentation der Entscheidung und die Information des Betroffenen zu wünschen übrig. Im Hinblick auf die Nachvollziehbarkeit der Entscheidung bei einem Bearbeiterwechsel oder der Nachprüfung der Zulässigkeit durch das Gericht ist eine Dokumentation der Begründung erforderlich. Die rechtzeitige und vollständige Information des Betroffenen ist erforderlich, damit dieser auch von seiner Rechtsweggarantie Gebrauch machen kann.

Da diese Feststellungen durch Prüfungen der Datenschutzbeauftragten auch in anderen Bundesländern getroffen wurden, hat der Arbeitskreis Steuer der Datenschutzbeauftragten des Bundes und der Länder (AK Steuer) ein Muster- und Maßnahme-Formular entwickelt, das helfen soll, die organisatorischen Mängel zu beheben. Es wurde vorgeschlagen, die Ermessensentscheidung, die zum Kontendatenabruf führt, jeweils durch einen summarischen Vermerk festzuhalten und diesen zusammen mit dem Antrag dem HSGL AO zur Plausibilitätsprüfung vorzulegen. Durch entsprechende Wiedervorlagefristen soll die Information des Betroffenen zum angemessenen Zeitpunkt gewährleistet werden. Der AK Steuer hat das Formular über den BfDI dem BMF mit der Bitte um Umsetzung zur Verfügung gestellt.

Inwieweit der Einsatz des Kontendatenabrufverfahrens hauptsächlich zum Zweck der Vollstreckung von Steuerrückständen zulässig ist, wird vermutlich erst das erwartete Urteil des Bundesverfassungsgerichts zum Normenkontrollverfahren klären.

6. Kommunen

6.1 Ergebnis der Prüfung von Kommunen

Kommunen haben ihre Datenverarbeitung sehr unterschiedlich strukturiert. Zwischen den Positionen eines autonomen DV-Betriebs und einer kompletten Auslagerung auf einen externen Dienstleister findet man alle Ausprägungen. Ich habe im Berichtszeitraum sowohl Kommunen geprüft, die ihre Datenverarbeitung weitgehend selbständig organisieren als auch solche, die sich der Hilfe externer Dienstleister bedienen, um festzustellen, ob es typische Problemstellungen gibt.

6.1.1 Ausgangslage

Nicht zuletzt aufgrund ihrer Größe haben Kommunen ihre EDV unterschiedlich organisiert. Während es für große Kommunen möglich ist, die EDV mit eigenem Personal zu betreiben, können gerade kleinere Gemeinden diese Aufgabe nicht oder nur zum Teil selbst bewältigen. Durch eine Eingabe wurde ich mit einem Fall konfrontiert, in dem es zwischen dem Bürgermeister und dem IT-Bereich der Verwaltung zu Streit kam. Es wurden Externe eingeschaltet, und nach kurzer Zeit eskalierte das Geschehen derartig, dass ein ordnungsgemäßer IT-Betrieb nicht mehr möglich war. Als ich eingeschaltet wurde, war die Lage so verworren, dass ich nur noch eine Schadensbegrenzung erreichen konnte. Beim Versuch, das Zusammenspiel zwischen Mitarbeitern der Verwaltung, externem Personal und politischen Gremien zu entwirren, zeigte sich, dass Verträge, Konzepte, die Dokumentation und Dienstanweisungen nicht oder nur rudimentär vorhanden waren. Bei der IT-Sicherheit gab es ebenfalls Defizite.

In der Zwischenzeit hat sich die Kommune von dem alten externen Dienstleister getrennt. Die Datenverarbeitung soll nun auch wieder mit Hilfe externen Sachverstands neu strukturiert werden. Ich habe gefordert, dass mir die Konzepte und Unterlagen, aus denen sich die zukünftige IT-Architektur und die Verantwortlichkeiten zwischen Auftraggeber (Kommune) und Auftragnehmer ergeben, zur Prüfung vorgelegt werden.

Für mich stellte sich die Frage, ob es sich um einen Einzelfall handelt oder ob vergleichbare Vorkommnisse auch in anderen Kommunen vorkommen könnten. Ich habe mich daher entschlossen, den IT-Einsatz von Kommunen mit dem Schwerpunkt auf vertragliche Regelungen mit externen Dienstleistern und organisatorische Regelungen zu prüfen. Weiterhin sollte festgestellt werden, ob es bei der Technik und den Sicherheitskonzepten Defizite gibt.

6.1.2 Prüfungen

Im Folgenden werde ich wesentliche Ergebnisse der Prüfungen skizzieren und meine Schlussfolgerungen darlegen.

6.1.2.1 IT-Betrieb mit eigenem Personal Technischer und personeller Rahmen

Die systemtechnische Betreuung nahmen vier Personen der IT-Abteilung vor. Es waren zwei Administratoren für die Infrastruktur (Netz, Betriebssystem) und zwei Mitarbeiter für die Betreuung der Hardware zuständig. Für die als Fachverfahren eingesetzte Software gab es jeweils eigene Administratoren und Betreuer. Lediglich der Internetauftritt und die Firewall wurden durch einen externen Dienstleister betreut.

Der Firewallrechner war im Serverraum der Kommune untergebracht. Er wurde ausschließlich von der externen Firma betreut. Erforderliche Anpassungen wurden von autorisierten Mitarbeitern der IT-Abteilung per E-Mail bzw. über ein Webinterface beim Dienstleister veranlasst, der dann die erfolgte Anpassung meldete. Mitarbeiter der Kommune, auch der IT-Abteilung, hatten weder schreibende noch lesende Zugriffsrechte auf dem System. Zur internen Kontrolle erfassten sie daher die in Auftrag gegebenen Änderungen in einer Tabelle. Da die Firewall ausschließlich für die Kommune betrieben wurde, habe ich gefordert, den mit dem Netzbetrieb betrauten und verantwortlichen Mitarbeitern der Kommune einen Lesezugriff auf das Regelwerk einzurichten, um die erforderliche Kontrolle und den Abgleich mit o. g. Tabelle zu ermöglichen. Bei Sicherheitsvorkommnissen sollte in der Kommune auch die IT-Abteilung informiert werden.

Ein Netzwerk auf Basis des Betriebssystems Windows besitzt ein Verzeichnis aller im Netz vorhandenen Ressourcen (wie Domänen, Organisationseinheiten, Benutzer oder Computer) mit deren Eigenschaften. In diesem sog. Active Directory (AD) werden auch die Sicherheitsoptionen festgelegt. Auf die Informationen können Netzwerkanwendungen oder andere Dienste zugreifen. Das AD ist das Nervenzentrum des Netzwerkes. Es wurde von Mitarbeitern der Kommune administriert. Die Abbildung der Organisationsstruktur der Verwaltung im AD erfolgt über Organisationseinheiten (OU).

Die Sicherheitseinstellungen im AD orientieren sich im Wesentlichen an den Windows-Standardeinstellungen. Diese lagen in einigen wenigen Punkten unter den Anforderungen des Grundschutzhandbuchs des BSI. Da die Vorgaben des Grundschutzhandbuchs bei personenbezogenen Daten das Mindestniveau beschreiben, habe ich eine Anpassung gefordert.

Beim Versuch, im Netz auf fremde Verzeichnisse zuzugreifen, konnte ich feststellen, dass in einigen wenigen Fällen unberechtigte Zugriffe möglich waren. Dies betraf vor allem Fachverfahren, bei denen es nicht möglich war, die Zugriffsmöglichkeiten über die Systemebene zu unterbinden. Um unzulässige Zugriffe zu erschweren, habe ich vorgeschlagen, über eine Gruppenrichtlinie das Netzwerk für den Benutzer an seinem Arbeitsplatz auszublenden. Mittels eines Skripts können dann die benötigten Laufwerke zugeordnet werden. Diese Option sollte insbesondere in Betracht gezogen werden, wenn Unbefugten die Zugriffsrechte wegen entgegenstehender Softwareanforderungen nicht entzogen werden können.

Die E-Mail-Nutzung war nur für dienstliche Zwecke zulässig. Der Posteingang wurde durch mehrere Virenscanner geprüft, verdächtige bzw. infizierte E-Mails wurden in Quarantäneverzeichnisse gestellt, die von den Administratoren geprüft wurden. Es erfolgte weiterhin eine Kennzeichnung von erkannten Spam-Mails. Diese wurden im Betreff gekennzeichnet und den Benutzern zugestellt.

Generell war der Gesichtspunkt der Revision und Nachvollziehbarkeit noch nicht ausreichend berücksichtigt. Es gab keine Vorgabe, was zu protokollieren ist, wer Auswertungen vorzunehmen hat und wem die Ergebnisse vorzulegen sind. Um die Revision der IT-Sicherheit möglich zu machen, habe ich angeregt, einen Sicherheitsprozess zu initiieren. Nachdem das zu erreichende Sicherheitsniveau definiert ist, können dann die Umsetzung und anschließend die permanente Kontrolle (i. S. v. Revision) festgelegt werden. Dazu müssen die Verantwortlichkeit und die Maßnahmen geregelt sein. Dies hat auch Konsequenzen für die Auftragskontrolle.

Vertragliche Regelungen

Der Dienstleister betrieb nicht nur den Internetauftritt, sondern administrierte auch die eingesetzte Firewall für den Internetzugang durch die Kommune. Im Rahmen der Administration der Firewall erhielt der Dienstleister auch Zugang zu personenbezogenen Mitarbeiterdaten. Das bedeutet, bei dem Dienstleistungsverhältnis handelte es sich um ein Vertragsverhältnis i. S. d. § 4 HDSG. Dies hatte zur Folge, dass die rechtlichen Rahmenbedingungen von § 4 HDSG einzuhalten waren und bedeutete insbesondere, dass sich aus den vertraglichen Regelungen ergeben muss, welche Rechte und Pflichten der Auftragnehmer im Einzelnen hat. Das war von besonderer Bedeutung für die Auswertung etwaiger Bedienstetendaten im Zusammenhang mit der Nutzung von E-Mail und Internet. Bei einem Vertrag zur Auftragsdatenverarbeitung ist es zudem erforderlich, dass sich der Auftragnehmer verpflichtet, die Vorschriften des HDSG einzuhalten und sich der Kontrolle durch den Hessischen Datenschutzbeauftragten unterwirft (§ 4 Abs. 3 HDSG). Der abgeschlossene Vertrag enthielt diesbezüglich keine Regelungen. Insoweit musste er ergänzt werden. Als Problem stellte sich heraus, dass der Auftraggeber zwar grundsätzlich die rechtliche Verantwortung für die Verarbeitung der Daten behält, aber nicht die Möglichkeit hatte nachzuvollziehen, was der Auftragnehmer im Zusammenhang mit den Protokolldaten der Firewall macht. Die Kommune hatte keinen Zugriff.

Organisatorische Regelungen zur Telearbeit sowie E-Mail- und Internetnutzung

Die Dienstanweisung zur Telearbeit musste an wenigen Stellen angepasst werden. Die Einbeziehung des behördlichen Datenschutzbeauftragten war nicht klar geregelt. Ferner gab es eine Nebenabrede über die alternierende Telearbeit in der es hieß: *"Die Arbeitnehmerin gestattet zu diesem Zwecke den berechtigten Mitarbeitern des Arbeitgebers den Zutritt zum häus-*

lichen Tele-Arbeitsbereich." Hierzu habe ich angemerkt, dass auch alle anderen erwachsenen Mitbewohner ihr Einverständnis zum Zutritt zur Wohnung erklären müssen, da sie nur persönlich dem Grundrechtseingriff zustimmen können.

In der Dienstanweisung zur E-Mail- und Internetnutzung war die private Nutzung von E-Mail und Internet untersagt. Es gab jedoch eine Diskussion, inwieweit eine E-Mail-Filterung vorgenommen werden darf. (Eine ausführliche Beschreibung der rechtlichen und technischen Problemstellung findet sich in Ziff. 8.2.) Der Diskussion lag zugrunde, dass die Zusendung privater E-Mails nicht komplett zu unterbinden ist. Gleichwohl fallen Informationen in diesen E-Mails selbstverständlich unter das Fernmeldegeheimnis. Der Außenstehende weiß u. U. von dem Verbot nichts. Um das Problem weitgehend in den Griff zu bekommen, habe ich angeregt, in der Dienstanweisung einen Hinweis aufzunehmen, dass die Mitarbeiter verpflichtet sind, den Absender einer privaten E-Mail unverzüglich auf das Verbot hinzuweisen. Weiterhin wurde angesprochen, ob E-Mails, die aufgrund eines Spamfilters als solche gekennzeichnet werden, vorab gelöscht werden können (dies sollte auch für erkennbar private E-Mails gelten). Eine solche Lösung halte ich sowohl rechtlich für unzulässig als auch faktisch für äußerst problematisch. Durch Spamfilter werden u. U. E-Mails als Spam-Mails gekennzeichnet, die ordnungsgemäßer Posteingang sind. Als bedenklich betrachte ich daher den Einsatz von ORDB (Open Relay Database): E-Mails von E-Mail-Domänen, die in die ORDB eingetragen waren, wurden direkt gelöscht. Bei der zunehmenden Bedeutung des elektronischen (Rechts-)Verkehrs ist dies insoweit bedenklich, da Provider, über deren Server viele Spam-Mails versandt werden (ohne dass sie selbst direkt beteiligt sind) sehr schnell in die ORDB-Listen eingetragen werden. Das Entfernen aus dieser Datenbank ist aufwändig (zuzüglich der Zeit, bis dies vom Betroffenen erkannt worden ist), sodass hierbei nicht auszuschließen ist, dass E-Mails von Bürgern, die zufällig diesen Provider benutzen, ungelesen gelöscht würden.

Da elektronische Nachrichten grundsätzlich rechtserheblich sind, würden u. U. solche rechtserheblichen Nachrichten praktisch automatisiert aus dem Posteingang gelöscht. Außerdem stellt das Löschen eine strafbewehrte Datenunterdrückung nach § 303a StGB dar, gleichgültig, ob nur dienstliche oder auch private E-Mail-Kommunikation über die IT-Systeme der Kommune zulässig ist. Eine rechtlich zulässige Lösung ist es, die Nachricht dem Empfänger nicht direkt zuzustellen, sondern in einen separaten Quarantänebereich zu verschieben, aus dem sie nach Ablauf einer per Dienstvereinbarung festgelegten Frist gelöscht wird. Hier hat der Empfänger die Möglichkeit, die eingehenden E-Mails zu überprüfen. Für den Bereich "ORDB-Listen" habe ich ebenfalls eine Quarantäne- bzw. Markierungslösung gefordert.

