16. Wahlperiode

Drucksache **16/8377**

HESSISCHER LANDTAG

19. 02. 2008

Sechsunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2007
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 19. Februar 2008 · Ausgegeben am 4. März 2008
Druck: Druckerei Chmielorz GmbH, 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags, Postfach 3240, 65022 Wiesbaden

INHALTSVERZEICHNIS

12. Materialien

Technische Aspekte der Online-Durchsuchung (Stand. 30. November 2007)

Organisationsplan des Hessischen Datenschutzbeauftragten

Sachwortverzeichnis zum 36. Tätigkeitsbericht

Abkürzungsverzeichnis

a.E.	am Ende
ABl.	Amtsblatt des Hessischen Kultusministeriums
ABlEG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
Alt.	Alternative
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Sammlung der Entscheidungen des BGH in Zivilsachen
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur
BRDrucks.	Bundesratsdrucksache
BrDSG	Bremisches Datenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTDrucks.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungssammlung des Bundesverwaltungsgerichts
BWG	Bundeswahlgesetz
bzgl.	bezüglich
BZR	Bundeszentralregister
BZSt	Bundeszentralamt für Steuern
bzw.	beziehungsweise
CAN	**C**ontroller **A**rea **N**etwork
CD	**C**ompact **D**isk
CIMECS	**C**entral **I**nterdisciplinary **Me**dic**a**re **S**ystem
CMS	**C**ontent **M**anagement **S**ystem
CR	Computer und Recht
d.h.	das heißt
d.J.	dieses Jahres
DOMEA	In der hessischen Landesverwaltung eingesetztes DV-System zum Dokumentenmanagement
DÖV	Die öffentliche Verwaltung
Drucks.	Drucksache
DV	Datenverarbeitung
DVBl.	Deutsches Verwaltungsblatt
DVD	**D**igital **V**ersatile **D**isc
DVO	Durchführungsverordnung
EDR	**E**vent **D**ata **R**ecorder
EG	Europäische Gemeinschaft
ELENA	**El**ektronische **E**inkommens**na**chweise
ElsterLohn	Elektronische Steuererklärung - Elektronische Lohnsteuerbescheinigung -
etc.	et cetera
EU	Europäische Union
EUROPOL	Europäisches Polizeiamt
evtl.	eventuell
ff.	fortfolgende/r/s
FreizügG/EU	Gesetz über die allgemeine Freizügigkeit von Unionsbürgern
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
ggf.	gegebenenfalls
GK	Gemeinsame Kontrollinstanz
GNU	GNU is not Unix (Akronym)
GnuPG	GNU Privacy Guard (Verschlüsselungssoftware)
grds.	grundsätzlich
GVBl.	Gesetz- und Verordnungsblatt für das Land Hessen
GVU	Gesellschaft zur Verfolgung von Urheberrechtsverletzungen
HBG	Hessisches Beamtengesetz
HBS	Hessische Bezügestelle
HCC	Hessisches Competence Center
HDSB	Der Hessische Datenschutzbeauftragte
HDSG	Hessisches Datenschutzgesetz
HessVGH	Hessischer Verwaltungsgerichtshof

HGO	Hessische Gemeindeordnung
HGöGD	Gesetz über den öffentlichen Gesundheitsdienst
HKHG	Hessisches Krankenhausgesetz
HKM	Hessisches Kultusministerium
HLB	Hessische Landesbahn
HLKA	Hessisches Landeskriminalamt
HLUG	Hessisches Landesamt für Umwelt und Geologie
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 Landwirtschaft
HR	Hessischer Rundfunk
HSchulG	Hessisches Schulgesetz
HSL	Hessisches Statistisches Landesamt
HSM	Hessisches Sozialministerium
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HStiftG	Hessisches Stiftungsgesetz
HStubeiG	Hessisches Studienbeitragsgesetz
HTML	**H**yper**t**ext **M**arkup **L**anguage
https	**H**yper**t**ext **T**ransfer **P**rotocol **S**ecure
HUIG	Hessisches Umweltinformationsgesetz
HVG	Hessisches Vermessungsgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i.d.F.	in der Fassung
i.d.R.	in der Regel
i.S.d.	im Sinne des/der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes
IMSI	**I**nternational **M**obile **S**ubscriber **I**dentity
ISO	International Organization for Standardization
IT	Informationstechnik
JVA	Justizvollzugsanstalt
KDW	Kultus-Data-Warehouse
Kfz	Kraftfahrzeug
KWG	Kommunalwahlgesetz
LFV	Landesamt für Verfassungsschutz
LG	Landgericht
LIN	**L**ocal **I**nterconnect **N**etwork, Master-Slave
Lkw	Lastkraftwagen
LTDrucks.	Landtagsdrucksache
LUSD	**L**ehrer- **u**nd **S**chüler-**D**atenbank
LWG	Landeswahlgesetz
m.E.	meines Erachtens
MAD	Militärischer Abschirmdienst
MDK	Medizinischer Dienst der Krankenversicherung
MeldeDüVO	Meldedatenübermittlungsverordnung
MMR	MultiMedia und Recht
MOST	**M**edia **O**riented **S**ystem **T**ransport
MP3	MPEG-1 Layer 3 (Verfahren zur Audiodatenkompression)
MPEG	Moving Picture Experts Group (Standards für Video- und Audiodaten)
NADIS	**Na**chrichten**d**ienstliches **I**nformations**s**ystem
NJW	Neue Juristische Wochenschrift
NStZ-RR	Neue Zeitschrift für Strafrecht-Rechtsprechungs-Report Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
o.g.	oben genannte/r/s
OASIS	**O**verall **A**nalysis **S**ystem for **I**ntelligence and **S**upport
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol
OSCI	**O**nline **S**ervices **C**omputer **I**nterface
PAYD	**P**ay-**a**s-**y**ou-**d**rive
PC	Personalcomputer
PDF/A	Portable Document Format/Archiv
PGP	Pretty Good Privacy (Verschlüsselungssoftware)
PKI	Public Key Infrastruktur
PKPL	Personalkostenplanung
Pkw	Personenkraftwagen
PPP	**P**ublic **P**rivate **P**artnerships
PStRG	Gesetz zur Reform des Personenstandsrechts

RDV	Recht der Datenverarbeitung
resp.	respektive
RFC	**R**equest **f**or **C**omments
RGebStV	Rundfunkgebührenstaatsvertrag
RP	Regierungspräsidium
s.	siehe
S.	Seite
SächsVBl.	Sächsisches Verwaltungsblatt
SAP R/3 HR	In der Hessischen Landesverwaltung eingesetztes DV-System zur Personaldatenverarbeitung
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SID	Schüler-Individual-Datei
SigG	Signaturgesetz
SIS	Schengener Informationssystem
sog.	sogenannte
SpD	Sozialpsychiatrischer Dienst
SPF	**S**ender **P**olicy **F**ramework
SQL	Structured Query Language
SSL	Secure Socket Layer
StA	Staatsanwaltschaften
StAnz.	Staatsanzeiger für das Landes Hessen
Steuer-ID	Steueridentifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
StVollzG	Strafvollzugsgesetz
TMG	Telemediengesetz
TPStV	Technische Personenstandsverordnung
TTCAN	**T**ime **T**riggered **C**ontroller **A**rea **N**etwork
u.Ä	und Ähnliches
u.a.	unter anderem
u.U.	unter Umständen
UDS	Unfalldatenspeicher
USB	Universal Serial Bus (Schnittstelle bei Geräten)
VAH	Vorläufige Anwendungshinweise
VBlBW	Verwaltungsblätter für Baden-Württemberg
VERONICA	**V**ehicle **E**vent **R**ecording based **on** **I**ntelligent **C**rash **A**ssessment
VerfGH	Verfassungsgerichtshof
VerfSchG	Verfassungsschutzgesetz
VGH	Verwaltungsgerichtshof
VN	Vereinte Nationen
VNC	Virtual Network Computing
XML	Extensible Markup Language
z.B.	zum Beispiel
ZDA	Zertifizierungsdiensteanbieter
ZEVIS	**Ze**ntrales **V**erkehrs**i**nformations**s**ystem
Ziff.	Ziffer
ZPO	Zivilprozessordnung

Register der Rechtsvorschriften

AO	Abgabenordnung 1977 vom 16. März 1976 (BGBl. I S. 613), zuletzt geändert durch Art. 3 des Gesetzes vom 21. Dez. 2007 (BGBl. I S. 3198)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) vom 30. Juli 2004 (BGBl. I S. 1950), zuletzt geändert durch Art. 1 des Gesetzes vom 19. Aug. 2007 (BGBl. I S. 1970)
BDSG	Bundesdatenschutzgesetz i.d.F. der Bekanntmachung vom 14. Jan. 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 22. Aug. 2006 (BGBl. I S. 1970)
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Art. 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten) (Bundeskriminalamtgesetz - BKAG) vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Art. 7 des Gesetzes vom 21. Dez. 2007 (BGBl. I S. 3198)
BWG	Bundeswahlgesetz i.d.F. vom 23. Juli 1993 (BGBl. I S. 1288, 1594), zuletzt geändert durch Art. 5 der Verordnung vom 31. Okt. 2006 (BGBl. I S. 2407)
DV-VerbundG	Datenverarbeitungsverbundgesetz i.d.F. vom 4. Apr. 2007 (GVBl. I S. 258)
EG-Beschluss 2007/533/JI	Beschluss 2007/533/JI des Rates der Europäischen Union vom 12. Juni 2007 Einrichtung, Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABlEG 2007/L 205/63)
EG-Datenschutzrichtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Okt. 1995 (ABlEG 1995/L 281/31)
EG-Richtlinie 2006/24/EG	Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden vom 15. März 2006 und zur Änderung der Richtlinie 2002/58/EG, (ABlEG 2006/L 105/54)
EG-Verordnung Nr. 1986/2006	Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates vom 20. Dez. 2006 über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten des Schengener Informationssystems der zweiten Generation (SIS II) (ABlEG 2006/L 381/1)
EG-Verordnung Nr. 1987/2006	Verordnung (EG) Nr. 1987/2006 vom 20. Dez. 2006 des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABlEG 2006/L 381/4)
EUROPOL-Abkommen	Übereinkommen auf Grund von Art. 31 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (EUROPOL-Übereinkommen) vom 26. Juli 1995 (BGBl. II 1997 S. 2150); geändert durch Protokoll vom 30. Nov. 2000 (BGBl. II 2002 S. 2138), Protokoll vom 28. Nov. 2002 (BGBl. II 2004 S. 83) sowie Protokoll vom 27. Nov. 2003 (BGBl. II 2006 S. 252)
EU-Signaturrichtlinie	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dez. 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABlEG 2000/L 13/12)
FreizügG/EU	Gesetz über die allgemeine Freizügigkeit von Unionsbürgern vom 30. Juli 2004 (BGBl. I S. 1950); zuletzt geändert durch Gesetz vom 7. Dez. 2006 (BGBl. I S. 2814)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. I S. 1), zuletzt geändert durch Gesetz vom 28. Aug. 2006 (BGBl. I S. 2034)
HandwO	Gesetz zur Ordnung des Handwerks (Handwerksordnung) i.d.F. der Bekanntmachung vom 24. Sept. 1998 (BGBl. I S. 3074, berichtigt BGBl. 2006 I S. 2095), zuletzt geändert durch Art. 9a des Gesetzes vom 7. Sept. 2007 (BGBl. I S. 2246)
HBG	Hessisches Beamtengesetz in der Fassung vom 11. Jan. 1989 (GVBl. I S. 25), zuletzt geändert durch Art. 4 des Gesetzes vom 5. Juli 2007 (GVBl. I S. 378)

HDSG	Hessisches Datenschutzgesetz in der Fassung vom 7. Jan. 1999 (GVBl. I S. 98)
HGO	Hessische Gemeindeordnung i.d.F. vom 1. Apr. 2005 (GVBl. I S. 142), zuletzt geändert durch Gesetz vom 15. Nov. 2007 (GVBl. I S. 757)
HGöGD	Hessisches Gesetz über den öffentlichen Gesundheitsdienst vom 28. Sept. 2007 (GVBl. I S. 659)
HKHF	Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2002 - HKHG) vom 6. Nov. 2002 (GVBl. S. 662)
HMG	Hessisches Meldegesetz i.d. Neufassung vom 10. März 2006 (GVBl. I S. 66)
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)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i.d.F. vom 14. Jan. 2005 (GVBl. I S. 14), zuletzt geändert durch Gesetz vom 28. Sept. 2007 (GVBl. I S. 634)
HStiftG	Hessisches Stiftungsgesetz vom 4. April 1966 (GVBl. I S. 77), zuletzt geändert durch Gesetz vom 6. Sept. 2007 (GVBl. I S. 546)
HStubeiG	Hessisches Studenbeitragsgesetz vom 16. Okt. 2006 (GVBl. I S. 512)
HSÜG	Hessisches Sicherheitsüberprüfungsgesetz vom 28. Sept. 2007 (GVBl. I S. 623)
HUIG	Hessisches Umweltinformationsgesetz vom 14. Dez. 2006 (GVBl. I S. 659)
HVG	Hessisches Gesetz über das Liegenschaftskataster und die Landesvermessung (Hessisches Vermessungsgesetz) vom 2. Okt. 1992 (GVBl. I S. 453), zuletzt geändert durch Art. 4 des Gesetzes vom 20. Dez. 2005 (GVBl. I S. 506)
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz) vom 5. Sept. 2005 (BGBl. I S. 2722)
Kindergesundheitsschutz-Gesetz	Hessisches Gesetz zur Verbesserung des Gesundheitsschutzes für Kinder vom 14. Dez. 2007 (GVBl. I S. 856)
KWG	Hessisches Kommunalwahlgesetz i.d.F. vom 1. April 2005 (GVBl. I S. 197)
LWG	Gesetz über die Wahlen zum Landtag des Landes Hessen (Landeswahlgesetz) i.d.F. vom 28. Dez. 2005 (GVBl. I S. 110, 439)
MeldDÜVO	Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (Meldedatenübermittlungsverordnung) i.d.F. vom 24. Sept. 1990 (GVBl. I S. 587, 590, 749), zuletzt geändert durch Art. 2 des Gesetzes vom 14. Dez. 2007 (GVBl. I S. 856)
Pflichtstundenverordnung	Verordnung über die Pflichtstunden der Lehrer, über die Anwendung dienstlicher Tätigkeiten und über Pflichtstundenermäßigungen vom 20. Juli 2006 (ABl. Nr. 08/06 S. 631)
Prümer Vertrag	Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich vom 27. Mai 2005 (BGBl. 2006 I S. 1458)
PStRG	Gesetz zur Reform des Personenstandsrechts vom 19. Februar 2007 (BGBl. I S. 122)
RGebStV	Rundfunkgebührenstaatsvertrag vom 31. August 1991, zuletzt geändert durch Art. 7 Neunter Rundfunkänderungsstaatsvertrag vom 31. Juli bis 10. Oktober 2006, in Hessen ratifiziert durch Gesetz vom 5. Februar 2007 (GVBl. I S. 206)
SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 19. Juni 1990 -Schengener Durchführungsübereinkommen (GVBl. 1993 II S. 1010)

SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dez. 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes vom 21. März 2005 (BGBl. I S. 818)
SGB V	Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dez. 1988 (BGBl. I S. 2477, 2482) zuletzt geändert durch Gesetz vom 19. Dez. 2007 (BGBl. I S. 3024)
SGB VIII	Achtes Buch Sozialgesetzbuch - Kinder und Jugendhilfe - i.d.F. vom 8. Dez. 1998 (BGBl. I S. 3546), zuletzt geändert durch Gesetz vom 8. Sept. 2005 (BGBl. I S. 2729)
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - i.d.F. vom 18. Jan. 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 9 des Gesetzes vom 9. Dez. 2004 (BGBl. I S. 3242)
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 des Gesetzes vom 26. Feb. 2007 (BGBl. I S. 179)
Staatsangehörigkeits-angelegenheiten, Zuständigkeiten	Gesetz zur Bestimmung der zuständigen Behörden in Staatsangehörigkeitsangelegenheiten vom 31. März 2005 (GVBl. I S. 229, 234)
StPO	Strafprozessordnung in der Fassung vom 7. Apr. 1987 (BGBl. I S. 1074), zuletzt geändert durch Art. 1 des Gesetzes vom 21. Dez. 2007 (BGBl. I S. 3198)
StrÄndG	41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. Aug. 2007 (BGBl. I S. 1786)
StVG	Straßenverkehrsgesetz i.d.F. vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 9 und 10 des Gesetzes vom 5. Jan. 2007 (BGBl. I S. 2)
StVollzG	Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung (Strafvollzugsgesetz) vom 16. März 1976 (BGBl. I S. 581), zuletzt geändert durch Gesetz vom 19. Feb. 2007 (BGBl. I S. 122)
Telekommunikationsüberwachung (Umsetzung der Richtlinie 2006/24/EG)	Gesetz zur Neuregelung der Telekommunikationsüber-wachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dez. 2007 (BGBl. I S. 3198)
Terrorismusbekämpfungs-ergänzungsgesetz	Terrorismusbekämpfungsergänzungsgesetz vom 5. Jan. 2007 (BGBl. I S. 2)
Terrorismusbekämpfungs-gesetz	Terrorismusbekämpfungsgesetz vom 9. Jan. 2002 (BGBl. I S. 361)
TMG	Telemediengesetz vom 26. Febr. 2007 (BGBl. I S. 179)
verdeckte Ermittlungsmaßnahmen (Umsetzung der Richtlinie 2006/24/EG)	Gesetz zur Neuregelung der Telekommunikationsüber-wachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dez. 2007 (BGBl. I S. 3198)
VerfSchG	Gesetz über das Landesamt für Verfassungsschutz vom 19. Dez. 1990 (GVBl. I S. 753); zuletzt geändert durch das Hessische Sicherheitsüberprüfungsgesetz vom 28. Sept. 2007 (GVBl. I S. 623)
Vertrag über die Europäische Union	Vertrag zur Gründung der Europäischen Gemeinschaft vom 25. März 1957 (BGBl. II S. 766) i.d.F. des Vertrags über die Europäische Union vom 7. Feb. 1992 (BGBl. II S. 1253/1256); zuletzt geändert durch die Akte zum Beitrittsvertrag vom 16. Apr. 2003 (BGBl. II S. 1410) und vom 25. Apr. 2005 (ABlEG 2005/L 157/11)
VIG	Gesetz zur Neuregelung der Verbraucherinformationen vom 5. Nov. 2007 (BGBl. I S. 2558)
VN-Übereinkommen	Gesetz zur Umsetzung des VN-Übereinkommens vom 13. Apr. 2005 zur Bekämpfung nuklearterroristischer Handlungen vom 26. Okt. 2007 (BGBl. I S. 2523)
Wohnraumüberwachung, akustische	Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005 (BGBl. I S. 1841)
Zollfahndungsdienstgesetz	Gesetz zur Änderung des Zollfahndungsdienstgesetzes vom 12. Juni 2007 (BGBl. I S. 1037)

Kernpunkte

1. Der Datenschutz hat in der Gegenwart einen schweren Stand. Der Gesetzgeber neigt zunehmend dazu, sich über Datenschutzbelange hinwegzusetzen. Die Abwehrkomponente des Datenschutzes droht in der Flut gesetzlicher Einschränkungen des Rechts auf informationelle Selbstbestimmung unterzugehen. Die Schutzkomponente wird durch staatliche Maßnahmen unterlaufen (siehe Kernpunkt 4). Die Zugangskomponente des Datenschutzes ist so schwach ausgeprägt, dass es an informationeller Ausgewogenheit fehlt (Ziff. 1).

2. Der öffentliche Bereich, für den der Hessische Datenschutzbeauftragte zuständig ist, reicht über den hoheitlichen Bereich hinaus. Er erstreckt sich auf alle Bereiche, in denen öffentliche Aufgaben wahrgenommen werden und deshalb Grundrechte gelten. Dazu zählen alle Aufgaben, die im Allgemeininteresse liegen - von der Daseinsvorsorge bis hin zur sog. Verwaltungsmittlung (Ziff. 2).

3. Innerhalb des von der Europäischen Union gestalteten Raums der Freiheit, des Rechts und der Sicherheit sind Datenschutzfragen bei Aufenthalt und Ausweisung von EU-Ausländern und bei der Suche von Straftätern zunehmend in europäischer Zusammenarbeit zu lösen. Nicht nur der räumliche Bereich, sondern auch die Qualität der Zusammenarbeit befindet sich in stetiger Weiterentwicklung. In den mit der Datenschutzberatung und -kontrolle befassten europäischen Gremien arbeitet der Hessische Datenschutzbeauftragte als Ländervertreter mit (Ziff. 3).

4. Aus der Fülle der modernen Datenzugriffe ragen die Online-Überwachungen und -Durchsuchungen heraus. Solche Maßnahmen führen zu erheblichen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung. Deshalb sind an deren verfassungsrechtliche Zulässigkeit besonders hohe Anforderungen zu stellen. Vor allem aber sind die Online-Durchsuchungen datenschutzpolitisch fragwürdig. Die vom Staat geförderten E-Government-Projekte sind für die Beteiligten nur im Umfeld einer geschützten und sicheren Kommunikation attraktiv. Gefährdet der Staat selbst die Sicherheit durch für Online-Durchsuchungen bewusst offen gehaltene, aber nicht bekannt gegebene Sicherheitslücken, gefährdet er zugleich die Akzeptanz dieser Projekte (Ziff. 4.1).