6.1.2.2 IT-Betrieb durch einen Dienstleister

Eine andere Kommune hat einen anderen Ansatz verwirklicht. Die IT der Stadtverwaltung wurde vollständig durch einen externen Dienstleister betreut. Sämtliche IT-Systeme, bis auf das Internetangebot, befanden sich in den Räumen der Kommune. Das Personal des Dienstleisters arbeitete in den Räumen und an Geräten der Kommune. Um auf die Anforderungen der Kommune schnell reagieren zu können, stellte die mit der Organisation der IT betraute Firma einen Mitarbeiter nur für die Kommune ab, der sämtliche DV-Komponenten betreute. Erforderliche Maßnahmen wurden mit dem Leiter des Hauptamts abgesprochen. Eine schriftliche Dokumentation der Anforderung von Maßnahmen gab es allerdings nicht.

Die Sicherheitseinstellungen im AD orientierten sich an den Windows-Standardeinstellungen. Gruppenrichtlinen wurden für sehr wenige Einstellungen (u.a. Internet Explorer) angewendet.

Die Arbeitsplätze wurden nach einer Standardvorgabe eingerichtet. Die Benutzer hatten im Wesentlichen Hauptbenutzer-Rechte, bei einigen Anwendungen waren lokale Administratorrechte erforderlich. Durch Ausblenden der Netzwerkumgebung war sichergestellt, dass die Benutzer nur die ihnen per Anmeldeskript zugeordneten Netzlaufwerke erreichen konnten.

Die Nutzung des Internetzugangs war nur für dienstliche Zwecke zulässig. Dies war in einer Dienstanweisung geregelt. Eine Protokollierung des Internetzugangs fand statt. Die Protokolle wurden täglich ausgewertet. Der Auftragnehmer informierte das Hauptamt bei besonderen Vorkommnissen. Ergänzend habe ich einen regelmäßigen, monatlichen Bericht angeregt. Die E-Mail-Nutzung war ebenfalls nur für dienstliche Zwecke zulässig. Jeder Mitarbeiter konnte E-Mails von seinem Arbeitsplatz aus versenden. Der E-Mail-Eingang erfolgte zentral über das Hauptamt. Die eingehenden E-Mails wurden nach Sichtung durch die Mitarbeiterinnen im Sekretariat des Hauptamts an die Mitarbeiter weitergeleitet.
Als Spam erkannte E-Mails wurden nach Markierung an ein zentrales Postfach umgeleitet, das vom IT-Dienstleister überwacht wurde.

Die Einzelaufträge an den Dienstleister wurden in der Regel telefonisch oder in Quartalsgesprächen mündlich erteilt. Dies galt beispielsweise auch für das Anlegen von Benutzerkennungen und die Zuordnung von Zugriffsrechten. Eine schriftliche Dokumentation der Aufträge, z.B. auch in Form eines Protokolls der Gespräche gab es nicht. Hier habe ich gefordert, die Aufträge schriftlich zu erteilen oder zu bestätigen, so dass sie mit der Konfiguration der Systeme und der Dokumentation abgeglichen werden können.

Organisatorische Regelungen

Die vorgelegten Unterlagen (Sicherheitsrichtlinien, Dienstanweisungen) waren vorbildlich in Vollständigkeit, Umfang und Verständlichkeit. Sie gaben während der Durchsicht nur an wenigen Stellen Grund zu Nachfragen oder Ergänzungen. Offensichtliche Abweichungen zwischen Richtlinien und der technischen Implementierung wurden nicht gefunden. Bei der Ausgestaltung der Verträge und der organisatorischen Abläufe waren noch Anpassungen nötig.

Vertragliche Regelungen

Die private Firma war mit der Erbringung sämtlicher IT-Dienstleistungen der Kommune beauftragt. Der Dienstleister administrierte das gesamte Netz der Kommune und hatte damit auch Zugang zu personenbezogenen Daten. Grundsätzlich

kann eine Kommune zur Erfüllung ihrer Aufgaben auch die Hilfe eines externen Dienstleisters in Anspruch nehmen. Sie kann im Wege der Auftragsdatenverarbeitung insoweit externes Know-how nutzen. Die datenschutzrechtlichen Voraussetzungen unter denen dies geschehen kann, ergeben sich aus § 4 HDSG.

Erteilt die Kommune einer privaten Firma einen derartigen Datenverarbeitungsauftrag, so bleibt sie jedoch für die Einhaltung der Vorschriften des Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich, soweit personenbezogene Daten verarbeitet werden. Der Auftragnehmer ist insoweit an die Weisungen seines Auftraggebers gebunden. Der Auftraggeber hat diese Weisungsbefugnis auch auszuüben. Hierzu ist in einem Vertrag genau festzulegen, welche Rechte und Pflichten jeweils Auftraggeber und Auftragnehmer im Einzelnen haben.

Dem Auftraggeber muss es auch möglich sein nachzuvollziehen, was der Auftragnehmer für ihn tut. Da im vorliegenden Fall das gesamte technische Know-how auf Seiten des Auftragnehmers lag, ist es besonders wichtig, dass die Festlegungen des Administrators dokumentiert werden. An eine derartige Dokumentation sind hohe Qualitätsanforderungen zu stellen; denn sollte - aus welchen Gründen auch immer - der private Dienstleister nicht mehr zur Verfügung stehen, muss die Verwaltung in der Lage sein, Ihren Betrieb fortzuführen. Die detaillierte Dokumentation dient dazu, dass die Kommune auch in einem solchen Fall (u. U. unter Zuhilfenahme eines sachverständigen Dritten) die getroffenen Festlegungen nachvollziehen kann. Auch dies ist vertraglich sicherzustellen.

An einer entsprechenden vertraglichen Regelung, aus der sich klar die Rechte und Pflichten von Auftraggeber und Auftragnehmer ergeben, fehlte es. Es gab lediglich eine Auftragserteilung für die DV-Dienstleistungen und die Verpflichtungserklärung, bekannt gewordene Daten nicht preiszugeben.

Ein zusätzliches Problem ergab sich daraus, dass der Auftragnehmer grundsätzlich die Möglichkeit hatte, auf Daten zuzugreifen, die dem Steuergeheimnis unterliegen (z.B. Hundesteuerdaten): Wenn man unterstellt, dass die Tätigkeit des privaten Auftragnehmers im weitesten Sinn der Veranlagung i. S. v. § 30 Abs. 4 Nr. 1 AO dienlich ist, muss er hinsichtlich der Wahrung des Steuergeheimnisses und unter Hinweis auf die strafrechtlichen Folgen einer Pflichtverletzung besonders verpflichtet werden.

Schließt eine öffentliche Stelle mit einer privaten Firma einen Vertrag zur Auftragsdatenverarbeitung ab, so gilt für die Firma im Regelfall das Bundesdatenschutzgesetz. Damit aber für die Daten verarbeitende Stelle Kommune und ihren Auftragnehmer gleiche Rechtsbedingungen herrschen, schreibt § 4 Abs. 3 HDSG für diesen Fall vor, dass sich der Vertragspartner, für den das Hessische Datenschutzgesetz nicht gilt, vertraglich verpflichten muss, diese Vorschriften einzuhalten. Zudem muss sich die private Firma, ebenfalls schriftlich, der Kontrolle durch den Hessischen Datenschutzbeauftragten unterwerfen. Auch an derartigen Regelungen fehlte es.
Die entsprechenden vertraglichen Regelungen werden zurzeit so überarbeitet, dass sie den o. g. Anforderungen genügen.

6.1.2.3 Schlussfolgerung

Um eine belastbare Aussage über die Verhältnisse in hessischen Kommunen treffen zu können, reichen die Prüfungen nicht aus, sie werden deshalb auch im kommenden Jahr fortgesetzt. Die gemachten Prüfungen ergaben als Bild:

- Die Frage, ob die IT einer Kommune datenschutzgerecht betrieben wird und wie die Qualität ist, hängt nicht davon ab, ob ein externer Dienstleister eingeschaltet ist.
- Die vertraglichen Regelungen waren zu verbessern.
- Die Auftragskontrolle, d.h. das Erteilen von Weisungen an den Dienstleister, die Umsetzung und die Dokumentation der Aufgabenerfüllung, wies in der Regel Lücken auf.
- Für Konzepte, Dienstanweisungen, Richtlinien und die Dokumentation ergab sich kein klares Bild. Hier ist es wichtig, dass die Unterlagen geeignet sind, bei Bedarf einem anderen Dienstleister die Möglichkeit zu geben, den Auftrag zu übernehmen. Es darf keine Abhängigkeit von einem Auftragnehmer geben.

6.2 Rechtliche Rahmenbedingungen bei der Erfassung von Unterstützungsunterschriften für Wahlvorschläge bei Kommunalwahlen

Der Gemeindevorstand prüft die Wahlberechtigung von Personen, die einen nicht etablierten Wahlvorschlag unterstützen. Den Tatbestand der Unterschriftsleistung darf die Gemeinde personenbezogen speichern.

Zum wiederholten Mal ist im vergangenen Berichtszeitraum die Frage an mich herangetragen worden, ob die Gemeinden bei der Überprüfung der Wahlberechtigung eines Bürgers, der einen neuen Wahlvorschlag unterstützt, diesen Umstand speichern dürfen. Ein Bürger hatte sich gegen eine derartige Speicherung gewandt und argumentiert, dass damit oppositionelle Bürger diskriminiert würden. Dies trifft jedoch nicht zu.

Grundsätzlich müssen Wahlvorschläge für nicht etablierte Gruppierungen oder Parteien von mindestens zweimal so vielen Wahlberechtigten persönlich und handschriftlich unterzeichnet sein, wie Vertreter zu wählen sind. Dies ist zwingende Voraussetzung für die Zulassung eines Wahlvorschlags zur Wahl.

§ 11 Abs. 4 Satz 1 KWG

Wahlvorschläge von Parteien oder Wählergruppen, die während der vor dem Wahltag laufenden Wahlzeit nicht ununterbrochen mit mindestens einem Abgeordneten oder Vertreter in der zu wählenden Vertretungskörperschaft oder im Landtag

oder aufgrund eines Wahlvorschlags aus dem Lande im Bundestag vertreten waren, müssen außerdem von mindestens zweimal so vielen Wahlberechtigten persönlich und handschriftlich unterzeichnet sein, wie Vertreter zu wählen sind.

Die Unterzeichner eines derartigen Wahlvorschlags müssen im Zeitpunkt der Unterschriftsleistung wahlberechtigt sein. Die Wahlberechtigung ist nachzuweisen (§ 11 Abs. 4 Satz 2 KWG). Die Bescheinigung der Wahlberechtigung erteilt der Gemeindevorstand (§ 13 Abs. 2 Nr. 3 KWG).
Außerdem darf jeder Wahlberechtigte nur einen Wahlvorschlag mit seiner Unterschrift unterstützen (§ 11 Abs. 4 Satz 3 KWG). Der Gemeindevorstand darf also pro Person nur eine Wahlrechtsbescheinigung erteilen.

Es fällt somit in die Prüfungskompetenz der Gemeinde, ob ein Unterschriftsleistender wahlberechtigt ist und ob er tatsächlich nur einen Wahlvorschlag für die anstehende Wahl unterschrieben hat. Um dies ordnungsgemäß tun zu können, muss sie den Tatbestand der Unterschriftsleistung speichern. Allerdings ist die Gemeinde nicht berechtigt, festzuhalten, zur Unterstützung welchen Wahlvorschlags sie dem Wahlberechtigten die Bescheinigung erteilt hat.

§ 23 Abs. 5 Satz 2 KWO

Der Gemeindevorstand darf bei einer Wahl für jeden Wahlberechtigten die Bescheinigung des Wahlrechts nur einmal zu einem Wahlvorschlag erteilen; dabei darf er nicht festhalten, für welchen Wahlvorschlag die erteilte Bescheinigung bestimmt ist.

6.3 Veröffentlichung von personenbezogenen Daten in einer Drucksache für eine Stadtverordnetenversammlung

Zu den Aufgaben der Stadtverordnetenversammlung gehören u.a. die Beschlussfassung über die Angelegenheiten der Kommune sowie die Überwachung der gesamten Verwaltung und der Geschäftsführung des Magistrats. Trotzdem dürfen den Stadtverordneten nur die personenbezogenen Daten übermittelt werden, die zur Durchführung ihrer Aufgaben erforderlich sind, alle übrigen Daten sind vor der Weitergabe unkenntlich zu machen.

Die Fraktion einer hessischen Stadt bat um datenschutzrechtliche Prüfung einer Drucksache. In den Anlagen zu dieser Drucksache wurden die Konditionen einer Kreditfinanzierung sowie der Notarvertrag zum Erbbaurecht für ein großes Bauprojekt den Stadtverordneten übersandt. Hierbei wurden Geburtsdaten der Betroffenen und die Beträge des zu zahlenden Erbbauzinses allen Stadtverordneten und den Magistratsmitgliedern bekannt gegeben. Die Stadtverwaltung hielt die Weitergabe dieser Informationen an die Stadtverordneten für rechtmäßig. Der für das Bauvorhaben geschlossene städtebauliche Vertrag sieht als Vertragsbestandteile zum Nachweis der Realisierungsfähigkeit des Vorhabens ausdrücklich die Vorlage der Finanzierungszusage der Bank sowie eine beglaubigte Abschrift des Erbbaurechtsvertrages vor.

Die Stadtverordneten müssen nach § 50 HGO über Angelegenheiten der Kommune beschließen bzw. die gesamte Verwaltung und die Geschäftsführung des Magistrats überwachen.