5. Sollen die neuen Zentralisierungs- und Konzentrationstendenzen auf Landesebene aber auch länderübergreifend nicht behindert, sondern datenschutzrechtlich gestaltet werden, ist die Weiterentwicklung des Hessischen Datenschutzgesetzes erforderlich (Ziff. 5.1).

6. Veröffentlichungen personenbezogener Daten im Internet sind wegen der vielfältigen Auswertungsmöglichkeiten und der Verkürzung der Individualrechte der Betroffenen von neuer Qualität. Sollen Veröffentlichungen mit einer Einwilligung der Betroffenen erfolgen, muss eine Aufklärung über Risiken vorangehen. Auch vor der Schaffung von Rechtsgrundlagen für solche Veröffentlichungen sind Risiken und Nutzen sorgfältig abzuwägen und im Zweifel datensparsame Lösungen zu wählen (Ziff. 5.1.2, 5.7.1 und 5.8.8).

7. Auf die in jüngster Zeit bekannt gewordenen Fälle von Misshandlung und Vernachlässigung von Kleinkindern hat der hessische Gesetzgeber mit der Verabschiedung des Kindergesundheitsschutz-Gesetzes reagiert. Das Datenschutzkonzept sieht einen sensiblen und am Kindeswohl orientierten, streng zweckgebundenen Umgang mit den Daten der Kinder, Eltern und Ärzte vor. Eine Evaluation der Wirksamkeit der neuen Datensammlungen und Datenflüsse ist rechtlich dringend geboten (Ziff. 5.8.2).

8. Auch im Zusammenhang mit der Gewährung von (Sozial-)Leistungen oder der Befreiung von Gebühren oder Verpflichtungen dürfen nur diejenigen Daten erhoben oder übermittelt werden, die zur Entscheidung über den Anspruch jeweils erforderlich sind. Dies gilt insbesondere für Gesundheits- oder Sozialdaten. Die Erhebung von Daten bei Dritten ist hier lediglich zulässig, soweit die Daten nicht zuverlässig beim Anspruchsteller erhoben werden können und sie für die Entscheidung über den Anspruch erforderlich sind (Ziff. 5.6.3, 5.9.1, 5.9.2, 7.1.1).

9. Die Notwendigkeit der vollständigen Löschung auf Speichermedien war eines der Themen der Beratungen im Bereich der Technik. Dieses Problem ist von erheblicher praktischer Relevanz, weil nicht nur Rechner und PDAs, sondern sehr viel mehr technische Geräte heute Speichermedien enthalten (Ziff. 8.2).

10. Die Zusammenhänge beim Einsatz für Verwaltungszwecke geeigneten Signaturen sind kompliziert. Die Entscheidung, welche Signatur für welche Zwecke eingesetzt werden soll, hat neben der Rechtswirkung der Signatur auch den unterschiedlichen Aussagewert der Signaturprüfung in die Betrachtung einzubeziehen (Ziff. 8.1).

1. Einführung

1.1 Allgemeines

Geburtsstunde der verfassungsrechtlichen Verankerung des Datenschutzes war der 15. Dezember 1983, der Tag an dem das Volkszählungsurteil (1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1) erging. Als Ausprägung des Persönlichkeitsrechts trägt seither das Recht auf informationelle Selbstbestimmung Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich für den Einzelnen aus informationsbezogenen Maßnahmen unter den Bedingungen moderner Datenverarbeitung ergeben (vgl. BVerfG, Beschluss vom 9. März 1988 - 1 BvL 49/86, BVerfGE 78, 77, 84; Beschluss vom 11. Juni 1991 - 1 BvR 239/90, BVerfGE 84, 192, 194; Beschluss vom 12. April 2005 - 2 BvR 1027/032, BVerfGE 113, 29, 46; Urteil vom 2. März 2006 - 2 BvR 2099/04, BVerfGE 115, 166, 188; Beschluss vom 4. April 2006 - 1 BvR 518/02, BVerfGE 115, 320, 341 f.; Urteil vom 13. Februar 2007 - 1 BvR 421/05, DVBl. 2007, 381, 382; Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a., DVBl. 2007, 1023; SächsOVG, Beschluss vom 19. April 2006 - 3 BS 322/05, NJW 2007, 169, 170; HambOVG, Beschluss vom 21. März 2007 - 3 Bs 396/05, DÖV 2007, 893). Trotz der hohen Datenschutzkultur, die im Land Hessen ihren Ursprung nahm, hat sich allmählich gezeigt, dass den Belangen des Datenschutzes allein durch die Abwehr von staatlichen Eingriffen in die informationelle Selbstbestimmung nicht hinreichend Rechnung getragen wird.

In Anknüpfung an die Ausführungen unter Ziff. 2.1.2 meines 34. sowie Ziff. 1.2 und 1.3 meines 35. Tätigkeitsberichts beginnt daher auch der vorliegende Tätigkeitsbericht mit allgemeinen Ausführungen zu den Hauptstoßrichtungen eines zeitgemäßen Datenschutzes und zu den 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. Richtungsweisend für die Entwicklung des Datenschutzrechts auch in Hessen ist hier namentlich die Rechtsprechung des BVerfG. Den Schwerpunkt dieses Tätigkeitsberichts bilden landesspezifische datenschutzrechtlich relevante Querschnittsthemen, Fragestellungen im Bereich der Justiz, des Verfassungsschutzes, des Ausländerrechts, des Verkehrswesens, der Schulen und Schulverwaltung, des Gesundheitswesens, des Sozialwesens, des Personalwesens, der Kommunen sowie sonstigen Selbstverwaltungskörperschaften. Ferner werden die Entwicklungen und Empfehlungen im Bereich der Technik 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 Datenschutz

Der Datenschutz weist eine Abwehr-, Schutz- und Zugangskomponente auf.

1.2.1 Abwehrkomponente

Die Abwehrkomponente des Datenschutzes betrifft Eingriffe in die informationelle Selbstbestimmung durch den Staat. Ein Grundrecht auf Abwehr staatlicher Datenzugriffe ist im Grundgesetz nicht ausdrücklich geregelt. Das BVerfG hätte insoweit allein auf die allgemeine Handlungsfreiheit zurückgreifen können. Das tat es nicht, sondern stützte das "Recht auf informationelle Selbstbestimmung" auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Das lässt sich wie folgt erklären: Die Grundrechte des Grundgesetzes bilden ein System, dessen Eckpunkte durch Art. 2 Abs. 1 und Art. 1 Abs. 1 GG gebildet werden. Die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG markiert dabei lediglich den Ausgangsbereich benannter und unbenannter Freiheitsrechte, die sich auf einer gleitenden Skala auf Art. 1 Abs. 1 GG zu bewegen. Je näher das Pendel bei der Menschenwürde ausschlägt, desto strenger sind die Rechtfertigungsanforderungen für etwaige Grundrechtseinschränkungen. Während die Menschenwürde selbst unbeschränkbar ist, handelt es sich bei der informationellen Selbstbestimmung um ein beschränkbares Grundrecht, das die anderen Ausprägungen des Persönlichkeitsrechts nicht nur ergänzt, sondern mit diesen in engem, bisweilen untrennbaren Zusammenhang steht. Die Reichweite der Beschränkbarkeit des Persönlichkeitsrechts und damit auch der informationellen Selbstbestimmung hängt demzufolge vom jeweiligen Sachzusammenhang ab (BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a., DVBl. 2007, 1023). Unmittelbarer Ausfluss der Menschenwürde ist ein für Dritte unzugänglicher Bereich individueller Privatheit, den das BVerfG seit dem Elfes-Urteil vom 16. Januar 1957 (1 BvR 253/56, BVerfGE 6, 32, 41) anerkennt. In der Mikrozensusentscheidung 16. Juli 1969 führte das BVerfG aus, dass es mit der Menschenwürde nicht zu vereinbaren wäre, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren (1 BvL 19/63, BVerfGE 27, 1, 6). Weiter argumentierte das Gericht, eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Bürger sei dem Staat auch deshalb versagt, weil dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein "Innenraum" verblieben müsse, in dem er "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt". Die Kernbereichthese wurde also lange vor der informationellen Selbstbestimmung entwickelt. Sie birgt die Gefahr einer räumlich-gegenständlichen Fehlinterpretation. Unantastbar ist die Privatheit, die die Menschenwürde ausmacht, eben der Kernbereich privater Lebensgestaltung (BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1783/05, DVBl. 2007, 1425, 1429). So verbietet es das Recht auf Privatheit, beginnend mit der physisch-psychischen Privatsphäre, den Menschen in seiner gesamten Persönlichkeit zu katalogisieren (BVerfG, Beschluss vom 15. Januar 1970 - 1 BvR 13/68, BVerfGE 27, 344, 350 ff.; Beschluss vom 24. Mai 1977 - 2 BvR 988/75, BVerfGE 44, 353, 372 f.; Beschluss vom 26. April 1994 - 1 BvR 1968/88, BVerfGE 90, 255, 260; Urteil vom 15. Dezember 1999 - 1 BvR 653/96, BVerfG 101, 361, 382 f.). Diesem absolut geschützten Kernbereich ist die Privatsphäre in der Schutzintensität nachgelagert (BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1783/05, DVBl. 2007, 1425,1429). Zur engeren äußeren Privatsphäre zählt insbesondere der Wohnbereich einschließlich der dort stattfindenden Kommunikation. Der Schutz der Wohnung insbesondere vor "Lauschangriffen" wurde in meinen früheren Tätigkeitsberichten ausführlich behandelt (33. Tätigkeitsbericht, Ziff. 4.1; vgl. nunmehr VerfGH Rheinland-Pfalz, Urteil vom 29. Januar 2007 - VGH B 1/06, DVBl. 2007, 569).

Der Übergang vom Wohnbereich zum Telekommunikationsbereich ist fließend. Nach dem Urteil des BVerfG vom 2. März 2006 (2 BvR 2099/04, BVerfGE 115, 166, 182) schützt Art. 10 GG die Fernkommunikation Privater, d.h. die Vertraulichkeit der individuellen Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und dadurch in besonderer Weise einen Zugriff Dritter - einschließlich staatlicher Stellen - ermöglicht. Außerhalb des laufenden Kommunikationsvorgangs werden die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation durch Art. 13 Abs. 1 GG und das Recht auf informationelle Selbstbestimmung gewährleistet. Mit der Telekommunikation wird faktisch die engere Privatsphäre verlassen und der Bereich der kommunikativen und mobilen Grundrechte eröffnet. Die informationelle Selbstbestimmung ist jedoch auch bei der mobilen Grundrechtsentfaltung, der gesellschaftlichen, sozialen wirtschaftlichen und politischen Betätigung zu beachten.

1.2.2 Schutzkomponente

Das informationelle Selbstbestimmungsrecht verpflichtet ferner die staatlichen Organe, dem Einzelnen **Schutz** dagegen zu bieten, dass private Dritte ohne sein Wissen und ohne seine Einwilligung Zugriff auf seine personenbezogenen Daten nehmen. Dabei spielt die Sicherheit der Kommunikation eine immer größere Rolle. Das vielfach nur als Schlagwort verwendete Sicherheitsargument bekommt beim Datenschutz eine besondere Bedeutung. Wie Freiheit sich nur in Sicherheit entfalten kann, setzt die informationelle Selbstbestimmung sicheren Datenaustausch voraus. Der Staat muss diese Sicherheit gewährleisten und aktiven Datenschutz betreiben.

1.2.3 Datenzugangsschutz

Auf die datenschutzrechtliche Bedeutung der Informationszugangsfreiheit ging bereits der 35. Tätigkeitsbericht ausführlich ein. Seit dem Inkrafttreten des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz - IFG) vom 5. September 2005 (BGBl. I S. 2722) ist die Entwicklung weiter vorangeschritten. Spezielle Informationszugangsgesetze wie das im Dezember 2006 verabschiedete Hessische Umweltinformationsgesetz (HUIG, GVBl. I S. 659; hierzu HessVGH, Urteil vom 20. März 2007 - 11 A 1999/06, DÖV 2007, 1019) oder das Gesetz zur Neuregelung der Verbraucherinformationen vom 5. November 2007 (BGBl. I S. 2558) traten In Kraft. Zweck dieser Gesetze ist es, durch Ansprüche auf Zugang zu amtlichen Informationen außerhalb konkreter Verwaltungsverfahren die demokratische Meinungs- und Willensbildung zu fördern (BVerwGE, Beschluss vom 15. Oktober 2007 - 7 B 9.07). Die internationale und nationale Rechtsentwicklung läuft erkennbar auf die Anerkennung eines derartigen Rechts auf Zugang zu Behördeninformationen zu (vgl. Schomerus/Tolkmitt, Informationsfreiheit durch Zugangsvielfalt, DÖV 2007, 985 ff.; Augsberg, Der Staat als Informationsmittler, DVBl. 2007, 733 ff.). Der Landesgesetzgeber sieht sich letztlich nur noch vor die Alternative gestellt, ob er in einen rollenden Zug einsteigen oder auf einen fahrenden Zug aufspringen will. Ich bin weiterhin bereit, beim Einsteigen Hilfestellung zu leisten.

1.3 Rechtsentwicklung

1.3.1 Überblick

Die Gesetzgeber in Bund und Land und auf Gemeinschaftsebene waren auch im vorliegenden Berichtszeitraum rührig und erließen eine Vielzahl datenschutzrechtlich relevanter Vorschriften (vgl. Gola/Klug, Die Entwicklung des Datenschutzrechts in den Jahren 2006/2007, NJW 2007, 2452 ff.). Diese sind im jeweiligen Sachzusammenhang gewürdigt. Vor die Klammer gezogen wird vorliegend lediglich die Gesetzgebung zur Bekämpfung von organisierter Kriminalität und Terrorismus.

1.3.2 Gesetzgebung

Die internationale organisierte Kriminalität erfasst neben Rauschgifthandel und Geldwäsche, Menschen- und Waffenschmuggel, Schleusung von illegalen Migranten, die Verschiebung von Kraftfahrzeugen und anderen hochwertigen Produkten, Produktpiraterie und sonstige Wirtschaftsstraftaten und Taten, die sich des Internets bedienen oder das Internet selbst angreifen (Cyber Crimes). Sie ist nicht weniger gefährlich, wohl aber weniger spektakulär, als der internationale Terrorismus. Nach den Anschlägen vom 11. September 2001 wurde in beiderlei Hinsicht durch einen Ausbau des Sicherheitsrechts reagiert. Erwartungsgemäß war das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) nur ein Zwischenglied in einer fortlaufenden Gesetzgebungskette, so dass mit dem im Berichtszeitraum ergangenen Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I S. 2) ebenfalls nur der Entwicklungsprozess fortgeschrieben wurde. Die Momentaufnahme ergibt: Wie beim Terrorismusbekämpfungsgesetz handelt es sich bei dem Terrorismusbekämpfungsergänzungsgesetz um ein Artikelgesetz. Geändert wurden u.a. das Bundesverfassungsschutzgesetz, das MAD-Gesetz und das BND-Gesetz, das BKA-Gesetz, das Artikel 10-Gesetz, das Sicherheitsüberprüfungsgesetz und die Sicherheitsüberprüfungsfeststellungsverordnung, das Bundespolizeigesetz, das Gesetz zu dem Schengener Übereinkommen, das Vereinsgesetz, das Pass- und Personalausweisgesetz, das Zollverwaltungsgesetz, das Straßenverkehrsgesetz, das Luftsicherheitsgesetz, eine Reihe ausländerrechtlicher Gesetze und das Bundeszentralregistergesetz. Zu erwähnen ist noch das Europäische Haftbefehlsgesetz, das weit über die Terrorismusbekämpfung hinausgreift. Einen Beitrag zur Terrorismusbekämpfung leistet das Gesetz zur Änderung des Zollfahndungsdienstgesetzes und anderer Gesetze vom 12. Juni 2007 (BGBl. I S. 1037). Hinzu kamen noch das Gesetz zur Umsetzung des VN-Übereinkommens vom 13. April 2005 zur Bekämpfung nuklearterroristischer Handlungen vom 26. Oktober 2007 (BGBl. I S. 2523) und das Einundvierzigste Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7. August 2007 (BGBl. I S. 1786; vgl. Ernst, Das neue Computerstrafrecht, NJW 2007, 2661 ff.). Die Anbieter elektronischer Kommunikationsdienste oder Kommunikationsnetze sollen ferner nach der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG vom 15. März

2006 (ABlEG 2006/L 105/54) verpflichtet werden, die bei ihren betriebsbedingt anfallenden Kommunikationsdaten ("Verbindungsdaten") über den betrieblich erforderlichen Zeitraum hinaus ab dem Zeitpunkt der Kommunikation mindestens sechs Monate und höchstens zwei Jahre auf Vorrat zu speichern (vgl. Gola/Reif, Datenschutz- und presserechtliche Bewertung der "Vorratsdatenspeicherung", NJW 2007, 2599 ff.). Der Bundestag hat am 9. November 2007 das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BTDrucks. 16/5846) verabschiedet. Alle diese Gesetze sind datenschutzrechtlich relevant. Dies gilt auf Landesebene auch für das Gesetz zur Änderung des Gesetzes über das Landesamt für Verfassungsschutz und des Hessischen Ausführungsgesetzes zum Gesetz zu Artikel 10 Grundgesetz vom 6. September 2007 (GVBl. I S. 542).

1.3.3 Rechtsprechung

Die akustische Wohnraumüberwachung ("großer Lauschangriff") beschäftigt immer noch das BVerfG. Der Gesetzgeber ergänzte mit dem Gesetz zur Umsetzung des Urteils des BVerfG vom 3. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005 (BGBl. I S. 1841) die Ausgestaltung des Lauschangriffs entsprechend den verfassungsrechtlichen Vorgaben. Mit Kammerbeschluss vom 11. Mai 2007 (2 BvR 543/06, NJW 2007, 2753) hat das BVerfG die Verfassungsmäßigkeit des neugefassten § 100c Abs. 1 StPO bestätigt. Hinsichtlich des absoluten Kernbereichs privater Lebensgestaltung hat sich der Kammerbeschluss eine Rückzugsmöglichkeit eröffnet, indem das BVerfG eine positive Konkretisierungspflicht verneinte und auf die Kasuistik setzte. Damit wird es möglich, unabhängig von der Wohnung private und öffentliche Bereiche zu unterscheiden, ohne gleich räumliche Tabuzonen zu errichten. Ich habe für Hessen eine entsprechende Konstruktion im Verfassungsschutzgesetz vorgeschlagen.

Da die Telekommunikation heute nicht mehr nur von der Wohnung, sondern über Mobiltelefon praktisch von jedem Standort aus abgewickelt wird, sind die technischen Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkgeräts und zur Ermittlung der Geräte- und Kartennummer sicherheitsrelevant. Diese Mittel werden vereinfachend unter dem Begriff des IMSI-Catchers zusammengefasst. Benötigt wird der IMSI-Catcher, wenn die Rufnummer nicht bekannt ist. Nur durch die Ermittlung der Bestandsdaten des genutzten Mobiltelefons wird dann eine Überwachung der Telekommunikation möglich. Ob dadurch bereits in das Fernmeldegeheimnis eingegriffen wird, ist zweifelhaft. Die erste Kammer des Zweiten Senats des BVerfG hat jedenfalls die Verfassungsbeschwerde gegen § 100i StPO nicht zu Entscheidung angenommen (Beschluss vom 22. August 2006 - 2 BvR 1345/03, NJW 2007, 351). Der erste Schritt in die schrankenlose Telefonüberwachung ist damit getan.

Interessanter ist der Zugriff auf vorrätige Daten der Telekommunikation. Hier hatte das BVerfG darauf aufmerksam gemacht, dass Anordnungen gegenüber Telekommunikationsunternehmen, im Rahmen der Strafverfolgung Auskunft über die für die Abrechnungszwecke bereits vorhandenen oder in Durchführung einer Zielwahlsuche zu ermittelnden Verbindungsdaten zu erteilen, in das Fernmeldegeheimnis des von der Auskunft betroffenen eingreifen (Urteil vom 12. März 2003 - 1 BvR 330/96, 348/99, BVerfGE 107, 299). Dennoch hat der Gesetzgeber das Gesetz zur Neuregelung der Telekommunikationsüberwachung beschlossen.

Die Vorratsdatenspeicherung greift in das Fernmeldegeheimnis und in die informationelle Selbstbestimmung ein. Die Verfassungsmäßigkeit des Gesetzes ist fragwürdig.