§ 50 Abs. 1 und 2 HGO

(1) Die Gemeindevertretung beschließt über die Angelegenheiten der Gemeinde, soweit sich aus diesem Gesetz nichts anderes ergibt. Sie kann die Beschlussfassung über bestimmte Angelegenheiten oder bestimmte Arten von Angelegenheiten auf den Gemeindevorstand oder einen Ausschuss übertragen. Dies gilt jedoch nicht für die in § 51 aufgeführten Angelegenheiten. Die Übertragung bestimmter Arten von Angelegenheiten auf den Gemeindevorstand kann in der Hauptsatzung niedergelegt werden. Die Gemeindevertretung kann Angelegenheiten, deren Beschlussfassung sie auf andere Gemeindeorgane übertragen hat, jederzeit an sich ziehen. Ist die Übertragung in der Hauptsatzung niedergelegt, ist die Vorschrift des § 6 Abs. 2 zu beachten.
(2) Die Gemeindevertretung überwacht die gesamte Verwaltung der Gemeinde und die Geschäftsführung des Gemeindevorstands, insbesondere die Verwendung der Gemeindeeinnahmen. Sie kann zu diesem Zweck in bestimmten Angelegenheiten vom Gemeindevorstand in dessen Amtsräumen Einsicht in die Akten durch einen von ihr gebildeten oder bestimmten Ausschuss fordern; der Ausschuss ist zu bilden oder zu bestimmen, wenn es ein Viertel der Gemeindevertreter oder eine Fraktion verlangt. Gemeindevertreter, die von der Beratung oder Entscheidung einer Angelegenheit ausgeschlossen sind (§ 25), haben kein Akteneinsichtsrecht. Die Überwachung erfolgt unbeschadet von Satz 2 durch Ausübung des Fragerechts zu den Tagesordnungspunkten in den Sitzungen der Gemeindevertretung, durch schriftliche Anfragen und auf Grund eines Beschlusses der Gemeindevertretung durch Übersendung von Ergebnisniederschriften der Sitzungen des Gemeindevorstands an den Vorsitzenden der Gemeindevertretung und die Vorsitzenden der Fraktionen. Der Gemeindevorstand ist verpflichtet, Anfragen der Gemeindevertreter zu beantworten.

Ohne Zweifel gehört hierzu auch der Beschluss zum Abschluss eines Durchführungsvertrags für ein umfangreiches Bauvorhaben und die Erstellung eines Bebauungsplanes für dieses Bauvorhaben. Die Stadtverordneten benötigen daher als Entscheidungsgrundlage über das Bauvorhaben auch den im Durchführungsvertrag aufgeführten Erbbaurechtsvertrag. Allerdings dürfen nach § 11 Abs. 1 HDSG personenbezogene Daten nur dann übermittelt werden, wenn dies für den jeweils damit verbundenen Zweck erforderlich ist.

§ 11 Abs. 1 HDSG

Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Die Erforderlichkeit einer Datenübermittlung muss nur bei einer der beteiligten Stellen vorliegen.

Dies gilt unabhängig davon, ob Empfänger der Daten die Öffentlichkeit oder die Stadtverordneten sind. Für die Entscheidungsfindung der Stadtverordneten sind die Geburtsdaten der Betroffenen sowie die Höhe des zu zahlenden Erbbauzinses irrelevant. Vor der Weitergabe des Erbbaurechtsvertrages hätten diese Daten daher unkenntlich gemacht werden müssen.

Ich habe die Stadt aufgefordert, künftig vor der Übermittlung von personenbezogenen Daten an die Stadtverordnetenversammlung zu prüfen, welche Daten für eine Entscheidungsfindung tatsächlich relevant sind.

6.4 Handyparken

Die Stadt Wiesbaden bietet eine Möglichkeit, mit dem Handy einen Parkschein zu lösen. Ich habe das System rechtlich und technisch geprüft.

6.4.1 Ausgangslage

Als Autofahrer erlebt man es immer wieder. Man ist nicht mit Absicht Falschparker, sondern man hat entweder kein passendes Kleingeld oder sich beim Lösen des Parkscheins bei der Parkdauer verschätzt. Plötzlich steht man ohne gültigen Parkschein da. Die Stadt Wiesbaden bietet seit diesem Jahr das sog. Handyparken an, das für die Nutzer diese Fälle ausschließen soll. Anders als beim Ziehen eines Parkscheins am Automaten erfolgt hier die Abrechnung minutengenau. Die Landeshauptstadt Wiesbaden hat mich bei der Einführung dieses Systems um datenschutzrechtliche Beratung gebeten.

6.4.2 Der Ablauf

6.4.2.1 Technische Vorbereitung

Die Stadt Wiesbaden musste mit dem Betreiber, einer Privatfirma, die das System speziell für die Belange von Kommunen entwickelt hat, viele Vorarbeiten erledigen. Zur Konfiguration des Systems gehörten u.a. die Bewirtschaftungszeiten der Parkzonen und ihrer Tarife, der Text der Benachrichtigungs-SMS an die Teilnehmer und nicht zuletzt eine eins zu eins Zuordnung der einzelnen Parkzone zu einer Telefonnummer. Natürlich mussten auch an den Parkzonen die Hinweisschilder mit den zugehörigen Telefonnummern aufgestellt werden. Außerdem wurden Benutzerkennungen angelegt. Zu Abrechungszwecken können Mitarbeiter der Stadt Wiesbaden auf die Abrechnungsdaten, d.h. die je Parkzone angefallenen Summen der Parkvorgänge, des Betreibers zugreifen. Zur Kontrolle von Parkvorgängen können sich die Überwachungskräfte je Parkzone die Parkvorgänge des Tages anzeigen lassen.

6.4.2.2 Registrierung

Um am Handyparken teilnehmen zu können, muss man registriert sein. Dies kann im Vorhinein über das Internet geschehen oder beim ersten Anruf, wenn der Parker einen Parkschein "lösen" will. Bei jedem Anruf prüft das System, ob die Handynummer bekannt ist. Wenn nicht, kann sich der Parker mit einem Call-Center verbinden lassen, das dann die Registrierung vornimmt. In beiden Fällen werden als Stammdaten

- Name,
- Adresse,
- Bankverbindung (bei einer Internetregistrierung kann auch ein Prepaidkonto angelegt werden),
- Handynummer,
- Kfz-Kennzeichen und
- die E-Mail-Adresse (für Mitteilungen)

erfasst. Ein Teilnehmer kann bis zu zwei Handys und vier Kennzeichen registrieren lassen. Um später auf die Rechnungen zugreifen zu können, erhält der Teilnehmer noch eine Benutzerkennung und ein Passwort. Das Passwort muss bei der ersten Anmeldung geändert werden.

6.4.2.3 Der Parkvorgang

Zum "Lösen" des Parkscheins, ruft der Parker die auf den Schildern für die Parkzone angegebene Telefonnummer an. Dort wird die Handynummer erkannt. Bei mehreren registrierten Kfz muss der Parker noch das richtige Kennzeichen auswählen. Es werden gespeichert:

- die Stadt und Parkzone,
- das Kfz-Kennzeichen,
- der Beginn der Parkzeit - minutengenau -,
- die Handynummer und
- das Parkende, wenn es eine Höchstparkdauer gibt oder der Betrag auf dem Prepaidkonto vorher verbraucht wäre.

Es wird dann eine Bestätigungs-SMS generiert, in der die Daten mitgeteilt werden.

Der Parkvorgang endet, wenn der Parker die Telefonnummer erneut anruft oder die Höchstparkdauer überschritten ist. Das Parkende und die Parkdauer werden - minutengenau - gespeichert sowie die Parkgebühr berechnet und gespeichert. In einer SMS wird insbesondere die Parkgebühr mitgeteilt.

Für jeden Teilnehmer wird am Monatsende eine Abrechnung über die für ihn angefallenen Parkvorgänge und den resultierenden Gesamtbetrag erstellt. Die Abrechnung ist im Internet für ihn abrufbar. Der Betrag wird abgebucht, wenn ein Lastschriftverfahren vorliegt. Bei einem Prepaidkonto sind die Beträge bereits abgezogen, sodass die Abrechnung zur Kontrolle genutzt werden kann.

6.4.2.4 Die Kontrolle der Parkberechtigung

Die Kontrolle der Parkberechtigung erfolgt durch Mitarbeiter des städtischen Ordnungsamtes. Die Mitarbeiter rufen mit einem Handy den Betreiber an, melden sich am System an und erhalten für die ausgewählte Parkzone eine Übersicht der Kfz-Kennzeichen mit gültigem Parkschein und solche mit an diesem Tag beendeten Parkvorgängen. Mit dieser Übersicht kann für ein parkendes Fahrzeug ohne Papierparkschein erkannt werden, ob ein gültiger Handyparkschein vorliegt, ein mittlerweile abgelaufener Handyparkschein vorlag oder ohne Parkschein geparkt wird. Wenn kein gültiger Parkschein vorhanden ist, wird die entsprechende Verwarnung vorgenommen.

6.4.2.5 Die Speicherfristen

Nach den Verträgen werden die mit der Registrierung verbundenen Stammdaten über das Ende der Registrierung hinaus noch sechs Monate gespeichert. Die Parkvorgänge werden über die Abrechnung hinaus 50 Tage vorgehalten, und die Abrechnungen selbst werden nach zwölf Monaten gelöscht.

6.4.2.6 Rechtliche Bewertung

Die rechtlichen Voraussetzungen für eine elektronische Abrechnungslösung beim Parken im öffentlichen Raum hat der Bundesminister für Verkehr, Bau- und Wohnungswesen durch die 11. Ausnahmeverordnung zur StVO vom 28. Januar 2005 geschaffen (BGBl. I, S. 229).

§ 1 der 11. Ausnahmeverordnung zur StVO

Abweichend von § 13 Abs. 1 und 2 der Straßenverkehrsordnung darf ohne Betätigung der dort genannten Einrichtungen zur Überwachung der Parkzeit für die Dauer der zulässigen Parkzeit halten, wer die für die Entrichtung der Parkgebühren und für die Überwachung der Parkzeit durch zusätzlich vorhandene elektronische Vorrichtungen oder Einrichtungen, insbesondere durch Taschenparkuhren oder Mobiltelefone, notwendigen Vorkehrungen getroffen hat. Satz 1 findet keine Anwendung, soweit eine dort genannte elektronische Vorrichtung oder Einrichtung nicht funktionsfähig ist.

Damit wollte der Verordnungsgeber die Erprobung neuer Möglichkeiten der Parkraumbewirtschaftung fördern. Allerdings ist die Regelung bis zum 31. Dezember 2007 befristet. Insoweit ist derzeit das Wiesbadener Handyparkverfahren auch als Pilotprojekt zu sehen. Nähere Vorgaben für die Umsetzung eines derartigen Projekts ergeben sich aus der Verordnung nicht.

Da die Landeshauptstadt Wiesbaden sich zur Realisierung dieses Projekts - wie oben beschrieben - mit einem privaten Dienstleister zusammengeschlossen hat, der für die technische Realisierung und Abwicklung des Zahlungsverkehrs sorgt, stellte sich die Frage nach der rechtlichen Einordnung dieses Lösungsansatzes.

Grundsätzlich tritt der Parker - gleichgültig ob der Bezahlvorgang per Handy oder am Parkscheinautomat abgewickelt wird - in eine Rechtsbeziehung mit der Stadt. Die Stadt hat im Rahmen dieser Aufgabenerfüllung allerdings die Möglichkeit, nach § 4 HDSG sich der Hilfe eines privaten Dienstleisters zu bedienen. Der private Anbieter ist insoweit als unselbständiger Verwaltungshelfer anzusehen, der keine eigenen Entscheidungsbefugnisse besitzt. Verantwortlich für die ordnungsgemäße Verarbeitung der Daten bleibt die Stadt. Die Stadt hat auf Grund dieser rechtlichen Bewertung einen Vertrag über eine Datenverarbeitung im Auftrag nach § 4 HDSG mit dem privaten Anbieter geschlossen, in dem im Einzelnen die Rechte und Pflichten von Auftraggeber und Auftragnehmer geregelt sind. Des Weiteren hat sich der Auftragnehmer vertraglich meiner Kontrolle unterworfen. Von diesem Kontrollrecht habe ich im Berichtszeitraum auch Gebrauch gemacht (s. u. Ziff. 6.4.2.7).

Darüber hinaus habe ich gefordert, dass der Auftragnehmer in seinen allgemeinen Geschäftsbedingungen umfassend über die Datenverarbeitungsabläufe im Zusammenhang mit der Abrechnung informiert, damit die Nutzer des Systems nachvollziehen können, was mit ihren Daten geschieht. Im Übrigen bleibt es selbstverständlich die freie Entscheidung der Parkplatznutzer weiterhin zu parken, ohne personenbezogene Daten zu offenbaren, indem ein Parkschein am Automaten gelöst wird.

6.4.2.7 Prüfung

Ich habe zusammen mit der Stadt Wiesbaden das Verfahren beim Betreiber geprüft. Von den vertraglichen Regelungen waren die Löschfristen nicht umgesetzt. Der private Dienstleister hat mir zugesichert, dass er die erforderlichen Anpassungen innerhalb kurzer Zeit vornehmen wird, sodass das Verfahren dann vertragsgemäß ablaufen wird.

6.5 Übermittlung von Adressdaten trotz Auskunftssperre Probleme der automatisierten Datenverarbeitung beim Wohnungsamt

Die Software eines Wohnungsamtes sieht vor, dass Wohnungssuchende für Wohnungen mit Belegungsrechten der Stadt neben der Telefonnummer auch die genauen Adressdaten des Eigentümers erhalten, unabhängig davon, ob ein Mietvertrag zustande kommt oder nicht. Besonders gravierend wirkt sich dies für Personen aus, die in der Einwohnermeldedatei eine Auskunftssperre wegen Gefährdung ihres Lebens eingetragen haben.

Eine Beschwerdeführerin kaufte eine Wohnung und erfuhr erst später, dass die Stadt noch ein Belegungsrecht für diese Wohnung hat. Da die Wohnung neu zu vermieten war, hatte das Wohnungsamt die Adresse der Eigentümerin an fünf berechtigte Interessenten weitergegeben. Die Beschwerdeführerin hat aufgrund besonderer Gefährdungsgründe im Einwohnermelderegister eine Auskunftssperre nach § 34 Abs. 5 HMG eingetragen, sie fühlte sich durch diese freigiebige Streuung ihrer Adresse besonders gefährdet. Nicht jeder der Interessenten würde einen Mietvertrag erhalten und damit ihre persönliche Adresse benötigen. Sie bat daher um datenschutzrechtliche Prüfung, ob der Umgang des Wohnungsamtes mit ihrer Adresse rechtmäßig ist.

Meine Recherchen ergaben, dass die vom Wohnungsamt eingesetzte Software allen Interessenten einer zu belegenden Wohnung die komplette Adresse und die Telefonnummer der Wohnungseigentümer übermittelt. Der Erforderlichkeitsgrundsatz des § 11 HDSG lässt eine Verarbeitung personenbezogener Daten nur dann zu, wenn es für die Erfüllung der jeweiligen Aufgabe und für den damit verbundenen Zweck erforderlich ist. Wohnungsinteressenten benötigen für die Vereinbarung eines Besichtungstermins ausschließlich die Adresse der zu vermietenden Wohnung sowie die Telefonnummer des Vermieters zur Kontaktaufnahme. Die regelmäßige Übermittlung der Adressdaten des Vermieters durch das Wohnungsamt ist daher unzulässig.

Das Wohnungsamt hat für den im Jahr 2007 geplanten Softwarewechsel die Beschränkung der zu übermittelnden Vermieterdaten auf die Telefonnummer aufgenommen.