Noch fragwürdiger sind die Online-Durchsuchung und Online-Überwachung, bei der ein Zugriff über das Internet auf den PC und sonstige "informationstechnische Systeme" von Verdächtigen erfolgen darf. Über die technische Vorgehensweise existieren noch keine abschließenden Vorstellungen. Computerprogramme zur Ermöglichung von entsprechenden Vorhaben sind aber erhältlich. Im Jahr 2006 beantragte die Bundesanwaltschaft beim Ermittlungsrichter I des Bundesgerichtshofs: "Gemäß §§ 102, 105 Abs. 2, 94, 98, 169 Abs. 1 Satz 2 StPO die Durchsuchung des von dem Beschuldigten benutzten Personalcomputers/Laptops, insbesondere der auf der Festplatte und im Arbeitsspeicher abgelegten Dateien…, und deren Beschlagnahme anzuordnen und den Ermittlungsbehörden zur verdeckten Ausführung dieser Maßnahme zu gestatten, ein hierfür konzipiertes Computerprogramm dem Beschuldigten zur Installation zuzuspielen, und die auf den Speichermedien des Computers abgelegten Dateien zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen." Der Ermittlungsrichter des BGH lehnte den Antrag ab. Mit Beschluss vom 31. Januar 2007 (StB 18/06, NJW 2007, 930 m. Anm. Hamm = MMR 2007, 174 m. Anm. Bär) wies der Bundesgerichtshof die hiergegen erhobene Beschwerde der Generalbundesanwaltschaft zurück, da die verdeckte Online-Durchsuchung mangels einer Ermächtigungsgrundlage unzulässig sei. Daraufhin wurden Forderungen laut, die gebotenen Rechtsgrundlagen zu schaffen. Als erste landesrechtliche Regelung sieht § 5 Abs. 2 Nr. 11 Satz 1 3. Alt. i. V. m. § 7 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GV NW 2006, S. 620) das heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie den heimlichen Zugriff auf informationstechnische Systeme auch mit dem Einsatz technischer Mittel vor. Gegen diese Regelung wurden fünf Verfassungsbeschwerden erhoben, die beim BVerfG unter dem Az. 1 BvR 377/07 und 1 BvR 595/07 anhängig sind. Verfassungsrechtlich ist bedeutsam, dass der PC mittlerweile am Kernbereich der Privatheit teilnimmt, da er vielen Menschen zur Aufbewahrung privatester Informationen (Fotografien, Tagebuchaufzeichnungen, persönliche Briefe, Reiseberichte u. dgl.) dient. Unabhängig davon, wo sich der PC befindet, ist damit der Kernbereich privater Lebensgestaltung berührt. Die Geeignetheit und Erforderlichkeit der Online-Durchsuchung zur Terrorismus- und Kriminalitätsbekämpfung ist noch nicht dargetan. Auch informationspolitisch ist die Online-Durchsuchung und -Überwachung problematisch, weil der Staat dadurch die von ihm selbst propagierte Sicherheit des Datenübermittlungsvorgangs gefährdet. Der Eindruck entsteht, dass der Staat sich bei der heimlichen Überwachung "schmutziger" Tricks in Anlehnung an die Heraklid-Sentenz: "sus magis in caeno gaudet quam in fonte sereno" (das Schwein zieht die trübe der klaren Quelle vor) bedeutet. Daher habe ich die Online-Überwachung als "datenschutzpolitische Sauerei" bezeichnet. Damit sollte nicht zum Ausdruck gebracht werden, dass sich Maßnahmen der Online-Durchsuchung und Online-Überwachung unter keinerlei Umständen verfassungsrechtlich rechtfertigen ließen. Vielmehr sollte in pointierter Form davor gewarnt werden, die E-Government-Projekte der

Landesregierung zu konterkarieren, indem das Vertrauen der Bevölkerung in die Sicherheit der elektronischen Kommunikation mit Behörden zerstört wird. In die gleiche Richtung zielt die von den Datenschutzbeauftragen des Bundes und der Länder im Rahmen ihrer 73. Konferenz im März 2007 erhobene und auf ihrer 74. Konferenz im Oktober 2007 noch einmal bekräftigte Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Schaffung von Ermächtigungsgrundlagen für die Online-Durchsuchung zu verzichten.

Der Kontext Mobilität und Datensicherheit (hierzu Ronellenfitsch, SächsVBl. 2006, 101 ff.) wird durch die Erstellung von Bewegungsprofilen berührt, die den freien Ortswechsel unmittelbar oder mittelbar beeinflussen. Der freie Ortswechsel wird zunächst durch eine überzogene Kamera- und Videoüberwachung beeinträchtigt. Für die Überwachungstätigkeit kann es gute Gründe geben, etwa das von mir mitgetragene Konzept der Sicherheitsinseln. Das Recht der Privatheit muss gleichwohl gewahrt bleiben. Der Kammerbeschluss des BVerfG vom 23. Februar 2007 zur Videoüberwachung von Resten einer ehemaligen mittelalterlichen Synagoge (1 BvR 2368/06, NVwZ 2007, 688 mit Besprechung von Zöller/Fetzer, NVwZ 2007, 775 ff.) brach in diesem Sinne eine Lanze für die mobile Privatheit. Ob dies im Hinblick auf den Datenabgleich bei der Erfassung von Kfz-Kennzeichen geschehen wird, ist noch völlig offen. Im Verfassungsbeschwerdeverfahren gegen § 14 Abs. 5 HSOG (1 BvR 2034/05) fand am 20. November 2007 die mündliche Verhandlung vor dem BVerfG statt.

Die wirtschaftliche Betätigungsfreiheit wird vor allem durch Datenzugriffe in die Konten beeinträchtigt. Nach der Rechtsprechung des Bundesgerichtshofs gelten Datenschutz und Bankgeheimnis nebeneinander. Dabei kommt dem Datenschutz kein Vorrang zu, vielmehr hat das Datenschutzrecht nur eine Auffangfunktion. Aus dem Datenschutzrecht lässt sich daher kein Abtretungsverbot von Darlehensforderungen eines Kreditinstituts gegen natürliche Personen ableiten (Urteil vom 27. Februar 2007, XI ZR 195/05, BGHZ 171, 180).

Das BVerfG hat dem unbestimmten Zugriff auf die Kontostammdaten mit Beschluss vom 13. Juni 2007 (1 BvR 1550/03 u. a., NJW 2007, 2464) zwar einen Riegel vorgeschoben. § 93 Abs. 8 AO, der den automatischen Kontenabruf ermöglicht, verstößt aber lediglich gegen den Bestimmtheitsgrundsatz. Ein gezielter Zugriff auf derartige Datenbestände zur Terrorismusbekämpfung und zur Bekämpfung der organisierten Kriminalität ist damit nicht ausgeschlossen. Der Datenzugriff des Staates wurde schon mit dem 2. Terrorismusbekämpfungsgesetz erleichtert, das dem Bundesamt für Verfassungsschutz und dem Bundesnachrichtendienst die Befugnis einräumte, von Kreditinstituten, Finanzunternehmen und Finanzdienstleistern Auskünfte zu Konten, Konteninhabern, Geldbewegungen und Geldanlagen zu verlangen. Mit Rücksicht auf die informationelle Selbstbestimmung und Art. 10 GG sah der Gesetzgeber jedoch verfahrensrechtliche Schutzvorkehrungen der Betroffenen vor (Einschaltung der G10-Kommission vor Vollzug einer beabsichtigten Maßnahme, Information der betroffenen Personen nach Abschluss der Maßnahmen). Durch das Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes wurde der Kreis der Auskunftsberechtigten um den Militärischen Abschirmdienst erweitert und die Prüfungszuständigkeit der G10-Kommission auf die Eingriffe in das Brief-, Post- und Fernmeldegeheimnis beschränkt (hierzu Bertold Huber, Das Bankgeheimnis der Nachrichtendienste, NJW 2007, 81 ff., der diese Kontrollreduktion für rechtsstaatlich bedenklich hält). Ob die Regelung mit der Rechtsprechung des BVerfG vereinbar ist (vgl. nur Beschluss vom 4. Februar 2005 - 2 BvR 308/04, CR 2005, 799, 800), ist noch ungeklärt.

Berufsfreiheit und informationelle Selbstbestimmung in ihrer Freiheits- und Zugangskomponente sind berührt bei Datenzugriffen auf Berufsgeheimnisträger. Bei der Überwachung des Mobiltelefonanschlusses (BVerfG, Kammerbeschluss vom 18. April 2007 - 2 BvR 2094/05, NJW 2007, 2749) sowie der sonstigen Telefonüberwachung eines Strafverteidigers (BVerfG, Kammerbeschluss vom 30. April 2007 - 2 BvR 2151/06, NJW 2007, 2753) steht der abwehrende Datenschutz, bei der Durchsuchung und Beschlagnahme in Verfahren gegen Presseangehörige, um deren Informanten zu ermitteln (BVerfG, Urteil vom 27. Februar 2007 - 1 BvR 538/06, NJW 2007, 1117), der Zugangsschutz im Vordergrund.

2. Hessischer Datenschutzbeauftragter

2.1 Daseinsvorsorge

Bereits in meinem 33. Tätigkeitsbericht habe ich dargelegt, weshalb sich die Kontrollbefugnis des Hessischen Datenschutzbeauftragten auf den gesamten Bereich staatlich gewährleisteter Daseinsvorsorge erstreckt, und dies unabhängig davon, wie, in welcher Rechtsform und von wem die Aufgaben der Daseinsvorsorge wahrgenommen werden. 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).

2.1.1 Flughafen Frankfurt

Eine originäre staatliche Aufgabe ist es, die für das Funktionieren der Industriegesellschaft unentbehrliche Verkehrsinfrastruktur zu gewährleisten. Im Zeitalter des Massentourismus gilt das auch für die Errichtung und den Betrieb von Verkehrsflughäfen (OLG Frankfurt, Urteil vom 30. August 1996 - 1 HEs 196/96, NStZ 1997, 200; LG Frankfurt, Urteil vom 13. Mai 1996 - 5/12 Qs 14/56, NStZ-RR 1996, 259). Eine ausgewogene und funktionierende Flughafenlandschaft mit guten verkehrlichen Anbindungen liegt im Interesse der Allgemeinheit (VGH Baden-Württemberg, Urteil vom 28. Februar 2005 - 8 S 2004/04, VBlBW 2005, 351, 354). Am Luftraum als Verkehrsweg besteht Gemeingebrauch. Der Gemeingebrauch setzt sich mit Rücksicht auf den Flugplatzzwang in der Nutzung der Verkehrsflughäfen und -plätze fort. Was insbesondere die Verkehrsflughäfen im Land Hessen angeht, hat das Bundesverwaltungsgericht für den Flughafen Frankfurt in der Startbahn-West-Entscheidung vom 7. Juli 1978 (4 C 79.76 u.a., BVerwGE 56, 119) zwar einerseits betont, dass die Errichtung und der Betrieb von Verkehrsflughäfen auch eine unternehmerische Entscheidung ist. Es qualifizierte Verkehrsflughäfen gleichwohl als Einrichtungen, mit denen öffentliche Zwecke verfolgt werden, zu deren Gunsten etwa eine gemeinnützige Planung betrieben werden kann. Verkehrsflughäfen haben daher zumindest auch Anstaltcharakter. Eine Anstalt des öffent-

lichren Rechts ist nach der klassischen Begriffsbestimmung "ein Bestand von Mitteln, sächlicher wie persönlicher Art, welche in der Hand eines Trägers öffentlicher Verwaltung einem besonderen öffentlichen Zeck dauernd zu dienen bestimmt sind." (Otto Mayer, Deutsches Verwaltungsrecht Bd. 2, 3. Aufl., 1924, S. 268). Der weite Anstaltbegriff gilt als "Sammelbecken" für unterschiedliche organisationsrechtliche Erscheinungen und erfasst alle organisatorischen Subjekte öffentlicher Verwaltung, die nicht Körperschaften und Stiftungen sind (Kemmler, Die Anstaltslast, 2001, S. 30 f.). Daseinsvorsorge und unternehmerische Betätigung liegen in Gemengelage. Das lässt es geboten erscheinen, den anstaltlichen Teil des Verkehrsflughafens dem öffentlichen Bereich zuzuordnen. Die Leistungen sowie personelle und sächliche Organisation dieses anstaltlichen Teils haben nach öffentlich-rechtlichen Kriterien zu erfolgen. Die Fraport AG unterliegt damit meiner datenschutzrechtlichen Kontrolle, soweit sie sich als Betreiberin des Flughafens Frankfurt betätigt.

2.1.2 Flughafen Frankfurt-Hahn

Da die Flughafen Hahn GmbH einen Annexbetrieb der Fraport AG darstellt, ist davon auszugehen, dass die Fraport AG auch den Flughafen Frankfurt-Hahn betreibt. Die Erfüllung einer öffentlichen Daseinsvorsorgeaufgabe in einem anderen Bundesland, ändert nichts an den datenschutzrechtlichen Zuständigkeiten. Im Interesse einer einheitlichen Kontrolle ist (entsprechend den bundesstaatlichen Nacheilegrundsätzen) mit Zustimmung der Datenschutzbehörde des Landes Rheinland-Pfalz von einer Annexzuständigkeit des HDSB auszugehen.

2.2 Public Private Partnerships

Im 35. Tätigkeitsbericht wurden unter Ziff. 2 diese Erwägungen auf den Bereich der Public Private Partnerships (PPP) oder Öffentlich-Privater Partnerschaften übertragen, die sich steigender Beliebtheit erfreuen. Es wurde schon erwähnt, dass unter dieser Bezeichnung die unterschiedlichsten Kooperationsformen von Hoheitsträgern mit privaten Wirtschaftssubjekten zusammengefasst sind. Trotz einer Tendenz zur Risikoabwälzung auf die privaten Partner, geht es doch immer um die Erfüllung öffentlicher Aufgaben. Auch wenn die Privaten (zunächst) die Aufgabenfinanzierung übernehmen und eine (formelle) Privatisierung eintritt, bleibt die Aufgabe öffentlich. In den Kategorien des klassischen deutschen Verwaltungsrechts liegt eine "Verwaltungsmittlung" vor. Die Verwaltungsmittlung ist neben der Beleihung und der Verwaltungshilfe die dritte Form der Beteiligung von Privaten an der Erfüllung von Verwaltungsaufgaben.

2.2.1 Beleihung

Beleihung bedeutet die Übertragung von Hoheitsbefugnissen. Da der Beliehene die gleichen Befugnisse wie eine Behörde wahrnimmt, muss er datenschutzrechtlich auch wie eine staatliche Behörde behandelt werden. Die Rechtsbeziehungen der Beliehenen zu Dritten betreffen den öffentlichen Bereich. Die Kontrollzuständigkeit des HDSB für die Beliehenen des Landes Hessen ist unstreitig gegeben (§ 3 Abs. 1 Satz 2 HDSG).

2.2.2 Verwaltungshilfe

Bei der Verwaltungshilfe führt der Private nach Würdigung der Behörde Hilfstätigkeiten aus. Solche Tätigkeiten können auch das Außenverhältnis, d.h. Rechtsbeziehungen zu Dritten betreffen (z. B. Abschleppen von Fahrzeugen durch Privatunternehmen auf polizeiliche Anweisung). Die rechtliche Zuordnung der jeweiligen Leistungsverhältnisse kann hier Verwirrung stiften. Da der Verwaltungshilfevertrag als fiskalisches Hilfsgeschäft dem Privatrecht zugewiesen wird, soll nach gelegentlich vertretener Auffassung auch das Leistungsverhältnis des Verwaltungshelfers zu Drittbetroffenen dem privaten Bereich zugehören. Zwischen dem Verwaltungshelfer und den Drittbetroffenen bestehen indessen überhaupt keine Leistungsbeziehungen. Rechtlich handelt im Außenverhältnis vielmehr die Behörde. Die Kontrollzuständigkeit des HDSB versteht sich daher von selbst. Datenschutzrechtlich ist dies der klassische Fall der Datenverarbeitung im Auftrag (§ 4 HDSG).

2.2.3 Verwaltungsmittlung

Während für die Verwaltungshilfe die unselbständige Aufgabenerfüllung charakteristisch ist, beauftragt bei der Verwaltungsmittlung eine Verwaltungsbehörde ein privates Unternehmen zumeist durch Vertrag mit der Durchführung einer bestimmten Verwaltungsaufgabe. Das private Unternehmen handelt hier selbständig (Stichworte: Betreibermodell, Betriebsführungsmodell, Konzessionsmodell). Die Verwaltungsmittlung fällt ebenfalls in den öffentlichen Bereich; denn hier kauft die Behörde nicht nur punktuell eine Dienstleistung ein. Vielmehr wird das private Unternehmen mit der eigenständigen Erfüllung einer öffentlichen Aufgabe betraut. Mögen die Verträge, durch die die Verwaltungsmittlung begründet wird, privatrechtlich qualifiziert werden (Abfallentsorgungsverträge, Energieversorgungsverträge, Erschließungsverträge, Konzessionsverträge), mögen die Leistungsbeziehungen zu Drittbetroffenen privatrechtlich strukturiert sein, so handelt es sich doch immer um die Erfüllung öffentlicher Aufgaben im unmittelbaren Allgemeininteresse. Das bedeutet, dass hier die Grundrechte unmittelbar gelten. Wo immer aber die informationelle Selbstbestimmung unmittelbar Geltung beansprucht, da beginnt datenschutzrechtlich der öffentliche Bereich.

3. Europa

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

3.1 Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Im Berichtszeitraum fanden fünf Sitzungen der Gemeinsamen Kontrollinstanz (GK) statt, an denen meine Mitarbeiterin als Ländervertreterin teilnahm. Die Delegationen, der zum 1. Mai 2004 der EU beigetretenen Staaten besaßen weiterhin nur einen Beobachterstatus in der Kontrollinstanz, da das Schengener Durchführungsübereinkommen (SDÜ) ihnen gegenüber noch nicht in Kraft gesetzt wurde. Dies hat sich Ende Dezember 2007 geändert, da dann SIS I Plus, d. h. die technische Erweiterung für die neuen Beitrittsländer mit Ausnahme Zyperns in Betrieb gegangen ist. Mit dem Anschluss der neuen Beitrittsländer an das SIS werden die Binnengrenzkontrollen zu Land und Wasser und ab Frühjahr 2008 die Kontrolle an den Luftgrenzen aufgehoben.

Mit der zeitgleich erfolgenden Inkraftsetzung des SDÜ für die neuen Länder erhalten diese dann auch einen vollberechtigten Mitgliedstatus in der GK.

Anders als in meinem 35. Tätigkeitsbericht (Ziff. 3.1) berichtet, will die Schweiz jetzt auch bei SIS I Plus teilnehmen, da die Realisierung von SIS II aus dortiger Sicht zu lange dauert.

Das in meinem 35. Tätigkeitsbericht unter Ziff. 3.1 angesprochene Schengen III-Abkommen, der sog. Prümer Vertrag vom 27. Mai 2005, wurde unter der deutschen Ratspräsidentschaft im ersten Halbjahr 2007 in den EU-Rechtsrahmen integriert (Entwurf eines Beschlusses des Rates zur Vertiefung der grenzüberschreitenden Zusammenarbeit insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Stand 19. Juni 2007 - CRIMORG 112, ENFOPOL 124). Dies bedeutet, dass die Regelungen des Prümer Vertrags nach den erforderlichen innerstaatlichen Umsetzungsakten in allen EU-Ländern gelten. Anders als das SIS, bei dem alle Staaten auf einen inhaltlich identischen Datenbestand Zugriff haben, verfolgt das Regelungswerk des Prümer Vertrags ein anderes Konzept, bei dem der gegenseitige Zugriff auf nationale Datenbanken (Fingerabdrücke, DNA, Fahrzeugregister) eingeräumt wird.

3.1.1 Neue Rechtsgrundlagen für das Schengener Informationssystem

Die neuen Rechtsgrundlagen für das SIS II, von denen ich in den letzten Tätigkeitsberichten (35. Tätigkeitsbericht, Ziff. 3.1.1; 34. Tätigkeitsbericht, Ziff. 3.3.1; 33. Tätigkeitsbericht, Ziff. 3.1.2) berichtet habe, sind mittlerweile veröffentlicht. Sie ersetzen insoweit die Art. 92 bis 119 SDÜ.

Da die neuen Regelungen für das SIS II auf unterschiedliche Kompetenzen in den Europäischen Verträgen gestützt werden, gibt es drei verschiedene Rechtsgrundlagen:

- Das Verfahren von Ausschreibungen von Drittausländern zur Einreiseverweigerung (Art. 96 SDÜ) und damit zusammenhängende Fragen werden in der Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) geregelt (ABlEG 2006/L 381/4).

- Der Zugriff von Kfz-Zulassungsstellen auf das SIS II ist in der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) geregelt (ABlEG 2006/L 381/1).

  Da die beiden Regelungsgegenstände Kompetenzen der ersten Säule der Europäischen Union (Visa, Asyl, Einwanderung und Verkehr) betreffen, konnte die Rechtsform der Verordnung gewählt werden, die unmittelbar in jedem Mitgliedstaat der Europäischen Union gilt.

- Alle weiteren Ausschreibungen von Personen und Gegenständen und die damit zusammenhängenden Fragen wurden durch Beschluss des Rates vom 12. Juni 2007 über die Einrichtung, Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) geregelt (ABlEG 2007/L 205/63).

Die dritte geschilderte Regelungsmaterie kann nur auf die Kompetenz für polizeiliche und justizielle Zusammenarbeit im Vertrag über die Europäische Union gestützt werden. Der hierzu ergangene Beschluss ist zwar für die Mitgliedstaaten verbindlich, aber für die Bürger nicht unmittelbar wirksam. Hierzu bedarf es der Umsetzung in nationale Rechtsvorschriften.

Inhaltlich hat sich an den Rechtsgrundlagen für das SIS II gegenüber dem Entwurfsstadium, von dem ich im 35. Tätigkeitsbericht (Ziff. 3.1.1) berichtete, nicht viel geändert. Als positiv anzumerken ist, dass - anders als damals geplant - der Zugriff von Nachrichtendiensten auf die Ausschreibungen von Drittstaatsangehörigen zur Einreiseverweigerung nicht realisiert wurde.

Durch die Veröffentlichung und das Inkrafttreten der drei neuen Rechtsgrundlagen für das SIS II steht der Wortlaut zwar fest. Anwendung finden diese aber erst, nachdem der Rat mit Zustimmung aller Mitgliedstaaten dies bestimmt. Wichtigste Voraussetzung dafür ist, dass SIS II in Echtbetrieb geht. Der Start wird allerdings immer wieder - vor allem aufgrund technischer Probleme - verzögert. Nach derzeitigem Informationsstand soll die Realisierung nun Anfang des Jahres 2009 erfolgen können.