Um der Beschwerdeführerin kurzfristig zu helfen, wurde darüber hinaus mit dem Wohnungsamt vereinbart, dass Anfragen zu dieser Wohnung ab sofort manuell ohne Einsatz der Datenverarbeitung behandelt werden und künftig nur noch die Telefonnummer zur Kontaktaufnahme übermittelt wird. Im Übrigen hat die Beschwerdeführerin hierauf nach § 7 Abs. 5 HDSG einen Anspruch, da der Verarbeitung ihrer Daten schutzwürdige, sich aus ihrer besonderen persönlichen Lage ergebende Gründe entgegenstehen.

§ 7 Abs. 5 HDSG

Wenn der Betroffene schriftlich begründet, dass der rechtmäßigen Verarbeitung seiner Daten auf Grund dieses Gesetzes schutzwürdige, sich aus seiner besonderen persönlichen Lage ergebende Gründe entgegenstehen, ist die Verarbeitung nur zulässig, nachdem eine Abwägung im Einzelfall ergeben hat, dass seine Gründe hinter dem öffentlichen Interesse der Verarbeitung zurückstehen müssen. Dem Betroffenen ist das Ergebnis mit Begründung schriftlich mitzuteilen.

6.6 Videoüberwachung im Fuldaer Stadtschloss

Auch eine inaktive Kamera kann menschliches Verhalten beeinflussen. Im Übrigen muss Videoüberwachung für die betroffenen Personen erkennbar sein. Es müssen deshalb Schilder auf eine Überwachung hinweisen.

6.6.1 Kamera im Magistratszimmer

In einer Eingabe wurde ich darüber informiert, dass an der Decke des Magistratssitzungszimmers der Stadt Fulda eine Kamera angebracht sei. Da der Sitzungssaal nicht nur vom Magistrat, sondern auch von anderen Institutionen als Tagungsort genutzt wird, sah ich mich veranlasst, eine sofortige Prüfung vor Ort durch meine Mitarbeiter durchführen zu lassen.

Der Hinweis erwies sich insoweit als korrekt, als tatsächlich unter der Decke eine Kamera angebracht war, die nach den Feststellungen meiner Mitarbeiter an Strom angeschlossen war. Die Informationen vor Ort ergaben folgendes Bild:

Da im Magistrat des Öfteren größere Papiervorlagen (z.B. Bebauungspläne) erörtert würden, sei eine Anlage installiert worden, die mit Hilfe der Kamera an der Decke Papiervorlagen auf dem darunter stehenden Tisch erfassen und mit Hilfe eines Projektors an eine Leinwand vergrößern sollte. Um flexibel auf die Vorlagen reagieren zu können, sei die Kamera mit einer Steuerung verbunden worden, die eine beliebige Ausrichtung des Aufnahmebereiches zugelassen habe. Da die Steuerung hinter der Projektionswand lag, konnte der steuernde Mitarbeiter die Kameraaufnahme anhand eines Monitors verfolgen.
Die Anlage brachte nicht den gewünschten Erfolg. Sie wird nun nicht mehr verwendet.

Die Begehung des Saals ergab, dass das Steuerungspult nicht mehr angeschlossen war. Gleichwohl konnten meine Mitarbeiter feststellen, dass die Kamera nach wie vor in Betrieb war, wie es der Beschwerdeführer beschrieben hatte. Es war deutlich zu erkennen, dass sich die Kamera unter der Rauchglaskuppel ständig drehte. Die Erklärung eines städtischen Mitarbeiters, dies sei auf die Verbindung der Kamera mit dem Projektor zurückzuführen, konnte nicht verifiziert werden. Auch nach Ausschalten des Projektors drehte sich die Kamera weiter. Zudem war der Erfassungsbereich offensichtlich nicht auf den darunter stehenden Tisch, sondern schräg in den Raum gerichtet, so dass es ohne weiteres möglich gewesen wäre, durch die Drehung der Kamera den kompletten Raum zu überwachen.

Obwohl mit dieser Kamera offensichtlich keinerlei Aufnahmen oder Aufzeichnungen mehr gefertigt wurden, habe ich darauf hingewiesen, dass eine Kamera, die sich erkennbar ständig bewegt, geeignet ist, das Verhalten der Nutzer eines solchen Sitzungssaales zu beeinflussen. Wer sich unter ständiger Überwachung sieht, wird sich nicht mehr natürlich verhalten. Im Übrigen wurde uns auch von Seiten des anwesenden städtischen Mitarbeiters bestätigt, dass diese Kamera schon verschiedentlich zu Irritationen und damit verbunden zu Nachfragen geführt habe.

Da das System für die ursprünglich geplante Nutzung nicht mehr in Betrieb war, habe ich gegenüber dem Oberbürgermeister nachdrücklich empfohlen, das System so außer Betrieb zu setzen, dass keine Missverständnisse über vorgebliche Überwachungen mehr auftreten können. Aufgrund meiner Intervention ist die Kamera inzwischen demontiert worden.

6.6.2 Videoüberwachung der historischen Räume des Stadtschlosses

Meine Mitarbeiter haben während ihres Besuches auch die in den historischen Räumen des Stadtschlosses installierten Videokameras in Augenschein genommen. Nach Angaben der städtischen Mitarbeiter erfolgte die Anbringung dieser Kameras zur Sicherung der historischen Räume und der musealen Gegenstände.

Grundsätzlich ist es nach § 14 Abs. 4 Satz 1 Nr. 2 HSOG rechtlich zulässig, zum Schutz besonders gefährdeter öffentlicher Einrichtungen Videokameras zu installieren. Allerdings hat eine derartige Überwachung stets offen zu erfolgen. D.h., die Daten verarbeitende Stelle ist verpflichtet, Besucher auf den Umstand der Videoüberwachung hinzuweisen. Des Weiteren muss die Möglichkeit bestehen, sich über die näheren Einzelheiten der Überwachung informieren zu können.

Hinweise auf eine Videoüberwachung fehlten völlig. Die Mitarbeiter der Stadtverwaltung, die an den Überwachungsmonitoren saßen, konnten über nähere Details keine Auskunft geben, da sie offensichtlich nur unzureichend mit dem neuen System vertraut gemacht worden waren.

Ich habe deshalb gegenüber der Stadt die Erstellung eines Sicherheitskonzepts gefordert, in dem Zugriffsregeln, Speicherdauer (max. zwei Monate nach § 14 Abs. 1 Satz 2 HSOG) und Verwendungszweck geregelt sind. Auch sollten alle mit dem Umgang des Systems betrauten Bediensteten ausführlich geschult werden, damit Bürger auf Nachfrage sachgerecht über die stattfindende Videoüberwachung informiert werden können. Die Mitarbeiter, die an den Monitoren sitzen, sollten auch Fragen zur Speicherdauer beantworten können.

Die Stadt hat in der Zwischenzeit ein Sicherheitskonzept erstellt, in dem die nötigen Festlegungen getroffen wurden. Die erforderlichen Hinweisschilder wurden ebenfalls angebracht. Das Aufsichts- und Kassenpersonal des historischen Stadtschlosses ist mit den Funktionalitäten der Videoüberwachung vertraut gemacht worden. Zur Information der Bürger ist es darüber unterrichtet worden, dass

- die Videoüberwachung ausschließlich dem Schutz der musealen Objekte in den historischen Räumen des Stadtschlosses dient,
- aus Sicherheitsgründen die durch die Kamera erfassten Bilder auf Datenträger aufgezeichnet werden, wobei außer im Falle einer Störung keine Auswertung erfolgt,
- die aufgezeichneten Bilder einen Monat gespeichert und anschließend automatisch gelöscht werden.

7. Sonstige Selbstverwaltungskörperschaften

7.1 Hochschulen

7.1.1 Ergebnis der Überprüfung der Bibliothek der Fachhochschule Fulda

Die Datenverarbeitung der Hochschulbibliotheken ist in Hessen auf einige Hochschulrechenzentren konzentriert; deshalb sind die Anforderungen der Datenverarbeitung im Auftrag zu erfüllen. Bei der Erhebung von Nutzerdaten ist der Aufklärungspflicht nach § 12 HDSG zu genügen – auch wenn die Daten online direkt von den Nutzenden eingegeben werden.

Im Berichtsjahr stattete ich der Bibliothek der Fachhochschule Fulda einen Prüfbesuch ab. Die Datenverarbeitung erfolgte weitgehend datenschutzkonform. Einige rechtliche Besonderheiten in der Gestaltung der Beziehungen der Bibliothek zum Nutzer als auch in der technischen Abwicklung sind jedoch noch nachbesserungswürdig und deshalb erwähnenswert, weil sie vermutlich auch bei anderen Hochschulbibliotheken relevant sind. Insoweit schließt dieser Bericht an entsprechende frühere Tätigkeitsberichtsbeiträge an (vgl. 30. Tätigkeitsbericht, Ziff. 22), wobei sich leider einige Mängel wiederholen.

7.1.2 Auftragsverhältnis mit der Universität Gießen

Die Hochschulbibliothek eröffnet dem Benutzer - auf der Basis einer Satzung - ein Benutzungsverhältnis und ist insoweit als Daten verarbeitende Stelle i. S. v. § 2 Abs. 3 HDSG anzusehen. Denn sie verwaltet seine persönlichen Benutzerdaten.

§ 2 Abs. 3 HDSG

Daten verarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

Dabei stellt sie dem Nutzer entsprechende DV-Geräte zur selbstständigen Eingabe von Daten zur Verfügung oder speichert die Nutzungsdaten mit eigenen Mitarbeitern. Der gesamte automatisierte Datenbestand des eingesetzten Systems auf der Basis von PICA (s. 30. Tätigkeitsbericht, Ziff. 22) wird jedoch vom Rechenzentrum der Universität Gießen DV-technisch betreut, d.h. die Datenbestände liegen ausschließlich dort. Dies erfolgt im Rahmen eines Landeskonzeptes, wonach verschiedene Rechenzentren hessischer Hochschulen jeweils mehrere Hochschulbibliotheken DV-technisch betreuen. Die Universität Gießen hat insoweit die interne Verantwortung der Systembetreuung u.a. gegenüber der Universitätsbibliothek Fulda übernommen. Rechtlich stellt das Verhältnis zwischen beiden Einrichtungen ein Auftragsverhältnis dar i. S. v. § 4 HDSG. § 4 Abs. 2 Satz 2 verlangt allerdings für die diesbezüglichen vertraglichen Absprachen die Schriftform.

§ 4 Abs. 2 HDSG

Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. Für ergänzende Weisungen gilt Satz 2 entsprechend. Der Auftraggeber hat zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen und die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen sowie der in § 7 Abs. 4 genannten Daten eingehalten werden. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse, noch überwiegende schutzwürdige Belange entgegenstehen.

Zudem muss der Vertrag alle in § 4 Abs. 2 erwähnten Punkte enthalten. Im Mittelpunkt stehen dabei die notwendigen technischen und organisatorischen Sicherheitsmaßnahmen. Ich musste leider feststellen, dass Vereinbarungen und Festlegungen in diesem Rahmen weder bekannt noch als schriftlicher Vertrag dokumentiert waren. Besonders problematisch war dieser Missstand deshalb, weil die permanente Verantwortung für die Sicherheit der Datenverarbeitung bei der Fachhochschule Fulda liegt, da sie die Rolle des Auftraggebers hat gegenüber der Universität Gießen. Mir wurde jedoch zugesagt, den notwendigen schriftlichen Vertrag umgehend zu schließen.

7.1.3 Aufklärung nach § 12 Abs. 4 HDSG

In der Phase der Eingabe der Benutzerdaten in das System erhebt und speichert die Bibliothek personenbezogene Daten i. S. v. § 2 Abs. 2 Nr. 1 und 2 HDSG. Dies sind die notwendigen Informationen über die Person des Nutzers und die eigentlichen Ausleihdaten der Bibliothek (u.a. Ausleihdatum).

§ 2 Abs. 2 HDSG

Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener Daten im Sinne der nachfolgenden Vorschriften ist

1. Erheben das Beschaffen von Daten über den Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. ….

Für die Phase der Erhebung verlangt § 12 Abs. 4 HDSG eine Aufklärung des Betroffenen über die dort erwähnten Punkte.

§ 12 Abs. 4 HDSG

Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, dann ist er von der Daten verarbeitenden Stelle in geeigneter Weise über deren Anschrift, den Zweck der Datenerhebung sowie über seine Rechte nach § 8 aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden Daten bei dem Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er auf die Rechtsgrundlage hinzuweisen. Im Übrigen ist er darauf hinzuweisen, dass er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

Diese Aufklärung wird in dem vom Bibliotheksnutzer eigenhändig unterzeichneten Anmeldeformular auch vorgenommen. Daneben besteht jedoch auch die Möglichkeit, sich online über eine Anmeldemaske direkt anzumelden. In dieser Maske fehlte der Text der Aufklärung, wie er in dem Anmeldebogen aufgeführt ist. Ich habe daher angeregt, ihn auch in der Online-Fassung aufzuführen, damit der betroffene Nutzer schon bei der Eingabe seiner Daten über seine Rechte nach § 12 Abs. 4 HDSG aufgeklärt wird.
Inhaltlich war der Aufklärungstext zur Verbesserung der Transparenz der Datenverarbeitung zu ergänzen um den Hinweis, dass die Benutzerdaten nicht an Dritte übermittelt und nur verschlüsselt an das Hochschulrechenzentrum der Universität Gießen weitergegeben werden.
Diese Ergänzungen sagte die Bibliotheksleitung ebenfalls zu.

7.2 Sparkassen

7.2.1 Sparkasse zeichnete rechtswidrig Telefongespräche auf

Eine hessische Sparkasse zeichnete Telefonanrufe von Kunden ohne wirksame Einwilligung der Betroffenen auf.

7.2.1.1 Aufzeichnungsverfahren

Durch eine Reihe von Beschwerden wurde ich darauf aufmerksam gemacht, dass eine Sparkasse dazu übergegangen war, die eingehenden Telefongespräche aufzuzeichnen. Die Überprüfung ergab, dass die Sparkasse ihre zentrale Telefonvermittlungsstelle auf die als Direktbank fungierende Tochtergesellschaft ausgelagert hatte. Dort wurden sämtliche unter der zentralen Rufnummer der Sparkasse eingehenden Telefongespräche aufgezeichnet. Darüber hinaus wurden Anrufe, die bei den Filialstellen eingingen, dort jedoch nicht entgegengenommen wurden, auf die Telefonzentrale der Direktbank umgeleitet und ebenfalls aufgezeichnet. Die Filialen konnten außerdem eingehende Telefonate aktiv auf die Telefonzentrale umleiten. Auch diese Gespräche wurden aufgezeichnet. Pro Monat wurden etwa 60.000 Gespräche aufgezeichnet. In den aufgezeich-

neten Telefonaten ging es in erster Linie um die Vermittlung an den zuständigen Sachbearbeiter oder um Anfragen ohne Bezug zu konkreten Bankgeschäften, z.B. Fragen nach Öffnungszeiten, Formularen oder Zinssätzen. Die Anfragen wurden vom Call-Center der Direktbank unmittelbar beantwortet. Anrufe bei Durchwahlnummern der Sparkasse wurden nicht aufgezeichnet.