Zur Konkretisierung und Ausfüllung der genannten Rechtsgrundlagen für das SIS II ist die Kommission dabei, Implementierungsregelungen zu erarbeiten und Änderungen des SIRENE-Handbuchs vorzunehmen. Die Gemeinsame Kontrollinstanz hat zu den Entwürfen Stellung genommen und Änderungen vorgeschlagen. Dabei ging es unter anderem um die praktische

Handhabung der Löschung von Daten, um Einschränkungen bei der Nutzung von biometrischen Daten, um Präzisierungen bei dem Begriff der "erweiterten Suche" und Einzelheiten der Protokollierung von Zugriffen anderer Behörden auf das SIS.

3.1.2 Gemeinsame Überprüfung von Ausschreibungen zur verdeckten Registrierung

Wie im 35. Tätigkeitsbericht (Ziff. 3.1.2) berichtet, hat die Gemeinsame Kontrollinstanz 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.

Die Ergebnisse der Überprüfung wurden in einem Bericht zusammengefasst, der nunmehr von den Mitgliedern der Gemeinsamen Kontrollinstanz verabschiedet wurde.

Für Deutschland sind insbesondere folgende Feststellungen wichtig:

- die Ausschreibung darf keine sogenannten Kontaktpersonen betreffen, da dies nicht mit Art. 99 Abs. 2 SDÜ zu vereinbaren ist.

- der Begriff "außergewöhnlich schwere Straftat" ist zu konkretisieren. Dabei kann auf die derzeitigen Kompetenzen für EUROPOL oder auf diesbezügliche Regelungen für den europäischen Haftbefehl zurückgegriffen werden.

- die Datenschutzbehörden sollten die Ausschreibungen regelmäßig überprüfen.

3.1.3 Überprüfung von Ausschreibungen von Drittausländern zur Einreiseverweigerung

Nach dem SDÜ dürfen nur solche Personen zur Einreiseverweigerung ausgeschrieben werden, die nicht Staatsangehörige eines der Mitgliedstaaten der Europäischen Gemeinschaft oder eines der assoziierten Staaten sind.

Anlässlich der Überprüfung, ob nach dem Beitrittsdatum der betreffenden Staaten noch rumänische und bulgarische Staatsangehörige im SIS zu finden waren, stieß man auf eine Reihe weiterer Speicherungen von EU-Staatsangehörigen. Im Januar 2007 gab es 46 unzulässig gespeicherte Ausschreibungen, die sofort gelöscht wurden.

3.2 Gemeinsame Kontrollinstanz für EUROPOL

3.2.1 Neue Rechtsgrundlagen für EUROPOL

Im 35. Tätigkeitsbericht (Ziff. 3.2.1) hatte ich berichtet, dass es Pläne für neue Rechtsgrundlagen für EUROPOL gibt. Die drei Protokolle zur Novellierung des EUROPOL-Abkommens sind mittlerweile von allen Mitgliedstaaten ratifiziert und im Frühjahr 2007 in Kraft getreten (Rechtsakt des Rates vom 30. November 2000 - ABlEG 2000/C 358/1, Rechtsakt des Rates vom 28. November 2002 - ABlEG 2002/C 312/1 - und Rechtsakt des Rates vom 27. November 2003 - ABlEG 2004/C 2/1).

Die wichtigsten Änderungen sind folgende:

- EUROPOL wird für die Ermittlung bei Geldwäsche insgesamt zuständig. Bisher war die Zuständigkeit nur dann gegeben, wenn die Geldwäsche im Zusammenhang mit Formen der Kriminalität stand, für die EUROPOL die Zuständigkeit besitzt.

- Bedienstete von EUROPOL dürfen an gemeinsamen Ermittlungsgruppen der Mitgliedstaaten teilnehmen und die dort gewonnenen Informationen verarbeiten. Ihnen stehen keine Exekutivbefugnisse zu.

- Die Voraussetzungen, unter denen Datenübermittlungen an Drittstaaten und Drittstellen erfolgen dürfen, werden erleichtert: Erstmals werden im Einzelfall Ausnahmen von dem Erfordernis zugelassen, dass ein angemessener Datenschutzstandard im Empfängerland gewährleistet sein muss. Unter der Voraussetzung, dass "der Direktor von EUROPOL es für absolut notwendig hält, um die grundlegenden Interessen der betreffenden Mitgliedstaaten im Rahmen der Ziele von EUROPOL zu wahren oder um eine unmittelbar drohende kriminelle Gefahr abzuwenden" darf davon abgesehen werden.

Parallel zu den sich jahrelang hinziehenden Ratifizierungsverfahren der Protokolle gibt es einen Entwurf zur Ersetzung des EUROPOL-Übereinkommens durch einen Ratsbeschluss. Zu dem Entwurf vom Frühjahr 2007 hat die Gemeinsame Kontrollinstanz Stellung genommen.

Wichtige Änderungen sind folgende:

- Die Beschränkung auf die Zuständigkeit von EUROPOL für Straftaten, die im Zusammenhang mit organisierter Kriminalität stehen, entfällt. Nunmehr ist EUROPOL zuständig für schwere Kriminalität allgemein (die Straftaten sind in einem Anhang aufgelistet) und für Terrorismus. Bei der Zuständigkeit für die Geldwäsche entfällt die Einschränkung in dem o.g. Protokoll, dass nur solche Vortaten in die Zuständigkeit von EUROPOL fallen, für die EUROPOL auch sonst befugt wäre. Die Gemeinsame Kontrollinstanz hatte hingegen vorgeschlagen, die Erfahrungen mit der neuen sich aus dem Protokoll ergebenden Rechtslage erst einmal abzuwarten.

- Zu den neuen Aufgaben von EUROPOL gehört auch die Unterstützung eines der Mitgliedstaaten bei Ermittlungen mit Hilfe des Internets begangener Straftaten. Diese neue Aufgabe ist auch zu sehen im Zusammenhang mit der unter der deutschen Ratspräsidentschaft im ersten Halbjahr 2007 propagierten Aktion "Check-the-Web", d.h. der verstärkten Kontrolle des Internets.

- EUROPOL darf über das Informationssystem und die Analysedateien hinaus andere Systeme zur Datenverarbeitung einsetzen oder errichten. Die Bedingungen für diese Datenverarbeitungssysteme soll der Rat festlegen können. Die Gemeinsame Kontrollinstanz hat eine präzisere Umschreibung der Voraussetzung für einen derartigen Einsatz angemahnt und darauf hingewiesen, dass sie vor dem Einsatz derartiger neuer Systeme eingeschaltet werden sollte.

- Das Recht auf Zugang des Betroffenen zu seinen Daten soll sich - wie bisher - nach nationalen Rechtsvorschriften richten. Dies führt dazu, dass EUROPOL sich mit 25 und bald 27 unterschiedlichen Regelungen der Mitgliedstaaten konfrontiert sieht und die Entscheidungen über das Zugangsrecht einer betroffenen Person im Einzelfall nicht immer in Übereinstimmung mit dem EUROPOL-Übereinkommen erfolgt. Die Gemeinsame Kontrollinstanz hat ein einheitlich geregeltes Zugangsrecht auf datenschutzrechtlich hohem Niveau vorgeschlagen.

- Positiv zu bewerten ist, dass erstmals die Bestellung eines Datenschutzbeauftragten bei EUROPOL vorgesehen ist.

Nach den jetzigen Plänen soll der Ratsbeschluss bis 30. Juni 2008 verabschiedet sein und zum 1. Januar 2010 in Kraft treten.

3.2.2 Verarbeitung der von den Mitgliedstaaten angelieferten Daten durch EUROPOL

Die Gemeinsame Kontrollinstanz wurde von EUROPOL zu dem sog. OASIS-Projekt (**O**ver-All-**A**nalysis-**S**ystem for **I**ntelligence and **S**upport) um Stellungnahme gebeten. Dabei handelt es sich um ein teilweise automatisiertes Verfahren von EUROPOL zur Sammlung und Bewertung der von den Mitgliedstaaten an EUROPOL gelieferten Daten. Es läuft derzeit bei EUROPOL in der Testphase. In der Oktobersitzung stellten Mitarbeiter von EUROPOL den Delegierten der Gemeinsamen Kontrollinstanz das Projekt vor. Nach Aussage von EUROPOL fließen derzeit ca. 76 % der von den Mitgliedstaaten angelieferten Daten nicht in Analysedateien ein. Diese Situation will man mit technischer Unterstützung in Art eines Data-Warehouse (Daten-Warenhaus) verbessern. Die Gemeinsame Kontrollinstanz sah eines der wichtigsten Probleme darin, klare Verantwortlichkeiten für diese Phase der Datenverarbeitung zu schaffen. Dies scheint jetzt dahin gelöst zu werden, dass EUROPOL zu einem früheren Zeitpunkt die Verantwortung von den Mitgliedstaaten übernimmt.

3.2.3 Kontrolle des Internets

Auch in das von EUROPOL betriebene "Check-the-Web"-Projekt wurde die Gemeinsame Kontrollinstanz eingebunden. Dieses Vorhaben wurde ebenfalls in der Oktobersitzung der Kontrollinstanz durch EUROPOL vorgestellt. Dabei geht es in einer ersten Phase zunächst um die Sammlung von öffentlich zugänglichen Informationen zu islamistischen, extremistischen Sachverhalten aus dem Internet. Diese sollen in eine Art Intranet, also ein internes Netz, gestellt werden, auf das die zuständigen Stellen der Mitgliedstaaten Zugriff haben. In einer zweiten Phase soll es um vertrauliche Informationen gehen und der Kreis der Nutzer vergrößert werden. Da seitens der Kontrollinstanz noch Informationsbedarf, insbesondere zur zweiten Phase des Projekts besteht, wird die Inspektionsgruppe "Check-the-Web" im März 2008 prüfen.

3.2.4 Kontrolle von EUROPOL

Die Gemeinsame Kontrollinstanz hat im Jahr 2007 wieder eine Kontrolle bei EUROPOL durchgeführt. Der Bericht über diese Kontrolle ist vertraulich.

4. Bund

4.1 Online-Durchsuchungen

Mit der Einführung der sog. Online-Durchsuchung begibt sich der Rechtsstaat auf einen bedenklichen Weg. Insbesondere der Schutz des Kernbereichs privater Lebensführung ist mit solchen Ermittlungsmethoden nicht zu gewährleisten.

Mit einer Entscheidung vom 31. Januar 2007 (StB 18/06) hat der BGH die heimliche Durchsuchung eines Computers im Rahmen eines Ermittlungsverfahrens abgelehnt, da dafür keine Rechtsgrundlage in der StPO existiere - weder die Bestim-

mungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung könnten zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Parallel dazu wurde in das Verfassungsschutzgesetz Nordrhein-Westfalen eine Befugnis eingefügt, die den heimlichen Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel erlauben soll. Diese Norm ist zurzeit Gegenstand eines Verfahrens vor dem BVerfG.

Seit Anfang des Jahres wird nunmehr eine heftige Diskussion darüber geführt, ob ein solches Ermittlungsinstrument überhaupt notwendig sei und wie es sich in den Katalog der vorhandenen Ermittlungsmethoden einfügt. Befürworter wollen eine entsprechende Befugnisnorm in die anstehende Novellierung des BKA-Gesetzes mit aufnehmen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im Laufe d.J. mehrmals mit dieser Thematik befasst (vgl. Ziff. 10.1 und Ziff. 10.9).

Auch ich gehe davon aus, dass sowohl die datenschutzrechtliche Praxis aber auch der Gesetzgeber technische Entwicklungen sorgfältig beobachten muss. Dazu gehört nicht zuletzt die Prüfung, ob die vorhandenen Rechtsgrundlagen den Einsatz neuer technischer Mittel, die den Ermittlungsbehörden aus taktischer Sicht sinnvoll oder gar zwingend notwendig erscheinen, zulassen. Soweit diese Frage zu verneinen ist, muss der Gesetzgeber entscheiden, ob dafür eine Rechtsgrundlage geschaffen werden soll - immer unter der Prämisse, dass die Vorgaben der Verfassung für zulässige Eingriffe in Grundrechte der Bürgerinnen und Bürger eingehalten werden können. Das bedeutet konkret eine Abwägung zwischen den Freiheitsrechten der Betroffenen - insbesondere dem Recht auf informationelle Selbstbestimmung - und der Sicherheit des Staates einschließlich der Anforderungen an eine effektive Strafverfolgung.

Nicht immer wird diese Debatte sachlich geführt: Insbesondere wurde schon zu Beginn der Diskussion von den Befürwortern des Instruments sofort eine Verfassungsänderung gefordert.

Naturgemäß legen die Sicherheitsbehörden nicht im Detail offen, wie das technische Instrumentarium ausgestaltet werden kann, das zum Einsatz kommen soll.
Einen Überblick über die verschiedenen Möglichkeiten sowie zu verschiedenen Einsatzszenarien, sind den Antworten zu entnehmen, die das Bundesinnenministerium am 22. August 2007 auf Fragenkataloge der SPD-Bundestagsfraktion sowie des Bundesjustizministeriums für eine Anhörung im Bundestag gegeben hat.

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf dieser Grundlage den Ablauf und die technischen Verfahren der geplanten Online-Durchsuchung erläutert und aus technischer Sicht bewertet. Dieses Arbeitspapier zu den technischen Aspekten der Online-Durchsuchung ist abgedruckt unter Ziff. 12.

Der Computer hat mittlerweile im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung sehr privater Informationen, wie beispielsweise Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Ein Online-Zugriff auf diese Daten berührt daher fast regelmäßig Aspekte, die den Kernbereich der privaten Lebensführung betreffen und damit einem Zugriff des Staates entzogen sind. Der notwendige Schutz dieser Daten war nicht zuletzt ein Grund für die Novellierung der Regelungen zu den verdeckten Ermittlungsmethoden in der Strafprozessordnung (vgl. dazu Ziff. 4.2).

In der Anwendungspraxis wird sich ein absoluter Schutz dieser Daten - dessen Notwendigkeit das BVerfG mehrmals hervorgehoben hat - allein durch technische Mittel, wie z.B. vorab definierte Suchkriterien kaum realisieren lassen. Suchkriterien können nie so gezielt eingesetzt werden, dass ohne Durchsuchung des Gesamtdatenbestandes und unter Ausklammerung des Kernbereichs ausschließlich nach terroristischen Aktivitäten gesucht wird. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Der Einsatz der sog. Remote-Forensic-Software wird regelmäßig zu erheblichen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung führen. Es sind deshalb an die Beurteilung der verfassungsrechtlichen Zulässigkeit einer solchen Befugnis besonders hohe Anforderungen zu stellen.

Nicht außer Acht gelassen werden darf auch, dass von Seiten der Bundesregierung das Thema E-Government vorangetrieben wird. Bürgerinnen und Bürger sowie Unternehmen werden teilweise sogar gezwungen, über das Internet mit der Verwaltung zu kommunizieren. Es wird außerdem auf die Gefahren des Internet hingewiesen, und Bürgerinnen und Bürger sowie Unternehmen werden angehalten, dafür Sorge zu tragen, dass ihre Datenverarbeitung vor unberechtigten Zugriffen und Datenklau geschützt ist. Dazu sollen z.B. Verschlüsselungsmechanismen, Firewalls und andere Sicherheitsmaßnahmen eingesetzt bzw. ergriffen werden. Es kann dann nicht Sinn staatlichen Handelns sein, dass dieser Methoden anwendet, die genau solche Sicherungen umgehen und nicht einmal über ihm bekannte Schwachstellen und Risiken informiert. Da der Staat sich aber Möglichkeiten verschafft, die Maßnahmen zu umgehen, dokumentiert er, dass ihm bekannte Sicherheitslücken existieren.

4.2 Novellierung der Strafprozessordnung

Zum 1. Januar 2008 ist die Neuordnung der verdeckten Ermittlungsmaßnahmen in der Strafprozessordnung in Kraft getreten. Gleichzeitig wurde auch die sogenannte Vorratsdatenspeicherung für sechs Monate eingeführt. Dieses Gesetzgebungsverfahren hat zu breiten öffentlichen Diskussionen geführt. Nicht in allen Bereichen wurde eine datenschutzgerechte Lösung gefunden.

Ziel des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (ABlEG 2006/L 105/54 Abs. 11) sollte ein harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden sein - so die Einleitung zum Gesetzentwurf (BTDrucks. 16/5846). Damit sollte sowohl auf technische Neuerungen als auch auf Schwierigkeiten der Strafverfolgungspraxis bei Anwendung der bisherigen Regelungen reagiert werden. Handlungsbedarf ergab sich auch aus der Rechtsprechung des BVerfG. Schließlich setzt dieses Gesetz die Richtlinie 2006/24/EG in innerstaatliches Recht um, die die Vorratsspeicherung von Daten verlangt, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt werden.

Insbesondere die sog. Vorratsdatenspeicherung hat eine intensive Debatte ausgelöst, die durch den Gesetzesbeschluss noch nicht beendet wurde. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Problematik mehrmals diskutiert und in ihren Entschließungen die Anforderungen des informationellen Selbstbestimmungsrechtes an die Ausgestaltung der Ermittlungsmaßnahmen formuliert (dazu s. Ziff. 10.3 und Ziff. 10.7).

Durch die Neuregelungen sind für verdeckte Ermittlungsmaßnahmen verfahrensrechtliche Schutzvorkehrungen getroffen worden, die dem Schutz des Rechts auf informationelle Selbstbestimmung dienen. Nicht immer geschieht dies im notwendigen Maße. Zum Teil wurden die im ursprünglichen Gesetzentwurf enthaltenen Änderungen im Rahmen der parlamentarischen Beratungen - vor allem auf Verlangen der Forderungen des Bundesrates - wieder abgeschwächt. Dies gilt etwa für die Berichte über die angeordneten Maßnahmen. Diese sind weiterhin nicht so differenziert, dass sie Grundlage einer effektiven Evaluierung sein können.

4.2.1 Überwachung der Telekommunikation

Zwar erfolgt eine Fülle von Änderungen in den Regelungen zu Eingriffen in das Telekommunikationsgeheimnis, allerdings ergeben sich nur begrenzt Veränderungen im sachlichen Anwendungsbereich. Auch nach der Neuregelung ist der Katalog von Straftaten, die zum Einsatz von Maßnahmen der Telekommunikationsüberwachung führen können, sehr umfangreich. Ein gewisses Korrektiv zur Schwere des Grundrechtseingriffs ergibt sich aus der im Gesetz formulierten Beschränkung, dass auch im Einzelfall die Tat schwerwiegen muss. Inwieweit dies die Zahl der Überwachungsmaßnahmen beeinflussen kann, wird erst die zukünftige Praxis ergeben. Die dafür notwendigen Informationen werden jedoch auch weiterhin nur begrenzt zur Verfügung stehen.

Die Regelung zur Berichterstattung über angeordnete Telekommunikationsüberwachungsmaßnahmen enthält weiterhin keine Angaben dazu, ob die Überwachungsmaßnahme Ergebnisse gebracht hat, die für das weitere Verfahren relevant sind. Dies wäre aber Voraussetzung für sinnvolle Evaluierungsprojekte. Zwar hat nunmehr der Staatsanwalt nach Abschluss der Maßnahme dem Gericht über den Verlauf und die Ergebnisse zu berichten. Allerdings bleibt im Gesetz offen, welche Konsequenzen aus diesem Bericht zu ziehen sind. Die in der Begründung des Gesetzentwurfs (BTDrucks. 16/5846 S. 48) genannte Möglichkeit einer Erfolgskontrolle, um die daraus resultierenden Erfahrungen bei künftigen Entscheidungen berücksichtigen zu können, erscheint sehr vage.

Im Gesetz ist nach dem Wortlaut des § 100a Abs. 4 StPO ein Kernbereichsschutz formuliert.

§ 100a Abs. 4 StPO

Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Abs. 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Abs. 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

Dass schon vor der Maßnahme deutlich ist, dass alle Gespräche dem Kernbereich privater Lebensführung zuzurechnen sind, ist wohl eher die Ausnahme. Bei einer Vielzahl von Überwachungsmaßnahmen wird nicht ausgeschlossen sein, dass zumindest auch kernbereichsrelevante Gespräche geführt werden. Auch die in der Diskussion immer wieder aufgeworfene Frage, wie zu reagieren ist, wenn wirklich höchst persönliche Gespräche geführt werden, ist nur begrenzt gelöst. Das Gesetz geht offensichtlich davon aus, dass dies grundsätzlich vorkommen kann und auch auf die eigentliche Maßnahme keinen Einfluss haben soll, d.h. die Erhebung solcher Informationen wird vom Gesetzgeber ausdrücklich in Kauf genommen. Insoweit spielt natürlich auch eine Rolle, dass in der Regel die Überwachung der Telekommunikation nicht in Echtzeit direkt abgehört wird, sondern zunächst (nur) technisch aufgezeichnet wird. Allerdings wird immerhin ein absolutes Verwertungsverbot ausgesprochen.

Weiterhin nicht im Gesetz klargestellt wurde, was mit den Daten geschieht, die aufgrund der Eilkompetenz der Staatsanwaltschaft erhoben wurden, dann aber die nachträgliche richterliche Genehmigung der Maßnahme versagt wird. In diesen Fällen ist eigentlich davon auszugehen, dass die richterliche Anordnung auch zum Zeitpunkt der Eilandordnung nicht ergangen wäre - damit hätten die Daten nicht erlangt werden können. Die Datenschutzbeauftragten hatten verlangt, dann sollten diese vernichtet werden. Jetzt bleibt es bei der Verschiebung auf den erkennenden Richter - ob die Daten verwertet werden - obwohl die Grundlage für die Erhebung weggefallen ist. Der Gesetzentwurf der Bundesregierung hatte hier noch die Verwertung der zwischenzeitlich erlangten Daten beschränkt auf die Fälle, in denen Gefahr im Verzug bestand. Die zunächst vorgesehene Entscheidung durch das im Rechtszug übergeordnete Gericht über eine Verlängerung der Anordnung über den Zeitraum von sechs Monaten hinaus wurde im Laufe des Gesetzgebungsverfahrens wieder gestrichen.

Auch die Neuregelung der Benachrichtigungspflichten kann nicht alle Defizite der bisherigen Regelungen beseitigen. So sind über das Abhören von Wohnungen z.B. die "erheblich mitbetroffenen Personen" zu benachrichtigen. Es fehlen jegliche Konkretisierungen zur Bestimmung dieses Begriffs.

Auch die sich an eine Benachrichtigung anschließende Frist von nur 14 Tagen, um die Rechtmäßigkeit der Maßnahme überprüfen zu lassen, erscheint kurz. Häufig wird der Benachrichtigte davon überrascht sein. Dann hat er kaum Zeit, etwa sich anwaltlich beraten zu lassen, ob er die Möglichkeit der Überprüfung wahrnehmen soll.

Dies sind nur einige Beispiele, wie der Gesetzgeber die Gelegenheit ungenutzt gelassen hat, eine ausgewogene Abwägung zwischen dem Recht auf informationelle Selbstbestimmung und der Gewährleistung einer effektiven Strafverfolgung zu treffen.

4.2.2 Schutz von Berufsgeheimnisträgern

Systematisch neu geregelt wurde der Schutz von Berufsgeheimnissen. Dazu wurde ein § 160a neu in die StPO eingeführt, der für alle Ermittlungsmaßnahmen gilt, von denen Personen betroffen sind, die aufgrund ihrer beruflichen Tätigkeit ein Zeugnisverweigerungsrecht haben.

§ 160a StPO

(1) Eine Ermittlungsmaßnahme, die sich gegen eine in § 53 Abs 1 Satz 1 Nr. 1, 2 oder Nr. 4 genannte Person richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Abs. 1 Nr. 1, 2 oder Nr. 4 genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte.

(2) Soweit durch eine Ermittlungsmaßnahme eine in § 53 Abs. 1 Satz 1 Nr. 3 bis 3 b oder Nr. 5 genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit besonders zu berücksichtigen; betrifft das Verfahren keine Straftat von erheblicher Bedeutung, ist in der Regel nicht von einem Überwiegen des Strafverfolgungsinteresses auszugehen. Soweit geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken. Für die Verwertung von Erkenntnissen zu Beweiszwecken gilt Satz 1 entsprechend.

(3) Die Absätze 1 und 2 sind entsprechend anzuwenden, soweit die in § 53a Genannten das Zeugnis verweigern dürften.

(4) Die Absätze 1 bis 3 sind nicht anzuwenden, wenn bestimmte Tatsachen den Verdacht begründen , dass die zeugnisverweigerungsberechtigte Person an der Tat oder an einer Begünstigung, Strafvereitelung oder Hehlerei beteiligt ist. Ist die Tat nur auf Antrag oder nur mit Ermächtigung verfolgbar, ist Satz 1 in den Fällen des § 53 Abs. 1 Satz 5 anzuwenden, sobald und soweit der Strafantrag gestellt oder die Ermächtigung erteilt ist.

(5) Die §§ 97 und 100c Abs. 6 bleiben unberührt.

Zukünftig wird differenziert zwischen Geistlichen, Verteidigern und Abgeordneten einerseits sowie den anderen einem beruflichen Zeugnisverweigerungsrecht unterliegenden Gruppen. Grundsätzlich halte ich eine solche Differenzierung nicht für ausgeschlossen. Das Vertrauensverhältnis - das mit dem jeweiligen Zeugnisverweigerungsrecht geschützt werden soll - ist ja auch unterschiedlich verankert. Schließlich gibt es auch keine absolute Gleichsetzung von Vertrauensverhältnissen im Rahmen der Strafbarkeit von Verletzung von Privatgeheimnissen mit dem Kreis der Gruppen, die auch ein Zeugnisverweigerungsrecht im Strafverfahren haben. Ob die getroffene Differenzierung in der Praxis zu sachgerechten Ergebnissen führt, wird sich zeigen müssen.

4.2.3 Vorratsdatenspeicherung

Das Gesetz greift zunächst die von der EG-Richtlinie 2006/24/EG vorgegebene Mindestspeicherfrist der Verbindungsdaten von sechs Monaten auf. Andererseits geht es aber auch über die Vorgaben der Richtlinie, diese Daten zur Ermittlung, Feststellung und Verfolgung von schweren Straftaten einzusetzen, hinaus. Dies gilt insbesondere für die Verwendungsmöglichkeiten der gespeicherten Daten. Im Telekommunikationsgesetz ist die Verwendung nicht auf bestimmte Straftaten beschränkt. Zusätzlich ist auch eine Verwertung dieser Daten für Zwecke der Gefahrenabwehr sowie für die Nachrichtendienste möglich.

Zwar gilt die Speicherungspflicht nur für jeweils die Verbindungsdaten, die der Anbieter auch für eigene Zwecke verarbeitet, aber dies ist im Kontext der Verpflichtung über die vom Betreiber zu speichernden Daten über Anschlusskennungen und Anschlussinhaber zu sehen. Diese Grunddaten sind auch dann zu speichern, wenn sie für betriebliche Zwecke des Providers nicht benötigt werden. Damit wird in aller Regel jegliche Kommunikation auch im Internet nachvollziehbar sein.

Gegen das Gesetz - insbesondere aufgrund der Verpflichtung zur Vorratsdatenspeicherung - sind eine Vielzahl von Verfassungsbeschwerden anhängig.

4.3 Reform des Personenstandsrechts - technische Umsetzung der automatisierten Registerführung

Mit dem Inkrafttreten des Gesetzes zur Reform des Personenstandsrechts ist das Personenstandsregister künftig automatisiert zu führen. Um sicherzustellen, dass über einen Zeitraum von mehr als 100 Jahren verlässlich Auskünfte gegeben werden können, sind hohe Anforderungen an die technische Umsetzung zu stellen.

Das Gesetz zur Reform des Personenstandsrechts (PStRG) vom 19. Februar 2007 (BGBl. I S. 122) beinhaltet als wesentliche Änderung, dass die früheren Personenstandsbücher ab dem 1. Januar 2009 als automatisierte Personenstandsregister zu führen sind. Das gilt sowohl für das eigentliche "Hauptregister" als auch für das Sicherungsregister.

§ 3 Abs. 2 Satz 2 PStRG

Die Personenstandsregister werden elektronisch geführt.

§ 4 Abs. 1 PStRG

Die Beurkundungen in einem Personenstandsregister sind nach ihrem Abschluss (§ 3 Abs. 2) in einem weiteren elektronischen Register (Sicherungsregister) zu speichern.

Der Gesetzentwurf der Bundesregierung vom 15. Juni 2006 (BTDrucks. 16/1831) enthielt in § 3 Abs. 2 Satz 3 noch die Vorgabe, dass jede Beurkundung mit der dauerhaft überprüfbaren qualifizierten elektronischen Signatur des Standesbeamten zu versehen ist. In der Begründung zur Führung der Personenstandsregister hieß es dazu:

§ 3 Abs. 2 Satz 3

Der Entwurf sieht vor, dass die in § 3 bezeichneten Personenstandsregister "elektronisch" geführt werden. Das bisherige Papierbuch gehört damit der Vergangenheit an. Ausschlaggebend für den Sinneswandel gegenüber dem noch am Papierbuch festhaltenden Vorentwurf von 1996 ist die fortschreitende Entwicklung auf dem Gebiet der elektronischen Medien mit neuen Sicherungsmöglichkeiten …. Das vorstehend angesprochene neue Sicherungselement ist der jeweilige Abschluss beurkundender Eintragungen mit der "dauerhaft überprüfbaren qualifizierten Signatur" des Standesbeamten.

Bedauerlicherweise ist dieser Satz 3 des § 3 Abs. 2 im Zuge der Bundesratsbeteiligung gestrichen worden.

Das verabschiedete Gesetz gibt keine näheren Vorgaben zur Umsetzung des automatisierten Registers, sondern bestimmt in § 73, dass dies in einer bundesrechtlichen Verordnung geregelt werden soll.

Im Frühjahr 2007 wurde mit den Vorarbeiten für eine Technische Personenstandsverordnung (TPStV) begonnen. Das HMDIS hat meine Dienststelle dankenswerterweise von Beginn an in die Überlegungen für die Vorgaben der technischen Umsetzung der automatisierten Personenstandsregister miteinbezogen.

In dem Entwurf der TPStV vom 17. Oktober 2007 war die Verwendung der qualifizierten elektronischen Signatur für den beurkundenden Standesbeamten vorgesehen. Das begrüße ich sehr. In einigen Punkten sehe ich jedoch noch Änderungsbedarf.

Das Personenstandswesen ist der Anker für wichtige gesellschaftliche und rechtliche Anliegen der Bürger und des Staates. Fragen der Herkunft und damit einhergehende rechtliche Konsequenzen im Erbrecht und anderen Gebieten betreffen den Bürger direkt. Das Personenstandswesen muss für solche Fragen mehr als hundert Jahre verlässliche Auskunft geben können. Aber auch der Staat baut auf diese Daten auf. Neben den Meldedaten betrifft es insbesondere die Ausstellung von Ausweisdokumenten. Wenn die Dokumente aus dem Personenstandswesen keine zutreffenden Informationen bieten, sind die Ausweisdokumente folglich auch fehlerhaft. Sie können trotz hoher Fälschungssicherheit und Zuordnung zur Person, für die der Ausweis ausgestellt wurde, falsch sein. Aus all diesen Gründen nimmt das Personenstandswesen nach meiner Auffassung einen herausragenden Stellenwert ein. Dies muss bei der Umsetzung des Gesetzes durch die TPStV Berücksichtigung finden.

Damit die elektronischen Daten für einen möglichst langen Zeitraum zur Verfügung stehen, hatte das HMDIS Überlegungen zu einer möglichen Umsetzung des Gesetzes in einer hessischen Arbeitsgruppe erarbeitet, zu der ich ebenfalls gehörte. Diese Vorarbeit und das Ergebnis des Projekts "Archisafe" lassen eine Lösung sinnvoll erscheinen, die von dem in dem Entwurf formulierten Ansatz XML-basierter Register abweicht. Ich halte das "Kombimodell PDF/A plus XML" für die richtige Lösung. In diesem Fall werden die Dokumente selbst als pdf-Dokumente und die Metadaten im XML-Format gespeichert. Metadaten sind u.a. die wesentlichen Informationen aus dem Dokument (Name, Geburtsdatum usw.) und Informationen zur Erstellung und Verwendung des Dokumentes. Mit dem pdf-Format können insbesondere die Anforderungen an die qualifizierte Signatur der Dokumente, als auch an eine korrekte Darstellung der Dokumente gut erfüllt werden. Die Metadaten erlauben es, die Register einfach in automatisierte Verwaltungsabläufe zu integrieren.

In einem Punkt habe ich jedoch weiter erhebliche Zweifel, dass das Konzept der Führung der Personenstandsregister den richtigen Weg beschreibt. Ich halte die Festlegung auf eine ausschließlich elektronische Langzeitarchivierung für falsch. Es gibt noch keine Erfahrungen, für welche Zeiträume elektronische Dokumente tatsächlich verkehrsfähig, also insbesondere lesbar, vorgehalten werden können. Angesichts der herausragenden Bedeutung der Dokumente sollte man sich ohne positive Erfahrungen nicht für diesen Weg entscheiden. Es ist nach meiner Meinung zum jetzigen Zeitpunkt unverzichtbar, analog der im Entwurf vorgesehenen Regelung zu Sammelakten eine Archivierung zu Sicherheitszwecken mit Mikrofilm oder vergleichbar sicherem Medium auch für das Register vorzuschreiben oder zumindest zuzulassen. Dafür werde ich mich im weiteren Verfahren einsetzen.

Ich werde weiterhin das Verfahren begleiten und hoffe, dass die gute Zusammenarbeit mit dem HMDIS zu einem für den Bürger guten Ergebnis führt.

5. Land

5.1 Querschnitt

5.1.1 Probleme in der Anwendung der Vorschriften des Hessischen Datenschutzgesetzes

Die Zentralisierungs- und Vereinheitlichungstendenzen im Land und darüber hinaus haben deutlich werden lassen, dass zum einen Vereinfachungsbedarf bei den Vorschriften des Hessischen Datenschutzgesetzes besteht, zum anderen die Vorschriften an neue Sachverhalte angepasst werden müssen.

5.1.1.1 Verantwortung bei Verfahren, über deren Einsatz bzw. Ausgestaltung zentral entschieden wird

5.1.1.1.1 Vorabkontrolle und Verfahrensverzeichnis

Bei der Novellierung des Hessischen Datenschutzgesetzes 1998 hatte man zwar vorhergesehen, dass über den Einsatz eines Verfahrens und dessen Modalitäten nicht die Daten verarbeitende Stelle, sondern eine übergeordnete Stelle entscheidet. Das ganze Ausmaß der Auswirkungen zentraler Entscheidungen über einzusetzende Verfahren, deren Technik und die Kompetenzkonzentration, wie es inzwischen anzutreffen ist, konnte aber seinerzeit noch nicht überblickt werden.

Deshalb sind im HDSG zwar z.B. die Pflichten zur Erstellung des Verfahrensverzeichnisses (§ 6 Abs. 1) sowie zur Durchführung der Vorabkontrolle (§ 7 Abs. 6) nicht mehr den Daten verarbeitenden Stellen, sondern denjenigen auferlegt, die für den Einsatz des Verfahrens zuständig sind.

In der EG-Datenschutzrichtlinie wird weder der Begriff "Daten verarbeitende" noch der Begriff "zuständige" Stelle verwendet. Hier ist vielmehr von dem "für die Verarbeitung Verantwortlichen" die Rede. Die Richtlinie definiert diesen Begriff in Art. 2d) als "jede natürliche oder juristische Person oder Behörde, Einrichtung und jede andere Stelle, die allein oder gemeinsam mit anderen über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet" und lässt es zu, in Rechts- oder Verwaltungsvorschriften die Zwecke und Mittel festzulegen wie auch die Kriterien für die Bestimmung des Verantwortlichen. Nach der Begründung für die Formulierung ist verantwortlich diejenige Person resp. Stelle, die in letzter Instanz für die Entscheidungen über die Definition und die Durchführung der Verarbeitung verantwortlich ist und nicht um Personen, die die Verarbeitung gemäß den Weisungen des Verantwortlichen vornehmen. Der Begriff des für die Verarbeitung Verantwortlichen ist dabei bewusst prozessorientiert konzipiert (vgl. Ehmann/Helfrich, EG-Datenschutzrichtlinie, Kurzkommentar, Art. 2 Rdnr. 43 f.). Zu Recht weist auch Dammann darauf hin, dass der in der EG-Datenschutzrichtlinie verwendete Begriff bewusst funktional angelegt ist: Wenn unterschiedliche Stellen über die Zwecke und Mittel der Datenverarbeitung zu entscheiden haben, sind diese nebeneinander als Verantwortliche der Verarbeitung anzusehen (Dammann/Simitis, Art. 2 Rdnr. 13). Nach der tatsächlichen Verantwortungsverteilung treffen daher die datenschutzrechtlichen Verpflichtungen - wie diejenige zur Erstellung des Verfahrensverzeichnisses - nicht immer nur eine Person oder Stelle, sondern mehrere jeweils für den von ihnen verantworteten Teil.

Die Formulierung der EG-Datenschutzrichtlinie ist besser für die neuern Entwicklungen geeignet als die "Daten verarbeitende Stelle", der bis dahin nach den in Deutschland geltenden Datenschutzgesetzen generell die Pflichten nach den Datenschutzgesetzen auferlegt waren. Deshalb können auch Gesetzestexte nicht überzeugen, die wie im Bund, in Bremen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt und im Saarland zwar den Begriff der verantwortlichen Stelle aus der EG-Datenschutzrichtlinie übernehmen, diesen aber unter Bezug auf die Daten verarbeitende Stelle definieren (vgl. z.B. § 2 Abs. 3 Nr. 1 BDSG: "Im Sinne dieses Gesetzes ist verantwortliche Stelle jede der in § 1 Abs. 2 genannten Stellen, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt.").

Obwohl in Hessen nicht der Begriff der verantwortlichen Stelle gewählt wurde, sondern auf die Zuständigkeit Bezug genommen wird, ist auch damit ein Ansatz gewählt, der einen funktionalen Hintergrund hat. Schon jetzt obliegt deshalb der Stelle, die über den Einsatz entscheidet oder diesen vorschreibt, die Erstellung von Vorabkontrolle und Verfahrensverzeichnis - soweit diese durch die Entscheidung vorbestimmt sind. Regelmäßig umfasst eine solche Entscheidung nicht alle Einzelheiten der Ausgestaltung in jeder Dienststelle, sondern es werden z.B. mit der Auswahl des Verfahrens oder in Einsatzkonzepten Bedingungen vorgegeben, von denen die einzelne Dienststelle gar nicht abweichen darf. Bei solcher Art verteilter Verantwortung ist jede Stelle für den ihrer Entscheidungskompetenz unterliegenden Bereich zuständig. Deshalb ist von jeder Stelle der Teil des Verfahrensverzeichnisses zu erstellen, der ihrer Entscheidungskompetenz entspricht. Ebenso ist die Vorabkontrolle auf Basis der zentralen Vorgaben zu erstellen. Beides ist so jedoch nicht vollständig, sondern nur in der Form eines Musters möglich, das von den Stellen vor Ort um die jeweiligen individuellen Angaben zu ergänzen ist. Ein Beispiel für eine solche Praxis ist das Verfahrensverzeichnis für das einheitlich in der Hessischen Landesverwaltung eingesetzte Verfahren zur Unterstützung der Personaladministration SAP R/3 HR. Hier sind die zentralen Vorgaben in ein Muster-Verfahrensverzeichnis eingesetzt, das um die von den Dienststellen vor Ort zu treffenden Angaben - wie z.B. die Vergabe der Berechtigungen in der Dienststelle - zu ergänzen ist. Bei der Vorabkontrolle ist ein Beispiel die für den Einsatz von DOMEA durchgeführte zentrale Vorabkontrolle, die ebenfalls um die Ausgestaltung vor Ort und das darauf basierende Votum ergänzt werden muss.

Gleichwohl wäre im Gesetzestext des HDSG eine Anpassung an die Begriffe und Definitionen der EG-Datenschutzrichtlinie wünschenswert, um Unsicherheiten bei der Interpretation zu beseitigen. Zwar entscheidet meist die für den Einsatz des Verfahrens zuständige Stelle (z.B. das Ressort für Verfahren im nachgeordneten Bereich) über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten und ist damit zugleich verantwortliche Stelle im Sinne der EG-Datenschutzrichtlinie. Es gibt inzwischen aber auch kompliziertere Strukturen, in denen zentrale Gremien wie ein Kabinettsausschuss oder die Gesamtprojektleitung entscheiden, wobei die Kosten des Einsatzes der Verfahren teilweise zentral

finanziert werden, teilweise aber auch aus den Ressorthaushalten zu tragen sind. Bei diesen Entscheidungsstrukturen passen die gängigen Zuständigkeitsbegriffe nur schwer. Datenschutzrechtlich muss die entscheidende Stelle die Verantwortung soweit tragen wie die Entscheidung die Datenverarbeitung vorbestimmt. Da in den Begriffsbestimmungen in § 2 HDSG nach wie vor nur die Daten verarbeitende Stelle definiert ist, bietet es sich an, künftig hier auch den Begriff der verantwortlichen Stelle zu erläutern.

5.1.1.1.2 Auftragsdatenverarbeitung

Probleme bereiten die Fälle, in denen eine übergeordnete Stelle, z.B. das Ressort für die ihm nachgeordneten Stellen oder gar das Kabinett für die gesamte Landesverwaltung nicht nur die Entscheidung über den Einsatz eines Verfahrens getroffen hat, sondern die einzelnen Dienststellen auch zur Nutzung zentraler Stellen oder Auftragnehmer verpflichtet.

Adressat der Pflichten bei der Datenverarbeitung im Auftrag nach § 4 HDSG ist nämlich nicht die verantwortliche oder wie bei der Vorabkontrolle oder dem Verfahrensverzeichnis die zuständige, sondern nach wie vor die Daten verarbeitende Stelle. Nach § 2 Abs. 3 HDSG ist dies diejenige Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt, also die jeweilige Dienststelle, die ihre Aufgaben mit Hilfe dieser Verarbeitung erledigt.

§ 4 Abs. 1 und 2 HDSG

(1) Die Daten verarbeitende Stelle bleibt für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz sowie für die Erfüllung ihrer sich aus § 8 ergebenden Pflichten auch dann verantwortlich, wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(2) 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.

Die im April 2007 in Kraft getretene Änderung des DV-VerbundG eröffnet nunmehr die Möglichkeit für die Landesregierung oder die jeweils zuständige Landesbehörde, der HZD für zentrale oder gemeinsame Verfahren Aufträge nach § 4 HDSG zu erteilen.

§ 1 Abs. 1 und 2 DV-VerbundG

(1) Die Hessische Zentrale für Datenverarbeitung ist zentraler Dienstleister für Informations- und Kommunikationstechnik für alle Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes Hessen. Sie arbeitet mit den Kommunalen Gebietsrechenzentren zusammen.