Die Gesprächsaufzeichnung wurde den Anrufern mit folgender automatisierter Ansage angekündigt:

"Guten Tag, … Sie sind verbunden mit dem … Kundentelefon. Zu Ihrer eigenen Sicherheit und zur Qualitätssicherung wird das nachfolgende Gespräch aufgezeichnet. Wünschen Sie lediglich eine Gesprächsvermittlung, so endet die Gesprächsaufzeichnung selbstverständlich mit der Übergabe an Ihren Gesprächspartner."

Die Gespräche wurden digital gespeichert. Eine individuelle Abschaltung der Aufzeichnung war weder gesprächsweise noch zeitgesteuert möglich. Dazu fehlten nach Angaben der Sparkasse der Telefonanlage die technischen Voraussetzungen.

Die Gesprächsaufnahmen wurden bis zum Ablauf des dritten Monats nach Quartalsende aufbewahrt. Die Sparkasse begründete dies damit, dass eine kürzere Speicherungsfrist eine ordnungsgemäße Reklamationsbearbeitung unmöglich mache.

Mittels einer Web-Oberfläche konnte ein beschränkter Kreis von Mitarbeitern der Direktbank (drei Personen aus der Bereichsleitung, drei Kommunikationstrainer und der Systemadministrator) auf die gespeicherten Gespräche zugreifen. Die Auswahl erfolgte zunächst aus einem Kalendermenü und in einem zweiten Schritt aus der nach Zeiten geordneten Liste. Neben Datum, Uhrzeit und Dauer des Gesprächs stand noch durch die Kanalnummer der Arbeitsplatz als Suchkriterium zur Verfügung. Auch in den Menüs zur Wiedergabe der Aufzeichnung bzw. zur Ansicht der Anrufdetails wurden keine weiteren Daten abgelegt. Das in den Anrufdetails u.a. vorgesehene Feld Anrufernummer legte allerdings nahe, dass es mit dem System möglich war, weitere Informationen zu verknüpfen und aus der Telefonanlage die Nummer des Anrufers, sofern sie übermittelt wurde, zu übernehmen.

Eine systematische Auswertung der Gespräche (z.B. Anzahl der Gespräche und Gesprächsdauer pro Agent) erfolgte nach Angaben der Sparkasse nicht. Zu Coachingzwecken wurde in einzelne Gespräche hineingehört. Mitarbeiter und Anrufer wurden in diesem Fall auf das Mithören hingewiesen. Der Anrufer hatte die Möglichkeit, das Mithören abzulehnen und aufzulegen. Mit den Mitarbeitern war über das Mithören eine arbeitsvertragliche Regelung getroffen worden.

Der Personalrat der Sparkasse hatte der Gesprächsaufzeichnung zugestimmt.

Die Sparkasse begründete die Gesprächsaufzeichnung folgendermaßen:
- Die Aufzeichnung diene der Vermeidung von Anmachanrufen,
- der Vorsorge bei Drohanrufen,
- solle Unverschämtheiten der Kunden entgegenwirken,
- eine einheitliche Reklamationsbearbeitung ermöglichen,
- ein einheitliches Coaching für die Verbesserung der Gesprächsqualität garantieren.

7.2.1.2 Möglicher Verstoß gegen § 201 Abs. 1 Nr. 1 StGB

Das Aufnehmen des nicht öffentlich gesprochenen Wortes eines anderen auf einen Tonträger ist strafbar, wenn es unbefugt erfolgt (§ 201 Abs. 1 Nr. 1 StGB). Eine Befugnis kann sich aus einem Gesetz oder der Einwilligung der Betroffenen ergeben. Da keine gesetzliche Regelung die Sparkasse zur Aufzeichnung der Gespräche berechtigte, kam als Rechtsgrundlage nur eine wirksame Einwilligung der Anrufer in Betracht. Anders als im Datenschutzrecht verlangt das Strafrecht keine Schriftform für die Einwilligungserklärung. Es genügt außerdem eine stillschweigende, konkludente oder mutmaßliche Einwilligung. Unter diesen Voraussetzungen hätte man angesichts der automatisierten Ansage, die zu Beginn des Telefonats erfolgte, davon ausgehen können, dass ein Anrufer, der danach das Gespräch führte, konkludent in die Aufzeichnung einwilligte. Die Frage konnte jedoch offenbleiben, da die Gesprächsaufzeichnung zumindest die datenschutzrechtlichen Anforderungen nicht erfüllte.

7.2.1.3 Verstoß gegen datenschutzrechtliche Vorschriften

Die Gespräche wurden unter Einsatz von Datenverarbeitungsanlagen verarbeitet, daher war für die Zulässigkeit der Gesprächsaufzeichnungen das Bundesdatenschutzgesetz maßgeblich (§ 3 Abs. 6 HDSG i. V. m. § 1 Abs. 2 Nr. 3 und § 27 Abs. 1 Satz 1 BDSG). Die Erhebung und Verarbeitung personenbezogener Daten ist danach nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder angeordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG).

Das Aufnehmen der Gespräche ließ sich nicht auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG stützen. Die Datenspeicherung war weder zur Erfüllung von Pflichten noch zur Wahrnehmung von Rechten aus einem Vertragsverhältnis zwischen Sparkasse und Anrufer erforderlich. Das wurde besonders daran deutlich, dass nach erfolgreicher Gesprächsvermittlung die Aufzeichnung beendet, das eigentliche bankgeschäftliche Gespräch somit nicht aufgenommen wurde. Auffallend war in diesem Zusammenhang, dass zum Teil relativ banale Inhalte gespeichert wurden, während Telefonate über Bankgeschäfte außerhalb des Telefonbanking nicht aufgenommen wurden. Es bestand auch keine Notwendigkeit für Zwecke vertragsähnlicher Vertrauensverhältnisse die Telefonate mit Anrufern, zu denen noch keine bankvertraglichen Beziehungen bestanden, aufzunehmen.

Die Anforderungen der in § 28 Abs. 1 Satz 1 Nr. 2 BDSG geregelten Zulässigkeitsalternative waren ebenfalls nicht erfüllt. Danach ist die Verarbeitung personenbezogener Daten zur Erfüllung eigener Geschäftszwecke zulässig, soweit sie zur Wah-

rung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt. Die von der Sparkasse angeführten Aufzeichnungszwecke konnten zwar als berechtigte Interessen angesehen werden, ihnen stand jedoch das überwiegende schutzwürdige Interesse der Anrufer, die Gespräche nicht zu speichern, entgegen. Wie nicht zuletzt die Strafbestimmung des § 201 Abs. 1 Nr. 1 StGB zeigt, sieht die Rechtsordnung in dem Aufnehmen nicht öffentlicher Gespräche auf Tonträger einen gravierenden Eingriff in die Privatsphäre der Gesprächspartner. Ein gleichwertiger rechtlicher Schutz existierte für die von der Sparkasse benannten Interessen nicht. Darüber hinaus war zweifelhaft, ob die Aufzeichnung sämtlicher Telefongespräche ein geeignetes und vor allem verhältnismäßiges Mittel war, um Anmache sowie Droh- und Schmähanrufe zu verhindern oder eine einheitliche Reklamationsbearbeitung und eine einheitliche Anleitung der Agenten zu gewährleisten. Den genannten Anrufen hätte sich z.B. durch eine Gesprächsaufzeichnung begegnen lassen, die nach Beendigung des Gesprächs automatisch gelöscht wird, wenn nicht ein Befehl zur Aufbewahrung erfolgt. Warum das praktizierte punktuelle Mithören durch Kommunikationstrainer nicht ausreichen sollte, um eine einheitliche Bearbeitung von Reklamationen und eine einheitliche Anleitung der Agenten zu gewährleisten, vermochte die Sparkasse gleichfalls nicht überzeugend zu begründen.

§ 28 Abs. 1 BDSG

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt …

Als mögliche Rechtsgrundlage für das Aufnehmen der Telefongespräche blieb daher nur die Einwilligung der Anrufer. Davon schien auch die Sparkasse ursprünglich auszugehen, denn andernfalls wäre der automatisierte Hinweis auf die Datenspeicherung überflüssig gewesen. Im Gegensatz zum Strafrecht kennt das Datenschutzrecht jedoch keine konkludente Einwilligung, sondern verlangt grundsätzlich die schriftliche Einwilligung des informierten Betroffenen (§ 4a Abs. 1 BDSG). Dementsprechend werden beim Telefonbanking die Kunden ausführlich schriftlich über den Zweck der Gesprächsaufzeichnung unterrichtet und willigen schriftlich in die Erhebung, Speicherung und Nutzung ihrer Daten ein. Auf die Schriftform kann allerdings verzichtet werden, wenn wegen besonderer Umstände eine andere Form angemessen ist (§ 4a Abs. 1 Satz 3 BDSG). Bei einmaligen telefonischen Kontakten wäre eine schriftliche Einwilligung ein auch den Interessen des Anrufers zuwiderlaufender Formalismus, sodass in diesen Fällen auch eine mündliche Einwilligung in Frage kommt.

Die Einwilligung ist allerdings nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht (§ 4a Abs. 1 Satz 1 BDSG). Daran mangelte es bei der Aufnahme der Telefongespräche durch die Sparkasse. Anrufer hatten nicht die Möglichkeit zu entscheiden, ob ihr Gespräch aufgezeichnet wird oder nicht. Wer mit der Gesprächsaufzeichnung nicht einverstanden war, hatte nur die Wahl, auf telefonische Kontaktaufnahme zu verzichten und sich schriftlich an die Sparkasse zu wenden, persönlich in einer Geschäftsstelle zu erscheinen oder das Kreditinstitut zu wechseln. Telefonische Erreichbarkeit gehört heute zum Grundangebot eines Kreditinstituts und ist für eine Reihe von Bankgeschäften ein unverzichtbares Kommunikationsmittel, das durch Schreiben oder persönliche Vorsprache nicht ersetzbar ist.

Weder von privatrechtlichen noch anderen öffentlich-rechtlichen Kreditinstituten ist bislang bekannt, dass sie ein derartiges Aufzeichnungsverfahren praktizieren. Kunden der Sparkasse, die keine Gesprächsaufzeichnung bei telefonischen Kontakten mit ihrer Bank wünschten, hätten daher zwar zu einem Kreditinstitut, das auf das Aufzeichnen von Telefonaten verzichtet, wechseln können. Für Kunden, die bei der Sparkasse ein Konto unterhielten, wäre dies allerdings mit erheblichem Aufwand verbunden gewesen. Sie hätten bei einem anderen Kreditinstitut ein neues Konto eröffnen müssen, die Bonität wäre möglicherweise nicht dieselbe gewesen, neue EC- und Kreditkarten hätten beantragt und Lastschriftaufträge geändert werden müssen, Aufdrucke auf Briefpapier hätten geändert werden müssen, evtl. einer Vielzahl von Stellen hätte die neue Kontoverbindung mitgeteilt werden müssen. Für Anrufer bestand daher ein die freie Entscheidung beeinträchtigender faktischer Zwang, in die Gesprächsaufzeichnung einzuwilligen.

Der Ansagetext erfüllte die gesetzlichen Informationspflichten der Sparkasse nicht ausreichend. Die für die Datenverarbeitung verantwortliche Stelle muss bei der Erhebung personenbezogener Daten die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festlegen (§ 28 Abs. 1 Satz 2 BDSG). Die Anrufer müssen über die Identität der verantwortlichen Stelle und den Zweck der Erhebung und Verarbeitung informiert werden. Dient die Verarbeitung mehreren Zwecken, muss dies den Betroffenen mitgeteilt werden (§ 4 Abs. 3 Satz 1 Nr. 1 und 2 BDSG). Der Ansagetext erfüllte diese Anforderung nicht. Er verschwieg zum Teil die wahren Verarbeitungszwecke und gab mit dem Hinweis, die Aufzeichnung des Gesprächs diene der Sicherheit des Kunden, einen unzutreffenden, zumindest aber missverständlichen Verarbeitungszweck an. Die in der Stellungnahme der Sparkasse mir gegenüber genannten Zwecke belegten, dass die Aufzeichnung der Vermittlungsgespräche nicht zur Sicherheit des Anrufers, sondern in erster Linie im Interesse der Sparkasse erfolgte, was jedoch dem Kunden nicht mitgeteilt wurde.

Das Aufnehmen der Telefongespräche verstieß außerdem gegen den in § 3a BDSG geregelten Grundsatz der Datenvermeidung und Datensparsamkeit. Gestaltung und Auswahl von Datenverarbeitungssystemen sind an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben und zu verarbeiten. Es waren durchaus Möglichkeiten vorhanden, die von der Sparkasse mit der Aufnahme sämtlicher Telefonate verfolgten Zwecke ohne eine solch umfassende Datenspeicherung zu erreichen.

Schließlich erschien auch die Dauer der Datenspeicherung zu lange. Gespräche, die zu Beginn eines Quartals erfolgten, wurden fast sechs Monate lang gespeichert. Drohanrufe und Beleidigungen sind aber sofort erkennbar, falls in diesen Fällen strafrechtliche Konsequenzen gezogen werden sollen, dürfte dies kurzfristig geschehen. Warum zusätzlich zu der Möglichkeit des Mithörens bei einzelnen Gesprächen die Gespräche zu Ausbildungs- und Anleitungszecken so lange gespeichert werden mussten, konnte die Sparkasse nicht plausibel darlegen.

7.2.1.4 Reaktion der Sparkasse

Auf meine Kritik hin hat die Sparkasse das Aufzeichnen der Telefongespräche eingestellt.

8. Entwicklungen und Empfehlungen im Bereich der Technik und Organisation

8.1 Zentrale DV in der Landesverwaltung

In meinem 33. und 34. Tätigkeitsbericht habe ich Probleme skizziert, die bei einer Zentralisierung der Datenverarbeitung auftreten können. In diesem Jahr habe ich die HZD vor dem Hintergrund geprüft, dass bei ihr als Dienstleister des Landes Hessen für die zentralen Verfahren mögliche Sicherheitslücken weitreichende Konsequenzen haben. Ich musste feststellen, dass einige der von mir befürchteten Schwachstellen aufgetreten sind.