(2) Die Hessische Zentrale für Datenverarbeitung kann durch die Landesregierung oder die jeweils zuständige Landesbehörde bei zentralen oder sonstigen gemeinsamen Verfahren beauftragt werden, verbindlich für alle beteiligten Stellen des Landes den Betrieb des Verfahrens zur automatisierten Datenverarbeitung als Auftragnehmerin im Sinne des § 4 des Hessischen Datenschutzgesetzes durchzuführen.

Die amtliche Begründung zu § 1 Abs. 2 DV-VerbundG (LTDrucks. 16/6058, S. 7) führt aus:

"Bei landeseinheitlichen dienststellenübergreifenden IT-Verfahren (z.B. SAP, DOMEA), welche zentral konzipiert, entwickelt und gepflegt und in mehreren beteiligten Stellen eingesetzt werden, sind diese Stellen als Daten verarbeitende Stellen im Sinne des § 2 Abs. 3 des Hessischen Datenschutzgesetzes (HDSG) durch Organisationsanweisungen und Standardisierungsvorgaben der verantwortlichen Behörden zum Einsatz und zur Anwendung der entsprechenden Verfahren verpflichtet. Zur Gewährleistung eines einheitlichen und qualitätsgesicherten Verfahrenseinsatzes ist in der Regel der Betrieb der Verfahren durch einen für alle beteiligten Stellen tätigen Auftragnehmer vorzusehen. Durch die vorgeschlagene Regelung wird diese Aufgabe typischerweise der HZD als dem zentralen IT-Dienstleiter des Landes Hessen bei entsprechender Beauftragung durch die Landesregierung oder die jeweils zuständige Landesbehörde übertragen."

Findet eine solche Beauftragung statt, so ist damit nicht mehr die einzelne Daten verarbeitende Stelle Auftraggeber, sondern der jeweilige zentrale Auftraggeber (Landesregierung oder zuständige Landesbehörde). Damit treffen die Pflichten (Auswahl des Auftragnehmers, Vertragsabschluss, Prüfung der technischen und organisatorischen Maßnahmen beim Auftragnehmer) nach § 4 HDSG diesen zentralen Auftraggeber. Er muss z.B. die Weisungen für die Datenverarbeitung erteilen, und der Auftragnehmer hat Hinweise nach § 4 Abs. 1 Satz 3 HDSG an ihn zu richten. Durch den Wortlaut des § 4 Abs. 1 Satz 1 HDSG verbleibt gleichwohl die Verantwortung für die Einhaltung des Datenschutzes bei der Daten verarbeitenden Stelle, in deren Hand allerdings die Vereinbarungen mit dem Auftragnehmer nicht liegen. Auch hier wäre es sinnvoll, diese Pflicht der jeweils verantwortlichen Stelle aufzuerlegen.

Eine solche Änderung im HDSG würde auch die Fälle lösen, in denen nicht die HZD - nur dieser Fall konnte mit dem DV-Verbundgesetz geregelt werden -, sondern auch z.B. dem HCC zentrale Aufgaben wie bei Buchungen im SAP-System ohne Einflussmöglichkeiten der Daten verarbeitenden Stelle übertragen wurden.

Da die Landesregierung nur für ihr angehörende Behörden Entscheidungen treffen kann, sind mit den Regelungen im DV-VerbundG außerhalb stehende Daten verarbeitende Stellen wie der Hessische Landtag, der Hessische Rechnungshof, der Staatsgerichtshof und meine Behörde nicht einbezogen.

5.1.1.2 Verantwortung, Rollen und Kontrollrechte bei gemeinsamen Verfahren

Die Besonderheiten von Verfahren, die der Erledigung von Aufgaben verschiedener Stellen dienen, sind in § 15 HDSG geregelt. Gemeinsame Verfahren umfassen Verfahren mit einer (teilweise) gemeinsamen Datenbasis einschließlich Abrufverfahren. Für Außenstehende sind diese Verfahren nicht transparent, insbesondere im Hinblick auf die Verantwortungsbereiche für die einzelnen Datenverarbeitungen. Da auch beim Einsatz gemeinsamer Verfahren sichergestellt sein muss, dass nur die für die Aufgabenerledigung der Daten verarbeitenden Stelle jeweils erforderlichen Daten von dieser verarbeitet werden, sind solche Verfahren regelmäßig komplex. Es bedarf daher einer Vielzahl von Festlegungen. Wichtig ist dabei, dass die Verantwortungsbereiche geregelt und abgegrenzt sind und klar ist, wer die Federführung hat.

§ 15 Abs. 1 und 2 HDSG

(1) Die Einrichtung eines automatisierten Verfahrens, das mehreren Daten verarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Benutzung des Verfahrens ist im Einzelfall nur erlaubt, wenn hierfür die Zulässigkeit der Datenverarbeitung gegeben ist. Vor der Einrichtung oder Änderung eines gemeinsamen Verfahrens ist der Hessische Datenschutzbeauftragte zu hören. Ihm sind die Festlegungen nach Abs. 2 Satz 1, das Verfahrensverzeichnis nach § 6 Abs. 1 und das Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3 vorzulegen.

(2) Die beteiligten Stellen bestimmen eine Stelle, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt und legen schriftlich fest

1. die Bezeichnung und die Aufgaben jeder beteiligten Daten verarbeitenden Stelle sowie den Bereich der Datenverarbeitung, für deren Rechtmäßigkeit sie im Einzelfall verantwortlich ist und

2. die für die Durchführung des gemeinsamen Verfahrens nach § 10 Abs. 2 getroffenen technischen und organisatorischen Maßnahmen.

Die mit der Durchführung des gemeinsamen Verfahrens betraute Stelle verwahrt ein Doppel des von den beteiligten Stellen nach § 6 Abs. 1 zu erstellenden Verfahrensverzeichnisses und hält es zusammen mit den Angaben nach Satz 1 Nr. 1 zur Einsicht für die Öffentlichkeit bereit; dies gilt auch für die Angaben nach Satz 1 Nr. 2, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird. § 6 Abs. 2 gilt entsprechend.

5.1.1.2.1 Beteiligte Stellen

§ 15 Abs. 2 HDSG geht dabei davon aus, dass die "beteiligten Stellen" eine Stelle bestimmen, der die Planung, Einrichtung und Durchführung des Verfahrens obliegt (Federführer) und dass sie die Verantwortungsbereiche der einzelnen Stellen schriftlich festlegen. Aus der Gesetzesbegründung lässt sich herleiten, dass mit dem Begriff "beteiligte Stellen" die Daten verarbeitenden Stellen gemeint sind, die dem Verfahren angeschlossen sind.

Begründung zu § 15 Abs. 2 HDSG (LTDrucks. 14/3830, S. 23)

Abs. 2 legt fest, dass eine Stelle aus Gründen der Praktikabilität die Federführung für die Organisation des gemeinsamen Verfahrens übernehmen soll. Damit ist keinerlei Übertragung der rechtlichen Verantwortlichkeit verbunden, die bei den beteiligten Daten verarbeitenden Stellen verbleibt.

Außerdem standen nur Praktikabilitätsgründe hinter der Regelung, dass ein Federführer für die Organisation des gemeinsamen Verfahrens bestimmt werden muss. Damit ist klar: dem Federführer ist keinerlei rechtliche Verantwortung übertragen; diese verbleibt vielmehr bei den beteiligten Daten verarbeitenden Stellen. Das bedeutet, dass der Federführer nur dann und insoweit die Verantwortung für die Datenverarbeitung und die Datenbestände hat, soweit ihm die beteiligten Stellen nach § 15 Abs. 2 Nr. 1 diese übertragen haben. Grundsätzlich aber bleiben die beteiligten Stellen für die Datenverarbeitung und ihre Daten auch im gemeinsamen Verfahren verantwortlich.

In die Konzeption eines gemeinsamen Verfahrens fließen Anforderungen, Informationen und Erfahrungen der mit dem Verfahren unterstützten Aufgabenbereiche ein. Dies gilt sowohl für die fachlichen wie für die technischen Anforderungen. Häufig übernimmt eine Projektarbeitsgruppe die Planung und Einführung; die Durchführung kann wieder bei einer anderen Stelle liegen.

Über die Konzeption und den Einsatz gemeinsamer Verfahren wird regelmäßig nicht gemeinsam von den Stellen entschieden, bei denen die Datenverarbeitung später stattfindet, sondern wegen der Komplexität solcher Verfahren entscheiden auch hier übergeordnete Stellen. Müssten die beteiligten Stellen die Festlegung treffen, würde das bedeuten, dass z.B. beim Verfahren E-Einbürgerung alle Ausländerämter und die Regierungspräsidien eine schriftliche Vereinbarung über die nach § 15

Abs. 2 Nr. 1 und 2 erforderlichen Festlegungen treffen müssten. Auch hier wäre es hilfreich, den Begriff der "beteiligten Stellen" durch die "verantwortlichen Stellen" zu ersetzen.

5.1.1.2.2 Beteiligung von Stellen, die nicht dem HDSG unterliegen

Der Gesetzgeber hat bei der Konstruktion der Vorschrift bereits vorausgesehen, dass gemeinsame Verfahren auch mit Beteiligung von Stellen vorkommen können, die nicht dem HDSG unterliegen. Im Auge hatte er dabei in erster Linie nicht-öffentliche Stellen. Deshalb wurde eine Vorschrift geschaffen, die der Auftragsdatenverarbeitung nachgebildet ist (vgl. § 15 Abs. 3 und § 4 Abs. 3 Satz 1).

§ 15 Abs. 3 HDSG

Stellen, auf die dieses Gesetz keine Anwendung findet, können am gemeinsamen Verfahren beteiligt werden, wenn vertraglich sichergestellt ist, dass sie in diesem Verfahren die Bestimmungen dieses Gesetzes beachten und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwerfen.

§ 4 Abs. 3 Satz 1 HDSG

Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. …

Wie sich in der Praxis herausstellt, ist die Sachlage aber nur partiell vergleichbar; auch diese Regelung bedarf deshalb der Überarbeitung. Zur Mitwirkung an dieser Aufgabe bin ich gerne bereit.

5.1.1.2.2.1 Nicht-öffentliche Stellen

Bei nicht-öffentlichen Stellen besteht regelmäßig schon aus Wettbewerbsgründen die Notwendigkeit, nicht nur einer Stelle die Teilnahme zu gewähren. Bei Verfahren mit beschränkten Benutzerkreisen müssen ohnehin die Anforderungen an den Anschluss sowie die Bedingungen der Nutzung festgelegt werden. Deshalb ist z.B. auch mit § 16a Hessisches Vermessungsgesetz für Datenabrufe aus dem Liegenschaftskataster im Wege des automatisierten Abrufs eine spezielle Vorschrift geschaffen worden, die an die Stelle des § 15 Abs. 3 HDSG tritt. Auch in gemeinsamen Verfahren, die für einen unbeschränkten Kreis von Teilnehmern konzipiert sind, wie z.B. das Stiftungsverzeichnis, kann die Vorgehensweise nach dem HDSG nicht praktikabel sein, weshalb § 17a Abs. 4 Hessisches Stiftungsgesetz auch die Anwendung des § 15 Abs. 3 HDSG ausschließt.

5.1.1.2.2.2 Öffentliche Stellen außerhalb Hessens

Sind z.B. Kommunen außerhalb Hessens, andere Bundesländer oder der Bund an gemeinsamen Verfahren beteiligt, so würde § 15 Abs. 3 bedingen, dass jede dieser Stellen sich der Anwendung des Hessischen Datenschutzgesetzes unterwerfen müsste. Regelmäßig sind diese Stellen aber verpflichtet, ein anderes Datenschutzgesetz, nämlich das jeweilige Landesdatenschutzgesetz bzw. für Bundesbehörden das Bundesdatenschutzgesetz anzuwenden. Da die Regelungen nicht immer deckungsgleich sind, kann das zu praktischen Problemen führen. Ähnliches gilt für die Zusage, sich der Kontrolle des Hessischen Datenschutzbeauftragten für das gemeinsame Verfahren zu unterwerfen. Kompetenzkonflikte sind bei dieser Regelung vorprogrammiert.

5.1.1.2.2.3 Öffentlich-rechtliche Religionsgesellschaften

Allen Religionsgesellschaften und den Vereinigungen, die sich die gemeinschaftliche Pflege einer Weltanschauung zur Aufgabe machen, ist durch Art. 140 GG i.V.m. Art. 137 Abs. 3 Weimarer Reichsverfassung das Recht garantiert, "ihre Angelegenheiten selbständig, innerhalb des für alle geltenden Gesetzes" zu ordnen und zu verwalten (Kirchenautonomie). Dazu gehört die zur Gewährleistung der Religionsfreiheit unerlässliche Freiheit der Bestimmung über Organisation, Normsetzung und Verwaltung, die für innerkirchliche Maßnahmen jede staatliche Einmischung ausschließt, und zwar unabhängig davon, ob es sich um öffentlich-rechtliche Körperschaften handelt oder nicht. Die beiden großen christlichen Religionsgesellschaften haben in dieser Tradition eigene Rechtswerke zum Datenschutz und eigene Datenschutzkontrollinstanzen geschaffen. Auch bei anderen Religionsgesellschaften, die dieses nicht haben, dürfen sich staatliche Instanzen aber nicht einmischen. Jedenfalls ist aus verfassungsrechtlichen Gründen eine Unterwerfung unter die Kontrolle des Hessischen Datenschutzbeauftragten bei Beteiligung solcher Stellen an einem gemeinsamen Verfahren ausgeschlossen.

Dass die Beteiligung von Religionsgesellschaften an gemeinsamen Verfahren durchaus konkret wird, zeigt die Entwicklung im Schulbereich, wo auch von Religionsgesellschaften getragene Schulen, die kirchlichem Datenschutzrecht unterliegen, an dem Verfahren LUSD und dem geplanten Kultus-Data-Warehouse teilnehmen.

5.1.2 Bereitstellung von Daten im Internet

Das Internet wird immer mehr zur Bereitstellung von Informationen genutzt. Suchmaschinen bieten dabei eine bequeme Möglichkeit, Informationen zu finden. Wenn irrtümlich Dokumente in das Internet gestellt werden, sind sie ebenfalls über Suchmaschinen zu finden. Es bereitet jedoch Probleme, die Dokumente dann aus dem Zugriff zu entfernen. Damit sind auch die Datenschutzrechte auf Löschung oder Berichtigung nicht wirksam durchzusetzen.

5.1.2.1 Internetpannen

In diesem Jahr musste ich in mehreren Fällen feststellen, dass ungewollt, aber eben auch unbefugt, im Internet Daten von Bürgern oder anderen Personen durch hessische Behörden preisgegeben wurden. Bekannt wurden die Vorfälle in aller Regel dadurch, dass Suchmaschinen wie Google unter einem Stichwort den Verweis auf das entsprechende Dokument aufgelistet hatten. Die Ursache war nie Absicht, sondern meist eine Kombination von menschlichem Versagen und unerwarteten technischen Möglichkeiten.

5.1.2.1.1 Polizeipanne Darmstadt

Das Polizeipräsidium Darmstadt nutzt ein CMS (Content Management System) für das interne Netz und für die Website im Internet. Ob ein Dokument im internen Netz, im Internet oder in beiden zur Verfügung gestellt wurde, wurde ursprünglich nur durch Setzen eines Häkchens entschieden. Die entsprechenden Zugriffsrechte für beide Informationsangebote besaß ein Mitarbeiter, der als Redakteur tätig war.

Das Protokoll einer Verkehrskontrolle sollte in das interne Netz gestellt werden. In dem Protokoll wurden auch die Personalien mehrerer Personen aufgelistet und welche Erkenntnisse der Polizei vorlagen. Der Redakteur setzte aber irrtümlich nicht nur das Häkchen für "internes Netz", sondern auch für "Internet". Von seinem Arbeitsplatz, der sich im internen Netz befand, war das Bild, was er erhielt, wie gewünscht: das Protokoll stand zur Verfügung. Er hatte jedoch nicht erkannt, dass das Dokument auch im Internet stand.

5.1.2.1.2 Informationen zur Sitzungsvorbereitung von parlamentarischen Gremien

In zwei Fällen traten bei der Bereitstellung von Unterlagen zu Sitzungen im Internet Fehler auf, die auf menschliche Irrtümer oder mangelnde Sicherheitsvorkehrungen zurückzuführen waren.

In dem einen Fall werden als Bürgerservice auf der Internetseite des Parlaments Sitzungsinformationen zur Verfügung gestellt. Diese enthalten keine personenbezogenen Daten. Die berechtigten Sitzungsteilnehmer erhalten Unterlagen, in denen sich auch personenbezogene Daten befinden. Durch ein Versehen wurden jedoch die Sitzungsunterlagen mit Personenbezug in das Internetangebot für die Bürgerinnen und Bürger eingestellt.

In dem anderen Fall war im Internet für berechtigte Sitzungsteilnehmer die Möglichkeit geschaffen worden, sich wichtige Unterlagen herunterzuladen. Wenn man sich an dem Informationssystem mit Benutzerkennung und Passwort angemeldet hatte, wurden die entsprechenden Dokumente zum Download zur Verfügung gestellt. Die Dokumente befanden sich in einem eigenen Verzeichnis auf dem Webserver, das jedoch nicht gegen direkte Zugriffe aus dem Internet gesperrt war.

5.1.2.1.3 Neues Internetangebot

Eine hessische Behörde hatte im Internetangebot neue Unterlagen zur Verfügung gestellt. Die neuen Unterlagen wurden im Angebot verlinkt. Die alten Unterlagen wurden jedoch nicht gelöscht. Mit den alten Links konnte weiterhin auf die Unterlagen zugegriffen werden.

5.1.2.1.4 Dokumente mit geschwärzten Informationen

Eine Behörde wollte pdf-Dokumente im Internet zur Verfügung stellen, die auch Informationen zu Personen enthielten. Um die Rechte der Betroffenen zu wahren, "schwärzte" man die entsprechenden Passagen, indem man eine schwarze Fläche darüber kopierte. Die eigentlichen personenbezogenen Daten blieben dabei jedoch erhalten. In dieser Form geänderte Dokumente wurden dann in das Internet gestellt.

In all diesen Beispielen wurde der Zugriff auf personenbezogene Daten durch Suchmaschinen möglich.

5.1.2.2 Suchmaschinen

Suchmaschinen sind Angebote im Internet, die zu Stichwörtern Treffer anzeigen in Form von Verweisen ("Links") auf Dokumente oder Seiten, die entweder das Stichwort selbst im Dokument haben oder das Stichwort als Metadatum in der Dokumentbeschreibung haben. Die Reihenfolge der angezeigten Dokumente wird durch ausgeklügelte Regeln bestimmt, sog. Ranking-Algorithmen. Die bekanntesten Suchmaschinen sind Google (Marktanteil in Deutschland fast 90%), Yahoo!search und MSN Search.

Suchmaschinen finden ihre Dokumente mit "webcrawlern". Das sind Programme, die im Internet nach Informationsangeboten suchen und dann alle dort angegebenen Links aufrufen. Von diesen Seiten aus werden dann wieder alle Links aufgerufen usw. Webcrawler suchen aber manchmal auch Verzeichnisse die allgemein zugreifbar sind und durchsuchen diese nach Dateien und Dokumenten.

Als weiteres Angebot laden Suchmaschinen oft auch Dokumente herunter und konvertieren sie in das allgemein lesbare HTML-Format. Diese konvertierten Dokumente stellen die Suchmaschinen dann auf eigenen Rechner zur Verfügung. Dabei entscheidet die Menge der Zugriffe, ob ein Dokument konvertiert wird und wie lange es vorgehalten wird.

Natürlich kann ein Internetbenutzer ein Dokument herunterladen und es dann auf einem eigenen Server als Duplikat speichern und für den Zugriff bereithalten. In diesem Fall finden Suchmaschinen das Duplikat und stellen dafür ebenfalls einen

Link ein. In aller Regel erkennt eine Suchmaschine, ob es das Dokument schon gibt und zeigt dies an. Da es aber nicht zwischen Original und Kopie unterscheiden kann, steht oft die Kopie vor dem Original in der Trefferliste. Daher führt die Löschung des Originaldokuments nicht automatisch dazu, dass das Dokument nicht mehr im Internet gefunden werden kann.

Es gibt auch weite Teile des Internets die den Suchmaschinen verborgen bleiben, das sog. "deep web". Hierzu gehören insbesondere Informationsangebote, für deren Nutzung man sich mit Benutzerkennung und Passwort anmelden muss.

5.1.2.3 Konsequenzen

In den genannten Beispielen wurden die Dokumente von Webcrawlern gefunden, für die Recherche in der Suchmaschine aufbereitet und auch als HTML-Dokument aufbereitet und vorgehalten. Das hatte zum Teil gravierende Konsequenzen.

Im Fall der Polizeipanne hat die Polizei das Dokument sofort gegen Zugriffe gesperrt, als sie davon erfahren hat. Da es aber bereits eine Pressemitteilung zu dem Vorfall gegeben hatte, hatten viele Interessierte bereits über Google auf das Dokument zugegriffen. Das Dokument war im Ranking nach oben gerutscht und es gab eine HTML-Version. Selbst als der Zugriff auf das Original-Dokument nicht mehr möglich war, gab es noch die HTML-Version auf die zugegriffen werden konnte. Trotz erheblicher Anstrengungen des Suchmaschinenbetreibers hat es mehrere Tage gedauert, bis der direkte Verweis und die HTML-Version verschwunden waren. Es gab aber weiterhin noch Kopien auf anderen Rechnern. Die gleiche Lage war bei den versehentlich mit personenbezogenen Daten ins Internet eingestellten Sitzungsunterlagen eingetreten.