8.1.1 Ausgangslage

Ende 2003 hat die Landesregierung mit ihrem "e-Government Masterplan 2003 - 2008" den Weg beschrieben, wie sie sich die Entwicklung der IT in den nächsten Jahren vorstellt. Ein wesentliches Element war und ist die Zentralisierung wesentlicher Teile der IT bei der HZD. Grundsätzliche datenschutzrechtliche Fragen dazu hatte ich gegenüber der Landesregierung 2004 formuliert; sie finden sich im 33. Tätigkeitsbericht, Ziff. 8. In der Folgezeit kam es dann zu Gesprächen, wie die teils widerstreitenden Anforderungen in den Konzepten berücksichtigt werden können. Wesentliche Ergebnisse habe ich in meinem 34. Tätigkeitsbericht dargestellt.

Konkrete Ziele und Vorgaben für das Hessen Corporate Network 2004 (HCN 2004) mit seiner zentralen Infrastruktur und IT-Architektur wurden in den "Standards der E-Government-Architektur in der Hessischen Landesverwaltung" (Staatsanzeiger für das Land Hessen vom 28. Februar 2005, S. 854 ff.) festgelegt. Sie betrafen das Meta-Verzeichnis, das Active Directory, die E-Mail und die Public-Key-Infrastructure (PKI). In den letzten beiden Jahren wurden große Anstrengungen unternommen, die Vorgaben umzusetzen. Dieses Jahr habe ich Teile der damit verbundenen Datenverarbeitung geprüft.

8.1.2 Wichtige Entscheidungen

Im Staatsanzeiger wurden die technischen Standards zu den genannten Komponenten veröffentlicht.

Die Angaben zum Meta-Verzeichnis entsprachen dem, was mit mir vereinbart wurde. Im 33. Tätigkeitsbericht, Ziff. 8.5 habe ich die aus meiner Sicht wesentlichen Aspekte dargestellt.

Für die PKI wird im Staatsanzeiger der technische Stand des Testsystems beschrieben. Bei den Meldungen, die den PKI-Nutzenden am Bildschirm angezeigt werden, konnten Veränderungen erreicht werden; hier sind aber noch weitere Verbesserungen nötig. Ferner habe ich mehrfach auf das Problem hingewiesen, dass nicht nur die qualifizierte Signatur eine eigene PIN erfordert, sondern dass dies auch für die fortgeschrittene Signatur erforderlich ist, um der Anforderung des § 2 Nr. 2c SigG "mit Mitteln erzeugt (werden), die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann" ohne großen Aufwand zu genügen. Ferner lässt sich mit einer eigenen PIN auch die sog. Warnfunktion der handschriftlichen Unterschrift für die elektronische Signatur umsetzen.

Im letzten Absatz der technischen Spezifikation der PKI wird festgelegt, dass verschlüsselt eingegangene E-Mails und Dokumente nicht dauerhaft verschlüsselt gespeichert werden dürfen. Diese Aussage kann sich nur auf die unveränderte Speicherung einer verschlüsselt eingegangenen E-Mail beziehen. Die Verschlüsselung einer E-Mail kann und soll die Geheimhaltung während des Transports zum Empfänger sicherstellen; sie ist aber für eine dauerhafte Speicherung in einem Dokumentenmanagementsystem (DMS) oder einem Filesystem insofern ungeeignet, als sie beispielsweise verhindert, dass ein Vertreter auf den Inhalt der E-Mail zugreifen kann. Für Dokumente mit hohem Schutzbedarf kann aber selbstverständlich eine dauerhaft verschlüsselte Speicherung erforderlich sein. Um Produkte zu finden, die für eine Gruppenverschlüsselung in ihrem DMS geeignet sind, hat die Landesverwaltung die nötigen Schritte eingeleitet. Den Sachstand beschreibe ich unten (Ziff. 8.1.4).

Die Standards für die E-Mail legen eine zentral betriebene Plattform fest. Solange die PKI noch nicht flächendeckend verfügbar ist, steht den Mitarbeitern der Landesverwaltung noch keine Möglichkeit zur Verschlüsselung von E-Mails zur Verfügung. Bei dieser Sachlage gibt es die technische Möglichkeit für Administratoren der zentralen Plattform, auf alle E-Mails zuzugreifen. Aus diesem Grund habe ich die technische und organisatorische Ausgestaltung geprüft.

Für das Active Directory wurde eine Änderung zu dem Konzept des HCN 2000 vorgenommen. In dem mit mir abgestimmten Konzept des HCN 2000 wurden die – technischen – Zugriffsmöglichkeiten der Organisationsadministratoren des Active Directories "hessen.de" dadurch kontrollierbar, dass ein "6-Augen-Prinzip" eingeführt wurde. Die Rahmenbedingungen habe ich in meinem 31. Tätigkeitsbericht, Ziff. 12.2 beschrieben; über Probleme musste ich im 33. Tätigkeitsbericht, Ziff. 8.3 berichten.

Das Konzept wurde nun dahin gehend abgeändert, dass die bisher in verschiedenen Domänen abgebildeten Teile der Landesverwaltung in die Domäne "itshessen.hessen.de" migrieren sollen. Ausnahmen sind die Polizei und die Justiz, die je ein eigenes Active Directory, einen sog. Forest, betreiben. Durch diese Änderung hat sich die Problematik weitreichender Zugriffsmöglichkeiten des Organisationsadministrators für "hessen.de" auf die Domänenadministratoren der "itshessen"-Domäne verlagert. Ziel der Standardisierung soll eine "Anpassung der IT-Sicherheit an die Anforderungen des BSI-Grundschutzes" sein. Ein auf die neuen Verhältnisse abgestimmtes Sicherheitskonzept lag mir im Herbst 2006 als Entwurf vor. Ob ein für die verschiedenen Zwecke ausreichendes Sicherheitsniveau erreicht wird, muss im Einzelfall geprüft werden. In einem Fall gab es eine Abweichung vom Standard:
Besonders hohe Ansprüche an den Datenschutz und die IT-Sicherheit müssen bei der E-Beihilfe erfüllt werden. In diesem Verfahren werden Daten zu Erkrankungen der Mitarbeiter und andere Sozialdaten verarbeitet, die der Arbeitgeber nicht zur Kenntnis nehmen darf. Als Konsequenz aus den Anforderungen wurde ausnahmsweise akzeptiert, dass abweichend von den Standards auch für E-Beihilfe ein eigener Forest betrieben wird. Dadurch wird es möglich, die Administration für E-Beihilfe technisch, organisatorisch und personell von der Administration anderer Verfahren zu trennen.

8.1.3 Prüfungen

In diesem Jahr habe ich die zentrale E-Mail-Plattform und die Datenverarbeitung für die Justiz in Hünfeld geprüft. An dieser Stelle möchte ich nur auf wenige, wesentliche Punkte eingehen und einige Konsequenzen darstellen.

8.1.3.1 Zentrale E-Mail

Die Situation für die zentrale E-Mail war dadurch geprägt, dass eine Vielzahl von Dienststellen auf die zentrale Plattform umstellte. Ferner sollte für die Administration auf eine neue, sicherere Terminalserver-Architektur umgestellt werden. Insgesamt war die Plattform noch nicht in ihrem Zielzustand.

Bei der Prüfung konnte ich feststellen, dass die E-Mails zwischen Arbeitsplatz und zentralem Server verschlüsselt übertragen wurden. Auf dem Server wurden sie unverschlüsselt gespeichert. Die mit dem Betrieb anfallenden Sende- und Empfangsprotokolle wurden für sieben Tage gespeichert. Sie konnten nach verschiedenen Kriterien ausgewertet werden. Insbesondere konnten mit den Protokollen Fehler lokalisiert werden. Es war allerdings auch möglich, für jedes Postfach die Absender und Empfänger mit Datum und Uhrzeit festzustellen. Eine derartige Auswertung ist nur zulässig, wenn sie zur Fehlersuche erforderlich ist. Sie war für andere Zwecke untersagt.

Die Administration war in einer Abteilung konzentriert. Die aktuellen Zugriffsrechte der Administratoren beinhalteten aber keinen vollständigen Zugriff. Es war möglich die Protokolle einzusehen, aber nicht auf den Inhalt von Postfächern zuzugreifen. Daneben waren die Mitarbeiter auch in der "itshessen"-Domäne als Domänenadministratoren tätig.

Es gab trotzdem eine erhebliche Schwachstelle: Technisch war es möglich, dass sich ein Administrator vollständige Zugriffsrechte für ein Postfach der zentralen E-Mail einträgt. Die Eintragung selbst und ein Zugriff auf das fremde Postfach wurden **nicht** protokolliert. Ein Zugriff auf fremde Postfächer durch Administratoren wäre daher möglich und nicht nachvollziehbar gewesen.

Ich habe daher gefordert, die Protokollierung zu erweitern. Es muss nachvollziehbar sein, wenn sich ein Administrator auf ein fremdes Postfach aufschaltet. Derartige Vorfälle müssen auch zeitnah erkannt werden. Hierfür und für die Information betroffener Personen und Stellen habe ich ein Revisionskonzept gefordert. Es muss gewährleistet sein, dass die im Revisionskonzept vorgesehene Protokollierung und Information tatsächlich implementiert ist. Die Möglichkeit zur Verschlüsselung von E-Mails sollte schnell eingeführt werden, damit die Administratoren brisante Inhalte nicht zur Kenntnis nehmen können.
Im Ergebnis habe ich eine IT-Revision gefordert, die über die zentrale E-Mail-Plattform hinaus die IT überprüft.

Die von mir aufgestellten Forderungen wurden sofort aufgegriffen. Mittlerweile ist eine IT-Revision bei der HZD eingerichtet. Die Protokollierung wurde implementiert.

8.1.3.2 Prüfung in Hünfeld

Die Struktur der DV der Justiz ist in einem Netzkonzept – der Netzbeschreibung – und einem Administrationskonzept beschrieben. In meinem 31. Tätigkeitsbericht, Ziff. 5.1.3 hatte ich die mittlerweile fortgeschriebenen Konzepte dargestellt. Ferner ist in § 5 der Betriebssatzung der HZD die Fachaufsicht der Justiz über die für sie zuständigen Mitarbeiter der HZD ausdrücklich festgelegt. Mit meiner Prüfung wollte ich feststellen, wie die Konzepte umgesetzt sind und wie die Administration im laufenden Betrieb stattfindet.

Zum Zeitpunkt der Prüfung waren wesentliche Teile der Justiz-Infrastruktur von der HZD Hünfeld zur HZD Wiesbaden verlagert. Dies umfasste das Servermanagement und die Verwaltung der Active-Directory-Benutzer und der Exchange-Postfächer. Die Umstellung erfolgte im Rahmen der Lotus-Notes-Ablösung durch die (zentrale) Microsoft-Exchange-Lösung ab Mitte 2005. Es waren auch bereits zwei Active-Directory-Domänencontroller der Justiz-Domäne in Wiesbaden installiert.

Die Aufgaben in Hünfeld beschränkten sich bei der E-Mail auf den Support von Outlook-Problemen. Selbst die verbliebenen administrativen Aufgaben fanden über einen Verwaltungsrechner auf den Systemen in Wiesbaden statt. Die noch gegebene Doppeladministration Wiesbaden/Hünfeld sollte im Rahmen einer Neukonzeption zentral in Wiesbaden stattfinden. Teile der Aufgaben sollten dann im Rahmen einer Rück-Delegation in Hünfeld ausgeführt werden. Das Konzept war aber nicht vorhanden, es wurde noch erstellt.

Als wesentliches Prüfergebnis musste ich feststellen, dass einzelne Mitarbeiter der HZD Wiesbaden sowohl Administratoren in der Justiz-Domäne waren als auch in der "itshessen"-Domäne. Damit verbunden konnten sie sich auf alle Verzeichnisse und die dort gespeicherten Dateien – das galt auch für die persönlichen Verzeichnisse von Richtern – Zugriffsrechte verschaffen.

Die Zuordnung dieser Funktion zu Mitarbeitern der HZD, die nicht der ausschließlichen Fachaufsicht des Justizministers unterliegen, halte ich für bedenklich und kaum vereinbar mit den Prinzipien, die in der "Netzbeschreibung" Version 1 des Projektes "Modernisierung der Justiz" formuliert waren. Denn mit diesen Prinzipien sollten die sich aus der Gewaltenteilung ergebenden Anforderungen umgesetzt werden. Auf dieser Grundlage wird auch über die weitere Entwicklung des "Justiznetzes" beraten. Da Vertreter der HZD die Netzbeschreibung wesentlich mitgestaltet hatten, musste der HZD der Widerspruch bekannt sein.
Ich habe mein Befremden über diese Umstellung ausgedrückt. Zumindest hätte ich im Rahmen des § 29 Abs. 3 HDSG über solch wesentliche Änderungen informiert werden müssen.

Für die zentrale E-Mail galten die gleichen Feststellungen wie ich sie unter Ziff. 8.1.3.1 beschrieben habe.

8.1.4 Sachstand zur Verschlüsselung

Im letzten Tätigkeitsbericht hatte ich berichtet, dass für das Dokumentenmanagementsystem und andere zentrale Verfahren nach einer Möglichkeit gesucht wird, die Kenntnisnahme durch Administratoren zu verhindern. Die ins Auge gefasste Lösung war eine verschlüsselte Ablage von Dokumenten und Dateien.

Mittlerweile wurde durch das Fraunhofer-SIT eine Marktrecherche durchgeführt. Auf Basis dieser Recherche hat es Präsentationen durch Hersteller gegeben. Da viele technische Details geklärt werden mussten, waren in einigen Punkten Gespräche zwischen den Anbietern des Dokumentenmanagementsystems und der Verschlüsselungsprodukte erforderlich, um die Machbarkeit technischer Ansätze beurteilen zu können. Im Ergebnis sollen jetzt zwei Anbieter konkrete Angebote vorlegen. Es wird dann ein Test und ein Pilotbetrieb folgen.