Auch im Fall der Bereitstellung von Sitzungsunterlagen in einem nicht gegen direkte Zugriffe gesicherten Verzeichnis sowie bei dem Belassen von alten Unterlagen im Internet wurden die Pannen durch Suchmaschinen aufgedeckt. Es gelang aber relativ schnell und ohne großes Aufsehen, die Zugriffe zu sperren bzw. die Dateien zu löschen.

Im letzten Fall ergab sich das Problem nur durch die HTML-Darstellung des Dokumentes. Während bei der Darstellung im Acrobat-Reader die geschwärzten Teile tatsächlich schwarz angezeigt wurden, erfasste die HTML-Darstellung den Text des eigentlichen Dokumentes. Da aber keine Daten gelöscht worden waren, konnte man im HTML-Text wieder alle Namen lesen.

Ob es weiterhin Kopien in den Teilen des Internets gibt, die den Suchmaschinen verborgen bleiben ("deep web") kann man nicht feststellen. In vielen Fällen muss man hiervon ausgehen.

5.1.2.4 Rechtliche Folgerungen

Die Veröffentlichung von personenbezogenen Daten im Internet stellt eine Datenübermittlung nach § 2 Abs. 2 Nr. 3 HDSG dar.

§ 2 Abs. 2 Nr. 3 HDSG

Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener Daten. 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,
….

Nach § 14 HDSG trägt dabei die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung.

Bei der Polizeipanne und bei der versehentlichen Einstellung vollständiger Sitzungsunterlagen in das Internet war die Einstellung der Daten ins Internet unzulässig; sie war auch nicht beabsichtigt, sondern in beiden Fällen die Folge eines menschlichen Fehlers.

In dem zweiten unter Ziff. 5.1.2.1.2 geschilderten Fall war die Art der Einstellung nicht sicher genug, um die Zugriffe auf den Kreis der Berechtigten einzugrenzen. Damit wurden auch unzulässige Datenabrufe möglich.

Alle genannten Fälle zeigten bei Maßnahmen zur Behebung der Fehler deutlich die Tücken des Internets: Aufgrund der Struktur des Internets und der Suchmaschinen können falsche oder rechtswidrig ins Internet eingestellte Informationen zwar korrigiert oder aus dem aktuellen Internetangebot herausgenommen werden. Damit sind aber die Rechte der Betroffenen nach §§ 8 Abs. 1 Nr. 4, 19 Abs. 1 und 4 in Verbindung mit § 2 Abs. 2 Nr. 5 HDSG nicht gewahrt.

§ 8 Abs. 1 Nr. 4 HDSG

Jeder hat nach Maßgabe des Gesetzes ein Recht auf
…
4. Berichtigung, Sperrung oder Löschung der zu seiner Person gespeicherten Daten (§ 19),
…

§ 19 Abs. 1 und 4 HDSG

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.
….
(4) Personenbezogene Daten sind zu löschen, wenn ihre Verarbeitung unzulässig ist.

§ 2 Abs. 2 Nr. 3 HDSG

Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener Daten. Im Sinne der nachfolgenden Vorschriften ist
…
5. Löschen das Unkenntlichmachen gespeicherter Daten,
….

Die einmal eingestellten Informationen bleiben über Suchmaschinen weiterhin abrufbar: das Internet "vergisst" nichts. Die Funktionen "Löschen" und "Berichtigen" sind damit im Internet nicht zu realisieren.

Dies ist einer der Gründe, warum ich grundsätzlich gegen eine Einstellung personenbezogener Daten in das Internet plädiere, wenn diese nicht auf der ausdrücklichen und informierten Einwilligung der Betroffenen beruht oder ganz gewichtige Allgemeininteressen für diesen Veröffentlichungsweg sprechen, die die damit verbundene Beschneidung der Betroffenenrechte hinnehmbar erscheinen lassen.

So habe ich bei der Anhörung zum Zweiten Gesetz zur Änderung des Hessischen Stiftungsgesetzes ausdrücklich dafür plädiert, in § 17a von der Veröffentlichung im Internet die Daten der vertretungsberechtigten Personen auszunehmen, weil ich ein gewichtiges Allgemeininteresse für die Veröffentlichung dieser Daten in diesem Medium nicht erkennen konnte. Gleichwohl wurde das Gesetz unverändert verabschiedet (GVBl. I 2007, S. 546 f.)

§ 17a Abs. 2 und 3 HStiftG

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

Änderungen hat die Stiftung der Aufsichtsbehörde unverzüglich mitzuteilen.

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

Ein Grund, warum nicht die Kommunikationsadressen von Stiftungen genügen, sondern auch die Namen der Vertretungsberechtigten erscheinen müssen, wurde im Gesetzgebungsverfahren nicht genannt. Die vorgebliche "Bürgerfreundlichkeit" kann aber nicht die Einschränkung der Rechte von Betroffenen rechtfertigen, die damit auf Dauer mit irgendwann einmal ausgeübten Funktionen im Internet abrufbar werden.

5.1.3 Entwicklungen im Bereich der Videoüberwachung

Videoüberwachung scheint en vogue zu sein. Immer mehr Kommunen und andere öffentliche Stellen wollen Videoüberwachungskameras installieren. Nicht immer werden allerdings die gesetzlichen Voraussetzungen für die Zulässigkeit von derartigen Überwachungskameras ordnungsgemäß geprüft oder es fehlt an den nötigen Informationen für die betroffenen Bürger.

Im Berichtszeitraum gab es eine erhebliche Zunahme von Realisierungen und/oder Plänen hinsichtlich der Einrichtung von Videoüberwachungsanlagen. Es ist zu beobachten, dass Videoüberwachung in immer mehr Bereichen eine Rolle spielt. Zum einen nimmt die Überwachung öffentlicher Plätze deutlich zu, zum anderen spielt die Videoüberwachung auch zunehmend bei der Objektsicherung öffentlicher Einrichtungen eine größere Rolle.

In manchen Fällen werde ich vor der Installierung derartiger Systeme angefragt und kann beratend tätig werden. In manchen Fällen erfahre ich geplante Maßnahmen aus der Presse und überprüfe dann die entsprechenden Projekte. Über wieder andere Überwachungsmaßnahmen werde ich durch betroffene Bürger oder Bürgerinnen benachrichtigt, die sich häufig schlecht informiert fühlen. Da es für die Einrichtung von Videoüberwachungsanlagen keine Informationspflicht gegenüber meiner Behörde gibt, vermute ich, dass viele derartige Einrichtungen ohne eine ausreichende datenschutzrechtliche Prüfung installiert werden.

Nachfolgend möchte ich einige Beispielsfälle aufführen, mit denen ich mich im vergangenen Jahr auseinanderzusetzen hatte.

1. In einem Schwimmbad mit mehreren Schwimmbecken sowohl im Innen- wie im Außenbereich waren an einem Becken des Innenbereichs und am Außenbereichsbecken Videokameras installiert. Eine Information der Badegäste erfolgte nicht. Zunächst könnte man meinen, dass es den Badegästen möglich sein müsste, ohne eine derartige Überwachung ihrem Schwimmvergnügen nachkommen zu können. Die Begründung für die Installierung der Kameras überzeugte jedoch. Das Bad hat nur einen Schwimmmeister, der von seiner "Kanzel" lediglich ein Schwimmbecken genau einsehen kann. Die anderen beiden Becken, eins innen, eins außen, kann er nicht einsehen. Die Bilder der Kameras werden an seinen Arbeitsplatz auf Monitore übertragen, damit er eventuelle Vorkommnisse wahrnehmen und gegebenenfalls einschreiten kann. Die Videokameras fungieren also in diesem Fall quasi als zusätzliches Auge des Schwimmmeisters. Die Bilder werden auch nicht aufgezeichnet, sondern dienen lediglich der aktuellen Information des Schwimmmeisters. Vor diesem Hintergrund halte ich die Maßnahme für zulässig. Ich habe allerdings gefordert, dass die Besucher des Schwimmbads über die Tatsache und über den Sinn und Zweck der Maßnahme durch entsprechende Beschilderung informiert werden. Dies ist zwischenzeitlich durch entsprechende Hinweisschilder geschehen.

   Dieses Becken wird durch die Badeaufsicht zu Ihrer Sicherheit videoüberwacht.

2. In einer städtischen Kindertagesstätte wurden über Monate ständig Sachbeschädigungen registriert. So wurde z.B. regelmäßig ein Eingangsschloss mit Sekundenkleber unbrauchbar gemacht. Um diesem Treiben Einhalt zu gebieten, erwog man eine Videoüberwachung der Eingangstür während der Schließungszeiten der Kindertagesstätte, die nur durch einen Bewegungsmelder in Betrieb gesetzt würde. Aufgenommen werden sollte nur ein Teil des Eingangsbereichs innerhalb des städtischen Grundstücks, das während der Schließungszeiten auch nicht frei zugänglich ist. Ich habe der Kommune mitgeteilt, dass nach § 14 Abs 4 Nr. 3 HSOG eine Videoüberwachung zur Wahrung des Hausrechts grundsätzlich zulässig, die geplante Maßnahme allerdings am Grundsatz der Verhältnismäßigkeit zu messen sei. Das von der Kommune vorgelegte Konzept entsprach diesen Anforderungen. Allerdings habe ich empfohlen, dass der betroffene Personenkreis, also insbesondere die Eltern der Kinder, über das geplante Konzept informiert wird.

3. Eine hessische Kommune wollte wegen wiederholter Sachbeschädigungen an gemeindlichen Einrichtungen an diversen Gebäuden Videokameras installieren, die neben Bild- auch Tonaufnahmen liefern sollten. Die Kameras sollten so angebracht werden, dass Betroffene davon gerade keine Kenntnis nehmen konnten. Erfreulicherweise hat die Kommune vor Realisierung des Vorhabens meine Behörde eingeschaltet, so dass das Vorhaben nicht in der geplanten Form umgesetzt worden ist. Auf die Tonaufnahmen wurde aus rechtlichen Gründen ganz verzichtet. Die Überwachungsmaßnahme wurde entsprechend den gesetzlichen Bestimmungen, dass offen zu überwachen ist (§ 14 Abs. 4 HSOG), durch Hinweisschilder kenntlich gemacht.

4. Ein Bürger wandte sich an meine Behörde und beschwerte sich darüber, dass in den Zügen der HLB Videokameras installiert seien, es aber keinen entsprechenden Hinweis auf die durchgeführte Überwachungsmaßnahme gebe. Da ich vor einigen Jahren mit der HLB das Konzept der Videoüberwachung abgesprochen hatte, überraschte die Beschwerde. Eine Überprüfung ergab, dass tatsächlich einige Züge neuerer Bauart nur mit einem kaum erkennbaren kleinen Piktogramm mit einer Kamera auf die Überwachungsmaßnahme hinwiesen. Für den normalen Reisenden war dieser Hinweis nicht zu entdecken. Es fehlte außerdem die Benennung einer Stelle, an die sich von der Überwachung Betroffene wenden können, um Näheres über die durchgeführten Überwachungsmaßnahmen zu erfahren. Die HLB hat zugesichert, hier die Hinweise für die Reisenden zu verbessern.

5. Neben der nach dem Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) geregelten Videoüberwachung muss auch der zunehmende Einsatz von Webcams genannt werden. Vielfach wollen Kommunen damit ihre Orte im Internet wirksam für den Tourismus präsentieren, indem sie Sehenswürdigkeiten ins rechte Licht rücken. Das stellt kein Problem dar, solange nur Übersichtsaufnahmen ins Internet übertragen werden. Allerdings hat es auch hier Fälle gegeben, die sich kaum von Videoüberwachungsmaßnahmen zur Gefahrenabwehr nach § 14 Abs. 3 oder 4 unterschieden haben, aber natürlich nicht die dort genannten rechtlichen Voraussetzungen erfüllten. Webcams zur Information über z.B. historische Örtlichkeiten dürfen grundsätzlich nicht so eingestellt sein, dass Personen oder Kfz-Kennzeichen erkannt werden können. Webcams stellen die Bilder ins Internet und damit für jeden zugänglich ein. Sind Personen oder Kfz-Kennzeichen erkennbar, so handelt es sich um personenbezogene Daten. Sind Webcams so eingestellt, dass sie personenbezogene Daten übertragen, ist dies datenschutzrechtlich unzulässig.

Zum Schluss möchte ich erneut die Videoüberwachung an der Konstabler Wache in Frankfurt am Main ansprechen, über die ich bereits im 34. und 35. Tätigkeitsbericht berichtet habe.

Ich hatte bemängelt, dass der Überwachungsbereich zu groß bemessen ist und dass teilweise Fenster und Balkone in den Schwenkbereich der Kameras fallen. Wiederholt hatte ich das Polizeipräsidium Frankfurt aufgefordert, hier einen rechtmäßigen Zustand herzustellen, wurde aber immer wieder vertröstet, u. a. mit dem Hinweis darauf, dass man mit der Stadt über eine Übernahme der Anlage verhandle.

Am 11. Dezember 2007 erreichte mich vom Polizeipräsidium Frankfurt am Main die Nachricht, dass die Polizei die Finanzierung neuer Kameras übernehmen werde, mit denen die datenschutzrechtlichen Anforderungen technisch umgesetzt werden können. Künftige Kosten werden dann von der Stadt Frankfurt getragen. Die Anlage wird aber weiterhin von der Polizei betrieben.

Sobald die neuen Kameras installiert sind, werde ich eine Überprüfung vor Ort durchführen.

5.2 Justiz

5.2.1 Bestimmung des Anzeigeerstatters als Sachverständiger im Ermittlungsverfahren

Auch in Sachgebieten, in denen es nur wenige kompetente Fachleute gibt, ist bei der Auswahl von Sachverständigen im Rahmen des Ermittlungsverfahrens darauf zu achten, dass der Sachverständige nicht auch in anderer Funktion - etwa als Anzeigeerstatter - von dem Verfahren tangiert ist. Das kann auch für Interessenverbände gelten, die für ihre Mitglieder zum selben Sachverhalt Schadenersatz oder Unterlassungserklärungen einfordern.

Oft ist spezifischer Sachverstand notwendig, um zu erkennen, ob sich aus einem bestimmten Dokument Anhaltspunkte für strafrechtlich relevante Vorgänge ergeben. Dann benötigen die Ermittlungsbehörden Sachverständige zur Auswertung von Unterlagen.

5.2.1.1 Einbeziehung der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen in staatsanwaltschaftliche Ermittlungen

Verschiedene Staatsanwaltschaften übergaben der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) in der Vergangenheit nicht nur DVDs und CDs, sondern auch ganze Festplatten und PCs mit dem Namen des Beschuldigten. Dabei handelte es sich um Ermittlungen zu Urheberrechtsverletzungen im Zusammenhang mit Downloads aus dem Internet. Brachte die Auswertung der Unterlagen das Ergebnis, das Herunterladen bzw. das Verwenden dieser Software ist unter Verletzung von Lizenzen erfolgt und somit liegt ein Urheberrechtsverstoß vor, wurde dieses Wissen verwendet, um es den GVU-Mitgliedern weiterzugeben oder gar in deren Namen bei den Beschuldigten Schadenersatz oder Abmahnungsgebühren geltend zu machen.

Das datenschutzrechtliche Problem liegt in der möglichen Übermittlung von personenbezogenen (Überschuss-)Daten auf einem übergebenen Rechner und des Beschuldigtennamens zur Stellung eines Strafantrags.

Die Mitteilung des Beschuldigtennamens kann nicht auf § 406e StPO gestützt werden, weil zurzeit der Übergabe der Hardware der Verletzte noch gar nicht feststeht und die GVU kein Rechtsanwalt ist.

§ 406e StPO

(1) Für den Verletzten kann ein Rechtsanwalt die Akten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, einsehen sowie amtlich verwahrte Beweisstücke besichtigen, soweit er hierfür ein berechtigtes Interesse darlegt. In den in § 395 genannten Fällen bedarf es der Darlegung eines berechtigten Interesses nicht.

(2) Die Einsicht in die Akten ist zu versagen, soweit überwiegende schutzwürdige Interessen des Beschuldigten oder anderer Personen entgegenstehen. Sie kann versagt werden, soweit der Untersuchungszweck gefährdet erscheint oder durch sie das Verfahren erheblich verzögert würde.

(3) Auf Antrag können dem Rechtsanwalt, soweit nicht wichtige Gründe entgegenstehen, die Akten mit Ausnahme der Beweisstücke in seine Geschäftsräume oder seine Wohnung mitgegeben werden. Die Entscheidung ist nicht anfechtbar.

(4) …

Ein Sachverständiger darf nicht in einem nahen Verhältnis zum Verletzten stehen. Die GVU ist ein Interessenverband der Urheber. Andererseits ist auch zu berücksichtigen, dass für die in diesem Kontext notwendigen Prüfungen die Anzahl von Personen, die die notwendige Sachkunde besitzen, beschränkt ist.

Als Konsequenz kann die GVU daher nur so in die Sachverhaltsermittlungen einbezogen werden, dass ihr dabei keine personenbezogenen Daten einschließlich der Beschuldigtennamen bekannt werden. Diese sind für die Klärung einer Urheberrechtsverletzung auch nicht erforderlich.

Es dürfen nur die verdächtigen Datenträger selbst, nicht ganze Rechner oder Festplatten übergeben werden, die möglicherweise personenbezogene Daten des Beschuldigten und Dritter enthalten.

5.2.1.2 Verdacht des Abrechnungsbetruges durch Pflegedienste

Bei der Bearbeitung von Ermittlungsverfahren gegen Pflegedienste wegen Abrechungsbetruges wurden teilweise von den Ermittlungsbehörden Krankenkassen, die mit ihrer Anzeige das Verfahren angestoßen hatten, bzw. deren Mitarbeiter als Sachverständige hinzugezogen.

Der Strafanzeige vorausgegangen war meist eine längere Auseinandersetzung, die sich u.a. an der Frage festmachte, ob die Kasse Einsicht in die Pflegedokumentation nehmen darf. Einsicht ist allerdings nur dem MDK und nicht der Krankenkasse direkt zu gewähren. Bei diesen Unterlagen handelt es sich um besonders sensitive Daten. Oft sind eine Vielzahl von Personen betroffen, bei denen keine Anhaltspunkte vorliegen, dass ihre Behandlung Gegenstand eines möglichen Ermittlungsverfahrens sein könnte.

In einem mir vorliegenden Fall ergab sich z.B. folgender Verfahrensablauf: Nach längeren Auseinandersetzungen im Vorfeld erstattete die Krankenkasse Strafanzeige. Als einer der ersten Ermittlungsschritte wurde ein Durchsuchungsbeschluss

beantragt, auf Grund dessen verschiedene Unterlagen beschlagnahmt wurden. Bei der Durchsuchung, vor allem bei der Auswahl der zu beschlagnahmenden Unterlagen, waren Mitglieder der Kasse als "Sachverständige" beteiligt. Durch die anschließende Überlassung dieser Unterlagen an die Sachverständigen, erhalten Mitarbeiter der Kasse Zugriff auf Unterlagen, die die Krankenkasse sonst nicht erhalten würde. Auf diese Weise besteht Gefahr, dass die strikten Regelungen des Sozialgesetzbuches zum Umgang mit Sozialdaten umgangen werden können.

Grundsätzlich gilt für alle Sachverständige, dass sie die zur Verfügung gestellten Unterlagen und damit die darin enthaltenen Daten vertraulich zu behandeln haben und auch die strikte Zweckbindung zu beachten haben. Das gilt selbstverständlich auch für einzelne Mitarbeiter gegenüber ihrem Arbeitgeber, soweit sie als Person zum Sachverständigen bestimmt werden. Dazu gehört im Übrigen auch ein sorgfältiger Umgang mit möglichen Kopien. Für einen Sachverständigen, der auch aus anderem Grund mit einem Fall befasst ist, etwa auf Grund einer Aufgabenstellung in seiner eigentlichen Tätigkeit, ist es nicht immer einfach, diese Grundsätze einzuhalten. Es lässt sich auch im Einzelfall wohl nicht immer ausschließen, dass sich einzelne Mitarbeiter über die Gebote für Sachverständige hinwegsetzen.

Die Ermittlungsbehörden begründeten ihr Vorgehen damit, dass es bei komplexen Angelegenheiten Probleme gäbe, geeignete Sachverständige zu finden. Grundsätzlich ist mir das Problem bewusst. Andererseits sind mir auch Ermittlungsbehörden bekannt, die sich häufiger mit Ermittlungsverfahren im Gesundheitsbereich beschäftigen und eine andere Verfahrensweise wählen.

Ich habe das Problem mit dem Justizministerium erörtert. Als Ergebnis hat das Ministerium die Staatsanwaltschaften nochmals auf das Problem hingewiesen und sie gleichzeitig über andere mögliche Gutachter, insbesondere im Sozialversicherungsbereich, informiert.

Ich gehe daher davon aus, dass zukünftig bei der Auswahl von Sachverständigen sensibel vorgegangen wird - auch wenn dies im Einzelfall dazu führen kann, dass höhere Kosten entstehen.

5.2.2 Die teilprivatisierte Justizvollzugsanstalt Hünfeld

Nach etwa eineinhalbjährigem Betrieb der teilprivatisierten Justizvollzugsanstalt Hünfeld habe ich vor Ort eine Datenschutzkontrolle vorgenommen. Die Prüfung führte nicht zu Beanstandungen. Trotz der Teilprivatisierung des Gefängnisses ist die Datenschutzkontrolle gewährleistet.