8.1.5 Sachstand Terminalserver

Im Februar 2004 hatte ich einen Fragenkatalog zur Zentralisierung der IT und der Einführung einer Terminalserver-Architektur erstellt und dem HMDIS mit der Bitte zugeleitet, die Fragen zu beantworten. Da es Fragen waren, die auch laufende Projekte betrafen, gab es keine Antwort des HMDIS, die alle Fragen abschließend beantwortet hätte. In diesem Jahr habe ich zusammen mit dem HMDIS festgelegt, in welchen Projekten und mit welchen Aktivitäten die noch offenen Fragen weiter behandelt werden. Dies waren:

- innerhalb des Projekts DOMEA die Zugriffsschutzmechanismen des DMS und die Schnittstelle zur PKI,
- bei den gemeinsamen Aktivitäten zur Gruppenverschlüsselung der Schutz gegen unbefugte Kenntnisnahme durch Administratoren bzw. den Betreiber,
- in der Projektgruppe Archivierung das Thema Revisionssicherheit und Übersignatur,
- im Projekt PKI Fragen zur Signatur und der Schnittstellen zu anderen Verfahren.

Die beteiligten Personen waren sich einig, dass die Erstellung einer qualifizierten elektronischen Signatur im Terminalserverumfeld grundsätzlich technisch möglich ist, da eine Lösung in diesem Umfeld, das Produkt GERVA, nach dem SigG geprüft und bestätigt wurde. Offen blieb die Frage, welches nach dem Signaturgesetz geprüfte und bestätigte Produkt hierfür zukünftig in der Landesverwaltung genutzt wird und welche durch den Betreiber zu erfüllenden Anforderungen damit verbunden sind.
Das Thema Einbindung der (qualifizierten bzw. fortgeschrittenen) Signatur in DOMEA und in Fachverfahren wird nach Beendigung der Ausschreibung zur Signatursoftware weiter behandelt. Dazu wird das HMDIS den HDSB bei Beendigung der Ausschreibung informieren und die weiteren Aktivitäten werden gemeinsam abhängig vom Ergebnis der Ausschreibung festgelegt.

8.2 Einsatz zentraler Spam-Filter in der Landesverwaltung

In Dienststellen, in denen die private E-Mail-Nutzung zugelassen ist, bedürfen Anti-Spam-Maßnahmen wie SPF und Greylisting der Einwilligung der Beschäftigten.

Die HZD, die für die Landesbehörden den zentralen Internetzugang bereitstellt, hat mich im Sommer des Berichtsjahres um Beratung bei der Einführung von Anti-Spam-Maßnahmen gebeten.

Hintergrund ist die laut HZD stark zunehmende Belastung der Mail-Relay-Systeme am Internet-Übergang des Landes Hessen durch Spam-Mail. Die HZD befürchtet bei einem weiteren Anwachsen der Spam-Mail erhebliche Betriebsstörungen im Mail-Transport von und zur Domäne .hessen.de und bei einem massiven Spam-Angriff sogar den Ausfall des gesamten E-Mail-Dienstes. Sie möchte daher an den externen E-Mail-Gateways zum Internet Anti-Spam-Maßnahmen treffen.

8.2.1 Anti-Spam-Maßnahmen

Im Zentrum der Überlegungen der HZD stehen die Anti-Spam-Maßnahmen SPF (Sender Policy Framework) und Greylisting.

Sender Policy Framework ist eine Abwehrmaßnahme, mit der das Fälschen des Absenders erschwert werden soll. Dabei wird über das Domain-Name-System (DNS) geprüft, ob der Domänen-Anteil der Absenderadresse und der absendende Mail-Server zusammenpassen. E-Mails, die diese Anforderung nicht erfüllen, wurden sehr wahrscheinlich mit einer gefälschten Absenderadresse versandt und sind wahrscheinlich Spam-Mails oder andere Schad-Mails. Sie werden daher vom System unterdrückt.

Beim Greylisting weist der Mailserver des Empfängers eine eingehende E-Mail mit einer temporären Fehlermeldung versehen zunächst zurück. Gleichzeitig vermerkt er in einer Datenbank Absenderadresse, Empfängeradresse und IP-Adresse des absendenden Rechners und versieht den Eintrag mit einem Zeitstempel und einer Gültigkeitsdauer. Auf die temporäre Zurückweisung reagiert der Mailserver des Absenders innerhalb eines definierten Zeitraumes mit einem erneuten Zustellversuch. Geht dieselbe E-Mail innerhalb der in der Datenbank des Mailservers des Empfängers eingetragenen Gültigkeitsdauer erneut ein, wird sie nunmehr dem Empfänger zugestellt. Die Eintragung in der Datenbank wird dann als "zulässige Kommunikationsbeziehung" markiert und mit einem Gültigkeitsstempel/Ablaufdatum versehen. Während dieser Zeit werden E-Mails mit den gleichen Merkmalen als zulässig angesehen und ohne Zeitverzögerung zugestellt. Dabei wird der Gültigkeitszeitraum jeweils verlängert. Eine Zeitverzögerung tritt also nur am Beginn der Kommunikationsbeziehung auf. Da Spam-Software in der Regel nach einer temporären Zurückweisung keinen erneuten Zustellungsversuch veranlasst, kann auf diese Weise Spam-Mail abgewehrt werden.

8.2.2 Private Nutzung des E-Mail-Dienstes

Die HZD geht bei der Einführung zentraler Anti-Spam-Maßnahmen davon aus, dass auch künftig in vielen Dienststellen des Landes die private Nutzung des E-Mail-Dienstes zulässig sein wird. Da die Dienststelle, wenn sie den Beschäftigten die private E-Mail-Nutzung gestattet, zum Anbieter eines Telekommunikationsdienstes und Teledienstes wird (letzteres ist umstritten), muss sie das Fernmeldegeheimnis beachten (§ 88 TKG). Im Verhältnis zu den Beschäftigten sind die Dienststellen und nicht die HZD Diensteanbieter. Die HZD wird im Auftrag der Dienststellen tätig. Die Dienststelle muss daher die straf-, vertrags- und datenschutzrechtlichen Pflichten eines TK-Diensteanbieters beachten.

Unzulässige Eingriffe in das Fernmeldegeheimnis können für die Dienststellenleitung und die den Eingriff ausführenden Mitarbeiter strafrechtliche Konsequenzen haben. Der Einsatz von SPF und Greylisting, die beide die Funktion haben, unerwünschte E-Mails zu blockieren bevor sie die Mailbox des Empfängers erreichen, könnte wegen unbefugten Unterdrückens einer dem Diensteanbieter zur Übermittlung anvertrauten Sendung nach § 206 Abs. 2 Nr. 2 StGB strafbar sein. Außerdem kommt eine Strafbarkeit wegen Datenunterdrückung (§ 303a StGB) in Betracht.

§ 88 TKG

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. …

§ 206 StGB

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigten eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt … 2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt …

§ 303a Abs. 1 StGB

Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

8.2.3 Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB

In der juristischen Literatur ist umstritten, unter welchen Voraussetzungen bei der Versendung einer E-Mail von einem Unterdrücken einer zur Übermittlung anvertrauten Sendung nach § 206 Abs. 2 Nr. 2 StGB auszugehen ist. Es wird die Auffassung vertreten, dass die E-Mail erst dann zur Übermittlung anvertraut sei, wenn Kopfzeile und Inhalt der E-Mail (header und body), also die komplette E-Mail, auf dem Mailserver des Empfängers eingegangen seien. Das Blockieren einer E-Mail vor der Data-Phase kann nach dieser Ansicht nicht den Tatbestand des § 206 Abs. 2 Nr. 2 StGB erfüllen, da beim Diensteanbieter des Empfängers keine E-Mail eingegangen ist, die er unterdrücken könnte.

Dagegen lässt sich einwenden, dass das Fernmeldegeheimnis nicht nur den Inhalt, sondern auch die näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, schützt. Auch die näheren Umstände erfolgloser Verbindungsversuche unterliegen dem Fernmeldegeheimnis. Um die IP-Adresse zu extrahieren, muss der Mailserver des Empfängers in die Kopfzeile der Mail schauen. Ist bereits ein Teil der E-Mail beim Empfängerserver eingegangen (Absender,

Empfänger, IP-Adresse) kommt tatbestandlich die Unterdrückung einer anvertrauten Sendung in Betracht. Sowohl SPF als auch das Greylisting-Verfahren könnten demnach den Tatbestand des § 206 Abs. 2 Nr. 2 StGB erfüllen.
Die Strafbarkeit ist jedoch nur dann gegeben, wenn das Instrument unbefugt eingesetzt wird. Eine Befugnis kann entweder aus einem Gesetz oder aus der Einwilligung des Adressaten resultieren. Mangels einer gesetzlichen Befugnis kann das strafrechtliche Risiko nur durch Einwilligung der Beschäftigten ausgeschlossen werden. Die Einwilligung muss ausdrücklich erklärt werden. Eine mutmaßliche Einwilligung kann beim Filtern von Spam nicht unterstellt werden, da zum einen die Einschätzung, was als Spam zu betrachten ist, subjektiv geprägt ist und zum anderen nicht auszuschließen ist, dass einzelne Empfänger durchaus an der einen oder anderen Art von Junk-Mail interessiert sind. Ob eine Dienstvereinbarung eine ausreichende Rechtsgrundlage sein kann, ist strittig. Zur Sicherheit sollte eine individuelle Einwilligung eingeholt werden.

8.2.4 Strafbarkeit nach § 303a StGB

Der Einsatz von SPF und Greylisting könnte außerdem nach § 303a StGB strafbar sein. Nach dieser Vorschrift macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Auch hierzu wird in der juristischen Literatur zum Teil die Meinung vertreten, dass Daten erst unterdrückt werden können, wenn sich der Inhalt der E-Mail in der Mailbox des Empfängers befindet. Da dies weder bei SPF noch beim Greylisting der Fall ist, wäre demnach eine Strafbarkeit nach § 303a StGB ausgeschlossen. Wie zu § 206 StGB könnte man allerdings auch zu der Auffassung gelangen, dass der Tatbestand der Datenunterdrückung bereits dann erfüllt ist, wenn nur Teile der E-Mail ohne Einwilligung des Empfängers unterdrückt werden.

Gerichtsurteile, die in der Frage der Strafbarkeit des Blockierens von E-Mails Rechtsklarheit schaffen könnten, gibt es bislang nicht.

8.2.5 Notfall

Nicht umstritten ist, dass das Blockieren unerwünschter E-Mails zulässig ist, wenn es zur Abwehr von akuten Angriffen, welche die Funktionsfähigkeit des IT-Systems der Dienststelle erheblich beeinträchtigen, notwendig ist. In diesem Fall könnte ein rechtfertigender Notstand (§ 34 StGB) die Strafbarkeit ausschließen (vgl. auch OLG Karlsruhe, Beschluss vom 10. Januar 2005, Az.: 1 Ws 152/04). Ist der Notfall vorüber, müssten die Filtermaßnahmen allerdings eingestellt werden.

8.2.6 Datenbank beim Greylisting

Die beim Greylisting erforderliche Datenbank könnte gegen § 96 Abs. 2 TKG verstoßen. Danach sind Verkehrsdaten in der Regel nach Beendigung der Verbindung zu löschen. Bei den Angaben Absender, Empfänger und IP-Adresse handelt es sich um Verkehrsdaten i. S. v. § 3 Nr. 33 TKG, denn es sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben und verarbeitet werden. Nach § 96 Abs. 2 Satz 1 i. V. m. § 100 Abs. 1 TKG dürfen Verkehrsdaten über das Ende der Verbindung hinaus gespeichert werden, soweit dies für das Erkennen, Eingrenzen und Beseitigen von Störungen und Fehlern an der Telekommunikationsanlage erforderlich ist. Soweit das Greylisting für diese Zwecke erforderlich ist, dürfen die Daten auch ohne Einwilligung des Empfängers in die Datenbank aufgenommen werden.

§ 109 Abs. 2 TKG, der den Betreiber von TK-Anlagen verpflichtet, bei den Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen der Telekommunikationsnetze führen, und gegen äußerliche Angriffe zu treffen, bietet keine Rechtsgrundlage für die Datenbank, da diese Vorschrift nur für Diensteanbieter gilt, die TK-Dienste für die Öffentlichkeit erbringen. Letzteres trifft auf Dienststellen, welche lediglich ihren Beschäftigten die private E-Mail-Nutzung erlauben, jedoch nicht zu.

Die Dienststelle wäre nach § 93 Satz 2 TKG verpflichtet, die Beschäftigten über die Datenbank zu informieren.
Da die Datenbank geeignet ist, Nutzerprofile zu bilden, was das TKG gerade verhindern will (§ 96 TKG), ist es notwendig, entweder die Empfängeradressen und die Absenderadressen einschließlich der IP-Adresse des absendenden Mailservers getrennt zu speichern und/oder die Absender- und Empfängeradressen nicht im Klartext, sondern lediglich als Hashwert zu speichern und/oder die Speicherung der erlaubten Kommunikationsverbindungen auf ein Minimum zu reduzieren, indem vertrauenswürdige Partner zum Beispiel auf einer White-List genannt werden.

Darüber hinaus muss sichergestellt werden, dass die in der Datenbank enthaltenen Daten nicht für andere Zwecke, insbesondere nicht zur Verhaltens- und Leistungskontrolle verwendet werden (§ 13 Abs. 5 HDSG).

8.2.7 Ausgehende E-Mail

Ist die private E-Mail-Nutzung erlaubt, so ist das Filtern ausgehender E-Mails ohne Einwilligung der Beschäftigten ebenfalls nach § 206 Abs. 2 Nr. 2 StGB und § 303a StGB strafbar. Darauf weist das OLG Karlsruhe (a. a. O.) ausdrücklich hin. In dem der Entscheidung des Gerichts zugrunde liegenden Fall hatte eine Hochschule nicht nur die eingehenden E-Mails eines ehemaligen wissenschaftlichen Mitarbeiters ausgefiltert, sodass sie die Empfänger nicht erreichten, sondern auch die von Mitarbeitern der Fakultät an den ehemaligen Beschäftigten gerichteten E-Mails.

8.3 Dokumentenmanagementsysteme in der öffentlichen Verwaltung

Die Erfahrungen mit den datenschutzrechtlichen Anforderungen bei der Einführung eines Dokumentenmanagementsystems in der Hessischen Landesverwaltung habe ich in eine Arbeitgruppe der Datenschutzbeauftragten des Bundes und der Länder eingebracht. Unter meiner Federführung wurde dazu eine Orientierungshilfe erarbeitet.

8.3.1 Dokumentenmanagementsystem in der Hessischen Landesverwaltung

In Dokumentenmanagementsystemen können personenbezogene Daten ganz unterschiedlicher Sensitivität – z.B. Adressdaten für Verteiler allgemeiner Informationen bis hin zu Gesundheitsdaten – enthalten sein. Die Einführung solcher Systeme muss deshalb sorgfältig geplant und datenschutzgerecht ausgerichtet werden. Wie bereits in meinem 34. Tätigkeitsbericht unter Ziff. 8.2 berichtet, habe ich die Einführung eines einheitlichen Dokumentenmanagementsystems in der Hessischen Landesverwaltung datenschutzrechtlich begleitet. Wesentliche Datenschutzaspekte sind in die Muster für die Vorabkontrolle für den Einsatz von DOMEA in den beiden Stufen

- **Stufe 1**: Umstellung der Poststellen und Registraturen,
- **Stufe 2**: Sachbearbeitung

jeweils eingearbeitet worden. Diese Muster enthalten die generellen Vorgaben und die von den Ressorts zu ergänzenden Angaben, die jeweils in die Schlussbewertung einzubeziehen sind. Sie geben für die Daten verarbeitenden Stellen den Rahmen, überlassen es ihnen aber, die bei ihnen jeweils zu bewertenden Gefahren und die Gegenmaßnahmen detailliert im Rahmen ihrer eigenen Ergänzung zu beschreiben. Außerdem müssen die Ressorts, soweit die einzelnen Einführungsschritte die dort vorhandene IT-Sicherheitsstruktur verändern, ihr eigenes nach § 10 Abs. 2 HDSG und Nr. 5.2 der IT-Sicherheitsleitlinie notwendiges Sicherheitskonzept fortschreiben. Diese Mustervorabkontrolle war für die Ministerien hilfreich. Auf ihrer Basis haben bereits HMDF, HMWVL, HSM, HMWK und HKM für den Einsatz in ihren Häusern angepasste Vorabkontrollen erstellt.

8.3.2 Orientierungshilfe Datenschutz bei Dokumentenmanagementsystemen

Die bei der Beratung der Landesverwaltung gewonnenen Erkenntnisse habe ich in eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eingebracht, in der unter meiner Federführung eine umfangreiche Orientierungshilfe für den datenschutzgerechten Einsatz von Dokumentenmanagementsystemen erarbeitet wurde. Die Orientierungshilfe ist von der Konferenz verabschiedet worden, sodass sie im Bund und allen Bundesländern zur Verfügung steht. In ihr werden nach einer Einführung und Begriffsdefinitionen

- Datenschutzaspekte der möglichen Datenhaltungsmodelle,
- organisatorische Rahmenbedingungen für Einführung und Einsatz,
- rechtliche Anforderungen und Vorüberlegungen,
- Sicherheitsziele und -maßnahmen bei der Behandlung von Dokumenten,
- Anforderungen an das Signieren in einem Dokumentenmanagementsystem,
- technische Maßnahmen gegen unbefugte Kenntnisnahme,
- Datenschutzaspekte bei der Übernahme eingehender Post in das Dokumentenmanagementsystem sowie
- beim Workflowmanagement und
- bei der Recherche

erläutert.

Zur Erleichterung des Verständnisses enthält die Orientierungshilfe für die - insbesondere auch für Personalvertretungen – wichtige Frage der Zweckbindung und damit der zulässigen **Auswertungen von Protokolldaten und Verfahrensdaten** eine tabellarische Aufstellung. Für die mit der Einführung eines Dokumentenmanagementsystems befassten Personen sind die wichtigsten Stationen und erforderlichen Festlegungen in diesem Prozess in einer **Checkliste** zusammengefasst, die jeweils einen Verweis auf die entsprechenden Kapitel in der Orientierungshilfe enthält.

Die Orientierungshilfe "Datenschutz bei Dokumentenmanagementsystemen" ist auf meiner Homepage veröffentlicht (www.datenschutz.hessen.de/o-hilfen/DSimDokumanagement.pdf). Sie ist auch als Broschüre bei mir erhältlich.

9. Bilanz

9.1 Videoüberwachung an der Konstablerwache in Frankfurt (34. Tätigkeitsbericht, Ziff. 5.3.1)

Noch immer nicht wirklich zufriedenstellend gelöst ist die Situation der Videoüberwachung in Frankfurt an der Konstablerwache. Dort hatten meine Bediensteten bei einer Prüfung festgestellt, dass der überwachte Bereich über den als solchen gekennzeichneten Platz hinausging und auch eine nicht ganz unerhebliche Anzahl von Fenstern und Balkonen im Aufnahmebereich der Kameras lagen. Dies ließ sich laut den Auskünften des Polizeipräsidiums Frankfurt nur schwierig bei den bestehenden Kameras abstellen, dafür sei ein hoher tatsächlicher und finanzieller Aufwand notwendig.

Deswegen wurde bei einer Besprechung im Frühjahr für eine Übergangszeit vereinbart, dass versucht wird, die technischen Möglichkeiten der Kameras zum Ausblenden soweit wie möglich auszunutzen und darüber hinaus in der Dienstanweisung nochmals ausdrücklich darauf hinzuweisen, dass für die entsprechenden Bereiche die Zoomfunktion der Kameras nicht zum Einsatz kommen kann.

Darüber hinaus sollte ein Konzept vorgelegt werden, wie mittelfristig eine technische Lösung - ggf. auch durch die Beschaffung neuer Kameras - gefunden werden kann. Dieses liegt mir allerdings bis heute nicht vor.

Gleichzeitig möchte ich schon jetzt darauf hinweisen, dass bei einer Ausstattung mit neuen Kameras die Gelegenheit genutzt werden sollte, zu überprüfen, ob für den gesamten derzeit überwachten Bereich die Erforderlichkeit der Maßnahme (noch) gegeben ist.

9.2 Sachstand zur korrekten Umsetzung der Löschung von auszusondernden Datenspeicherungen der Polizei (34. Tätigkeitsbericht, Ziff. 5.3.2)

Im 34. Tätigkeitsbericht hatte ich unter Ziff. 5.3.2 über das Verfahren und das Konzept der hessischen Polizei zur Löschung von personenbezogenen Daten nach Abschluss eines Verfahrens und Ablauf der verfügten Aufbewahrungsdauer berichtet. Eine Datenschutzprüfung hatte Unstimmigkeiten und technische Mängel in der praktischen Umsetzung des Konzeptes offenbart.

Das HMDIS hat mir mitgeteilt, dass es zu den von mir aufgezeigten Mängeln das Präsidium für Technik, Logistik und Verwaltung zur Stellungnahme und Vorlage von Lösungsvorschlägen aufgefordert habe. Dabei habe es deutlich gemacht, dass den Fehlern mit größtem Nachdruck und höchster Priorität nachzugehen ist.

In der Stellungnahme der Landesregierung zu dem Bericht wurde ergänzend ausgeführt, dass ein eigens eingerichteter Workshop fachliche Vorgaben an das Aussonderungsprüfverfahren festgelegt habe, damit den gesetzlichen Anforderungen Rechnung getragen werde. Derzeit werde im INPOL-Land-Polas Competence Center die Umsetzung geprüft. Hinsichtlich der Fälle, in denen das BKA aus Hessen stammende löschungsreife Datensätze nicht löschte, sei eine Bund-Länder-Kommission mit den unterschiedlichen Laufzeiten von Aussonderungsprüffristen in den Ländern und ihren Wirkungen auf das Gesamtsystem INPOL befasst. Ein Vorschlag sei erarbeitet, müsse aber noch abgestimmt werden.
Der Innenausschuss des Hessischen Landtages hat im Oktober 2006 diesen Sachstand zur Kenntnis genommen. Das Plenum des Hessischen Landtages hat sich bis zum Redaktionsschluss dieses Berichtes noch nicht abschließend mit dem vorigen Bericht befasst.

Zusammenfassend ist festzuhalten, dass die in meinem 34. Tätigkeitsbericht (Ziff. 5.3.2) beschriebenen Mängel und Unzulänglichkeiten nach wie vor vorhanden sind.

9.3 Liegenschaftsdatenabruf (34. Tätigkeitsbericht, Ziff. 6.2)

Im 34. Tätigkeitsbericht hatte ich unter Ziff. 6.2 die unzureichende Umsetzung der Vorgaben des Hessischen Landesamtes für Bodenforschung und Geoinformationen beim automatisierten Abruf von Daten aus dem Liegenschaftskataster moniert. Wie angekündigt, haben meine Mitarbeiter bei den im Jahr 2005 kontrollierten Stellen nachgeprüft, ob diese inzwischen die einzelnen Abrufe aus dem Liegenschaftskataster wie vorgeschrieben dokumentieren. Die Dokumentation dient der Überprüfbarkeit des berechtigten Interesses zum Abruf personenbezogener Daten aus dem Liegenschaftskataster; denn nur bei einem berechtigten Interesse des Abrufenden ist der Zugriff rechtlich zulässig (§ 16 Abs. 2 HVG).
Die Überprüfung ergab, dass die im Jahr 2005 geprüften Stellen nunmehr die Vorgaben des Hessischen Landesamtes für Bodenforschung und Geoinformationen erfüllen und ihrer Dokumentationsverpflichtung in dem erforderlichen Maße nachkommen.

9.4 Hartz IV - Vorlage von Kontoauszügen (34. Tätigkeitsbericht, Ziff. 5.9.1)

Im 34. Tätigkeitsbericht hatte ich ausgeführt, dass das behördliche Verlangen, Kontoauszüge der letzten drei bis sechs Monate vorzulegen, als bisher auch schon im Sozialhilferecht übliche Standardmaßnahme bei der Entscheidung über die Gewährung von Arbeitslosengeld II zulässig ist.

Mittlerweile hat sich das Landessozialgericht Sachsen mit Beschluss vom 25. April 2006 (Az.: L 3 B 93106 AS-ER) meiner Rechtsposition ebenfalls unter expliziter Ablehnung der Rechtsansicht des Hessischen Landessozialgerichts angeschlossen. Zutreffend betont das Landessozialgericht Sachsen: "Es besteht auch insoweit ein Vorrang des öffentlichen Interesses an der Feststellung des wahren Sachverhalts vor dem Interesse der Beschwerdeführerin (Bf.) an einem Unterbleiben eines Eingriffs in ihr als Grundrecht geschütztes Recht auf informationelle Selbstbestimmung. Handelt es sich doch bei Leistungen nach dem SBG II um die Auszahlung erheblicher Beträge aus vom Steuerzahler aufgebrachten Mitteln. Hinter diesem Interesse hat das Recht der Bf., ihre Kontobewegungen nicht preiszugeben, zurückzutreten. Wer wegen Bedürftigkeit Geld will, das alle Steuerzahler aufbringen müssen, muss seine Bedürftigkeit nachweisen und daher darauf verzichten, seine wirtschaftlichen Verhältnisse, die sich gerade in den Kontobewegungen widerspiegeln, vor dem Leistungsträger zu verbergen."

Inzwischen sind denn auch Eingaben an meine Behörde, die sich gegen die Vorlage von Kontoauszügen im Rahmen der Grundsicherung für Arbeitsuchende richten, deutlich zurückgegangen.

9.5 Schuleingangsuntersuchung durch die Gesundheitsämter (34. Tätigkeitsbericht, Ziff. 5.8.5)

Meine im vergangenen Berichtsjahr geäußerte Kritik zum Umfang der Datenerhebung durch die Gesundheitsämter im Zusammenhang mit der Schuleingangsuntersuchung hat dazu geführt, dass sich eine Arbeitsgruppe der hessischen Schulärzte mit dem Thema befasst hat und nach internen Diskussionen mit dem Entwurf eines landeseinheitlichen Anamnesebogens an mich herangetreten ist.

Dieser Bogen, der zusammen mit der Einladung zum Untersuchungstermin im Gesundheitsamt an die betroffenen Eltern der schulpflichtigen Kinder verschickt wird, beinhaltet nun die wesentlichen, aus ärztlicher Sicht notwendigen Fragestellungen zur Gesundheitsvorgeschichte des Kindes. Neben den personenbezogenen Angaben des Kindes sowie seiner Eltern werden

künftig nur noch wenige, medizinische Daten erfragt, die sich für die Beurteilung der Schulfähigkeit des Kindes auf den notwendigen Umfang beschränken.

Für besonders begrüßenswert halte ich das Vorhaben, den Bogen in allen Gesundheitsämtern Hessens zu nutzen. Damit ist ein landeseinheitliches Verfahren im Zusammenhang mit der Datenerhebung und Nutzung der Informationen durch die zuständigen Fachbereiche der öffentlichen Gesundheitsämter gewährleistet.

In den Bogen aufgenommen ist eine Information über die Art der Datenverarbeitung bei den Gesundheitsämtern, deren Rechtsgrundlagen sowie die Informationsrechte der Eltern, an deren Formulierung meine Dienststelle maßgeblich beteiligt war und die in wenigen Sätzen auf verständliche Weise den Sachverhalt darstellt.

Keine rechtlichen Bedenken habe ich, die Eltern zum Ausfüllen des Fragebogens zu verpflichten. Nach § 71 Abs. 2 des HSchulG haben Kinder und Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler die für die Untersuchung erforderlichen Angaben zu machen. Der Anamnesebogen ist als Bestandteil der Schuleingangsuntersuchung anzusehen. Da die nunmehr auf das Erforderliche reduzierten medizinischen Daten des Fragebogens in die Beurteilung der Schulfähigkeit des Kindes durch die Schulärzte einfließen, ist es sachgerecht, die Datenerhebung zur Pflicht zu machen.

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

10.1 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006

Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat[1]. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der so genannten "Dritten Säule" der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u.a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen - unter Beachtung der richterlichen Unabhängigkeit - gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung - auch sofern sie in Akten erfolgt - einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Verwendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

10.2 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006

Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterlie-

[1] KOM (2005) 475 vom 4. Oktober 2005

gen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.
Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z.B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwerwiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

10.3 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006

Keine kontrollfreien Räume bei der Leistung von ALG II

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer "Weisung" vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

10.4 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006

Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines "Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums" vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über - durch das Fernmeldegeheimnis geschützte - Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.
Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses - erstmals zur Durchsetzung wirtschaftlicher Interessen - zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

10.5 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006

Verfassungsrechtliche Grundsätze bei Antiterrordateigesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz, BTDrucks. 16/2950) - verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Antiterrordatei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.
- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.
- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.
- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.
- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.
- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

10.6 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006

Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der "Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes" kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der "Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes" ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

10.7 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006

Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- **Transparenz**
  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.
- **Kennzeichnungspflicht**
  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.
- **Keine heimliche Profilbildung**
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.
- **Vermeidung der unbefugten Kenntnisnahme**
  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.
- **Deaktivierung**
  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

10.8 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006

Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte "Schulleben" ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:

Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen "Bildungsregisters" nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im Übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.
- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.
- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

10.9 Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006[2]

Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BRDrucks. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

[2] Die Entschließung wurde einstimmig bei Enthaltung Schleswig-Holsteins gefasst.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicherweise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine "Warnfunktion" mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.