Am 7. Dezember 2005 wurde die Justizvollzugsanstalt Hünfeld eröffnet. Das hessische Justizministerium hatte mich im Vorfeld über das Vorhaben, eine teilprivatisierte Justizvollzugsanstalt betreiben zu wollen, informiert und mich über die vorgesehene Beteiligung eines privaten Dienstleistungsunternehmens in Kenntnis gesetzt. Bei der Entscheidung, an den in einer Justizvollzugsanstalt anfallenden Aufgaben Private zu beteiligen, handelt es sich vorrangig nicht um eine datenschutzrechtliche, sondern um eine strafvollzugsrechtliche und politische Entscheidung. Andererseits folgen dieser Entscheidung datenschutzrechtlich relevante Konsequenzen.
Das Grundgesetz und das Strafvollzugsgesetz regeln:

Art. 33 GG Abs. 4

Die Ausübung hoheitlicher Befugnisse ist als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen.

§ 155 StVollzG

(1) Die Aufgaben der Justizvollzugsanstalten werden von Vollzugsbeamten wahrgenommen. Aus besonderen Gründen können sie auch anderen Bediensteten der Justizvollzugsanstalten sowie nebenamtlichen oder vertraglich verpflichteten Personen übertragen werden.

(2) Für jede Anstalt ist entsprechend ihrer Aufgabe die erforderliche Anzahl von Bediensteten der verschiedenen Berufsgruppen, namentlich des allgemeinen Vollzugsdienstes, des Verwaltungsdienstes und des Werkdienstes, sowie von Seelsorgern, Ärzten, Pädagogen, Psychologen und Sozialarbeitern vorzusehen.

Eindeutig ist demnach, dass eine vollständige Privatisierung des Strafvollzuges in der Bundesrepublik Deutschland nicht mit der Verfassung in Einklang zu bringen wäre.

In der Literatur zum Strafvollzugsrecht (z.B. Callies/Müller-Dietz, Strafvollzugsgesetz, Einleitung Nr. 45 - mit vielen weiteren Fundstellen) wird das Thema der Rechtmäßigkeit einer Teilprivatisierung im Strafvollzug vorwiegend unter Anführen von verfassungs- und strafvollzugspolitischen Aspekten lebhaft diskutiert.

Unabhängig davon, welchen Standpunkt man zu diesem Thema einnimmt, müssen auch bei einem teilprivatisierten Strafvollzug die Datenschutzrechte der von der Datenverarbeitung Betroffenen ausreichend berücksichtigt sein. Denn egal, ob in der Küche, beim Reinigungsdienst oder der sozialen oder medizinischen Betreuung - nahezu jegliche Aufgabenwahrnehmung in einer Justizvollzugsanstalt verlangt zwingend die Verarbeitung personenbezogener Daten. Diesen Aspekten bin ich bei der Prüfung der Justizvollzugsanstalt Hünfeld nachgegangen.

5.2.2.1 Die Trennung zwischen hoheitlicher und nicht hoheitlicher Aufgabenwahrnehmung

Eine vom hessischen Justizministerium eingesetzte Arbeitsgruppe analysierte sehr genau, inwieweit eine Privatisierung im Strafvollzug rechtlich möglich ist. Die Ergebnisse sind veröffentlicht (s. www.hmdj.hessen.de).

Als Aufgaben, die nicht privatisiert werden können, wurden benannt:
- Organisationshoheit
  Gesamtsteuerung und Überwachung der Dienstabläufe
- Behandlungsmanagement
  (z.B. Aufnahme und Entlassung von Gefangenen, Vollzugsplanung, Lockerungsentscheidungen, Disziplinarmaßnahmen oder sonstige Entscheidungen über den Status der Gefangenen)
- Teile des Bewachungsmanagements,
  soweit mit Befugnissen zu Zwangsmaßnahmen oder Eingriffen in Persönlichkeitsrechte verbunden - z.B. Kontrolle der Außenkontakte (Brief-, Besuchskontrolle etc.), Anwendung unmittelbaren Zwangs.

Privatisiert wurden dagegen folgende Aufgaben:
- Wartung und Instandhaltung technischer Anlagen, Maßnahmen der Bauunterhaltung
- Reinigung innerhalb der Gebäude (ausgenommen der Haftbereiche),
- Pflege der Außenanlagen,
- Reinigung und Instandhaltung der Dienstfahrzeuge,
- Betrieb der Anstaltsküche und die Versorgung der Gefangenen mit Verpflegung,
- Organisation des Gefangeneneinkaufs,
- Organisation und der Betrieb der Werkstätten,
- Organisation und Durchführung der arbeitstherapeutischen Beschäftigung und der Maßnahmen der schulischen und beruflichen Bildung der Gefangenen,
- Medizinische Versorgung der Gefangenen,
- Sozialarbeiterische, psychologische und pädagogische Betreuung der Gefangenen,
- Beratungsleistungen für die Gefangenen (Drogen-, Ausländer-, Schuldnerberatung),
- Organisation und Durchführung von Freizeitveranstaltungen für die Gefangenen, insbesondere der Gefangenensport,
- Teile der Verwaltungstätigkeiten (Zahlstelle, Rechnungswesen, Versorgungswesen, Poststelle, Telefonzentrale, Schreibdienst)
- Hilfsdienste für die Stationen und den Besuchsbereich,
- Überwachung der Monitore der Videoüberwachungsanlage der Liegenschaft.

Die Beschäftigten des privaten Dienstleistungsunternehmens handeln gegenüber den Insassen der Justizvollzugsanstalt nicht in eigenem Namen, sondern ausschließlich im Auftrag der Justizvollzugsbehörde. Sie sind insoweit Verwaltungs- bzw. Vollzugshelfer i.S.v. § 155 Abs. 1 StrafVollzG. Für einen Einsatz als Beliehene, der auch eine Übertragung von Eingriffsbefugnissen ermöglichen würde, fehlt es nach dem Ergebnis der Analyse der Expertengruppe an einer hinreichend konkretisierten gesetzlichen Grundlage.

Meine Zweifel an dem Ergebnis der Arbeitsgruppe, auch den Bereich der sozialen Dienste vollständig in die private Hand zu übertragen, wies das Justizministerium zurück. Sozialarbeiter leisten in der künftigen JVA Hünfeld - so der damalige Justizstaatssekretär - "Arbeit mit und am Gefangenen", treffen hingegen keine Entscheidungen über den vollzuglichen Werdegang des Gefangenen. Sämtliche Arbeiten, die die sozialen Dienste insoweit verrichten, seien als Vorarbeiten zu verstehen (z.B. Mitarbeit bei der Erstellung der Vollzugspläne, Stellungnahmen zu Vollzugslockerungen etc.), die dem Entscheidungsträger (Anstalts- oder Vollzugsabteilungsleiter) lediglich als Entscheidungshilfe dienten.

Die Prüfung der Umsetzung der Trennung zwischen hoheitlicher und privatisierter Aufgabenerfüllung in der JVA Hünfeld ergab, dass die Trennlinie richtig gezogen ist.

Beispielsweise erfolgt die Überwachung der Monitore, mit der die Liegenschaft videoüberwacht wird, in der Sicherheitszentrale der Anstalt durch Beschäftigte des privaten Dienstleisters. Wird eine Unregelmäßigkeit beobachtet, informiert der Mitarbeiter des Dienstleisters einen Bediensteten der Anstalt. Der Justizvollzugsbeamte vollzieht die Beobachtung nach und löst ggf. Alarm aus. Auch die Pforte ist doppelt besetzt. Mit der Beobachtung des Umgebungsbereiches der Pforte ist ein Mitarbeiter des Dienstleisters beauftragt. Die Entscheidung über den Einlass oder Auslass und die Mitnahme von Gegenständen obliegt einem Vollzugsbediensteten. Mitarbeiter des Dienstleisters sind auch in der Telefonzentrale eingesetzt. Eine Überwachung der ausgehenden Telefonate der Gefängnisinsassen, die aus Gründen der Sicherheit der Anstalt stattfindet, darf aber nur durch Justizvollzugsbedienstete erfolgen.

Die Technik war konsequent getrennt. Es gab getrennte Netze für den hoheitlichen und den privaten Bereich. Da das Administrationspersonal nicht doppelt vorgehalten werden sollte, übernahm ein Mitarbeiter der Justizverwaltung auch die Administration des privaten Netzes.

5.2.2.2 Die Sicherstellung der Datenschutzkontrolle

Grundsätzlich müssen die Insassen von Justizvollzugsanstalten die Verarbeitung ihrer personenbezogenen Daten insoweit hinnehmen, als es für den Vollzug einer Freiheitsstrafe erforderlich ist (§ 179 Abs. 1 StVollzG). Der Vollzug einer Freiheitsstrafe bringt naturgemäß breit gefächerte und teilweise auch sehr intensive Einschränkungen des informationellen Selbstbestimmungsrechts mit sich. Dabei ist die Intensität des Eingriffes nicht erheblich unterschiedlich, ob der Eingriff durch einen Bediensteten der Anstalt oder durch einen privat verpflichteten Verwaltungshelfer erfolgt.

Trotzdem bleibt es bei dem Selbstverständnis wie ich es z.B. schon bei meinen Ausführungen zur Kontrollzuständigkeit bei der FRAPORT (s. Ziff. 2.1) oder bei sonstigen Wahrnehmungen öffentlicher Aufgaben durch Private einfordere: Wenn der Staat sich auf die Ebene des Privatrechts begibt und sich zur Erfüllung seiner Aufgaben Privater bedient, ändert das nichts an der Zugehörigkeit zum öffentlichen Bereich. Deshalb darf die Auslagerung der Wahrnehmung öffentlich-rechtlicher Aufgabenerfüllung an Private nicht zu einer Schmälerung des Datenschutzes und der Datenschutzkontrolle führen. Auch wenn das Strafvollzugsgesetz nach einigen bereichsspezifischen Regelungen in den §§ 179 ff. in § 187 zunächst auf das Bundesdatenschutzgesetz verweist, die Bestimmungen über die Kontrollbefugnisse des Landesdatenschutzbeauftragten bleiben unberührt (§ 187 StVollzG, letzter Satz). Das gilt auch für den Fall einer Teilprivatisierung. Dementsprechend hat sich der private Dienstleister der Justizvollzugsanstalt Hünfeld in einer vertraglichen Vereinbarung gegenüber dem Land Hessen verpflichtet, das Hessische Datenschutzgesetz anzuwenden. Er ist damit auch meiner Kontrolle und meinen Kontrollbefugnissen unterworfen. Für die Beschäftigten des privaten Dienstleisters gilt das Datengeheimnis nach § 5 BDSG. Verpflichtungserklärungen der privat Beschäftigten über das Datengeheimnis nach § 5 BDSG wurden mir vorgelegt.

5.3 Verfassungsschutz

5.3.1 Novellierung des Verfassungsschutzgesetzes

Die seit mehreren Jahren geplante Änderung des Gesetzes über das Landesamt für Verfassungsschutz ist in Kraft getreten. Ich habe zu den verschiedenen Gesetzentwürfen wie auch in der Anhörung im Hessischen Landtag Stellung genommen.

Wichtige Änderungen des Gesetzes vom 6. September 2007 (GVBl. I 2007, S. 542) sind folgende:

5.3.1.1 Einsatz des IMSI-Catchers

Vorgesehen ist nunmehr auch für den Verfassungsschutz der Einsatz des sog. IMSI-Catchers (**I**nternational **M**obile **S**ubscriber **I**dentity).

§ 5 Abs. 2 VerfSchG

Das Landesamt für Verfassungsschutz darf im Einzelfall zur Erfüllung seiner Aufgaben nach § 2 Abs. 2 unter den Voraussetzungen des Abs. 1 technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkgerätes und zur Ermittlung der Geräte- und Kartennummer einsetzen. Die Maßnahme ist nur zulässig, wenn ohne die Ermittlung die Erreichung des Zwecks der Überwachungsmaßnahme aussichtslos oder erheblich erschwert wäre. Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Satz 1 unvermeidbar ist. Sie unterliegen einem absoluten Verwertungsverbot und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

Mit dem IMSI-Catcher sollen beispielsweise bei Observationen Mobiltelefone lokalisiert werden können. Der IMSI-Catcher simuliert dabei eine Basisstation für den Mobilfunk. Das Mobiltelefon wählt sich an diesen Stationen ein und überträgt sowohl die Karten- als auch die Gerätenummer. Anhand dieser Daten können über die jeweiligen Anbieter dann auch Telefonnummern ermittelt werden, die ansonsten unerkannt bleiben würden. Dabei wird auch die ungefähre Position des mobilen Telefons übertragen und der Betroffene kann lokalisiert werden.

Anders als auf Bundesebene ist der Einsatz des IMSI-Catchers in Hessen auch bei der Beobachtung verfassungsfeindlicher Bestrebungen und der Bekämpfung der organisierten Kriminalität zulässig. Ob der IMSI-Catcher im Rahmen gerade dieser Aufgabenbereiche überhaupt geeignet bzw. verhältnismäßig ist, muss sich erst noch erweisen.

5.3.1.2 Einsatz akustischer und optischer Überwachungsmittel in der Wohnung

Ziel der Gesetzesänderung war es weiterhin, die schon bestehenden Befugnisse zur akustischen und optischen Wohnraumüberwachung an die Vorgaben des BVerfG (Urteil vom 3. März 2004 - BVerfGE 109, 279) anzupassen. Danach gehört zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische (z.B. durch Wanzen) oder optische Überwachung zu Zwecken der Strafverfolgung - aber auch - wie im Fall des Tätigwerdens des Verfassungsschutzes - zu präventiven Zwecken nicht eingreifen.
Ich hatte vorgeschlagen, die vom BVerfG in den Leitsätzen aufgestellten verfahrensrechtlichen Sicherungen in den Gesetzestext aufzunehmen. Dem ist der hessische Gesetzgeber nur insoweit gefolgt, als formuliert wird:

§ 5a Abs. 4 Satz 2 VerfSchG

Die Behörde hat dafür Sorge zu tragen, dass in keinem Fall in den Kernbereich privater Lebensgestaltung eingegriffen wird.

Diese Vorgabe wird erst in der Gesetzesbegründung konkretisiert. Danach ist, wenn Anhaltspunkte dafür vorliegen, dass der Kernbereich privater Lebensgestaltung berührt wird, das Abhören und Aufzeichnen zu unterbrechen. Eine Fortsetzung darf erst dann erfolgen, wenn eine Kernbereichsbetroffenheit nicht mehr zu besorgen ist. In der Begründung heißt es weiter, Aufzeichnungen von Äußerungen, bei denen zunächst keine Anhaltspunkte für eine Kernbereichsrelevanz vorgelegen haben, seien unverzüglich zu löschen, wenn sich nachträglich herausstellte, dass der Kernbereich berührt wird.

Ich empfehle dringend, diese in der Gesetzesbegründung enthaltenen Vorgaben in eine normkonkretisierende Verwaltungsvorschrift des HMDIS aufzunehmen.

Das nach dem Urteil des BVerfG (a.a.O.) erforderliche Verwertungsverbot für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung findet sich im Gesetzestext.

§ 5 Abs. 4 Satz 3 VerfSchG

Erkenntnisse aus dem Kernbereich privater Lebensgestaltung unterliegen einem Verwertungsverbot.

5.3.1.3 Schutz der Berufsgeheimnisträger

Nicht berücksichtigt wurden im Gesetz meine Vorschläge zum Schutz von Berufsgeheimnisträgern im Rahmen der Wohnraumüberwachung. Ich hatte angeregt, die in § 53 StPO im Rahmen des Zeugnisverweigerungsrechts genannten Personen (u.a. Verteidiger, Rechtsanwälte, bestimmte Beratungsstellen, Journalisten) insoweit zu privilegieren als eine Wohnraumüberwachung nur dann zulässig sein sollte, wenn bei diesen Personen die Voraussetzungen vorliegen, unter denen eine Wohnraumüberwachung beim Verdächtigen erfolgen darf.

Die Begründung des Gesetzentwurfs stellt darauf ab, dass sich für verschiedene Berufsgruppen ein Schutz unmittelbar aus der Verfassung ergebe und deshalb eine Überwachung "in der Regel" nicht in Betracht käme. Aus meiner Sicht wäre gerade die Konkretisierung dieses sich aus verschiedenen verfassungsrechtlichen Vorschriften ableitenden Schutzes von Berufsgeheimnisträgern in einer normenklaren Regelung zur Vermeidung verfassungsrechtlicher Auseinandersetzungen in diesem Fall wichtig und dem Normenvollzug des Gesetzes dienlich. Leider konnte ich mich mit dieser Auffassung nicht durchsetzen.

5.3.1.4 Verwertungsverbot für zu löschende Daten in Sachakten

Auf meinen Vorschlag wurde eine Vorschrift zum Umgang mit Daten in Sachakten in das Gesetz aufgenommen. In Akten, die beispielsweise zu einer verfassungsfeindlichen Organisation geführt werden, befinden sich oftmals personenbezogene Angaben, die als solche z.B. wegen Fristablaufs zu löschen wären. Ich hatte vorgeschlagen, diese Informationen unkenntlich zu machen bzw. ein Verwertungsverbot festzuschreiben. Dem ist der Gesetzgeber jetzt durch die Festlegung eines Verwertungsverbots gefolgt.

§ 6 Abs. 6 Satz 3 VerfSchG

Enthalten Sachakten oder Akten zu anderen Personen personenbezogene Daten, die nach Satz 2 zu löschen sind, dürfen diese nicht mehr verwertet werden.

5.3.1.5 Verfassungsschutzberichte im Internet

Auch die im Gesetz vorgesehene Befristung der Einstellung der Verfassungsschutzberichte in das Internet wurde von mir angeregt. Allerdings halte ich die vorgesehene Frist von fünf Jahren für zu lange.

§ 9 Abs. 3 Satz 3 VerfSchG

Der Bericht darf vom Landesamt für Verfassungsschutz höchstens fünf Jahre im Internet eingestellt werden.

5.3.2 Sicherheitsüberprüfungsgesetz

Das Hessische Sicherheitsüberprüfungsgesetz ist im September 2007 in Kraft getreten. Ich habe zu den verschiedenen Fassungen des Gesetzentwurfs Stellung genommen. Meine Anregungen wurden weitgehend berücksichtigt.

Im Hessischen Sicherheitsüberprüfungsgesetz (GVBl. I 2007 S. 623) 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. Je nach Grad der sicherheitsempfindlichen Tätigkeit wird entweder eine einfache Sicherheitsüberprüfung, eine erweiterte Sicherheitsüberprüfung oder eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen durchgeführt.

Im 35. Tätigkeitsbericht (Ziff. 5.3.1) hatte ich davon berichtet, dass ich in das Gesetzgebungsverfahren eingebunden wurde. In der Diskussion ist das Hessische Ministerium des Innern und für Sport in weiten Teilen meinen Vorschlägen gefolgt, an anderer Stelle konnte ich meine Bedenken zurückstellen.

Wichtig war mir Folgendes:

- Aus meiner Sicht ist im Rahmen der Sicherheitsüberprüfung eine Anfrage bei den hessischen Polizeidienststellen nicht erforderlich, da die dort eventuell vorliegenden Informationen über laufende Ermittlungsverfahren etc. auch vom hessischen Landeskriminalamt zu erhalten sind. Dieser Vorschlag wurde insoweit berücksichtigt, als das Gesetz - anders als der Entwurf - bei einer einfachen Sicherheitsüberprüfung derartige Anfragen nicht vorsieht.

- Das Gesetz sieht im Rahmen der Sicherheitsüberprüfung eine Befragung nicht nur der vom Betroffenen selbst angegebenen sog. Referenzpersonen durch die zuständige Behörde vor, sondern auch von sog. Auskunftspersonen, die die Behörde von sich aus auswählt. Hier habe ich mich dafür eingesetzt, dass derartige Auskunftspersonen nur mit Zustimmung des Betroffenen befragt werden dürfen. Der Betroffene muss gerade in einem derart sensiblen Bereich wissen, welche weiteren Informationserhebungen die zuständige Behörde durchführen will. Verweigert der Betroffene die Zustimmung, muss er sich allerdings auch im Klaren sein, dass daraus negative Schlüsse gezogen werden können. Meinem Anliegen wurde in diesem Punkt insoweit Rechnung getragen, als das Gesetz jedenfalls bei der einfachen und erweiterten Sicherheitsüberprüfung eine Befragung von Auskunftspersonen nur mit Zustimmung des Betroffenen vorsieht.

5.3.3 Prüfung des Dezernats "Bekämpfung der organisierten Kriminalität" beim Landesamt für Verfassungsschutz

Die bei einer im Frühjahr 2006 durchgeführten Prüfung der Datenverarbeitung im Bereich der Beobachtung der organisierten Kriminalität getroffenen Feststellungen führten nach intensiven Gesprächen zur Vereinbarung einer Verfahrensweise, die den datenschutzgerechten Umgang mit den gesammelten Informationen besser unterstützt.

Das LFV hat seit Mai 2002 die zusätzliche Aufgabe der Beobachtung von Bestrebungen und Tätigkeiten der organisierten Kriminalität erhalten.
Im Frühjahr 2006 konnten meine Bediensteten die schon seit längerem geplante Prüfung in diesem neuen Bereich der Datenverarbeitung durchführen.

5.3.3.1 Ansatz der Prüfung

Ansatz für die Prüfung war zum einen ein Ausdruck aus dem nachrichtendienstlichen Informationssystem (NADIS) von den mit dem entsprechenden Aktenzeichen eingestellten Personen und Organisationen. Zum anderen wählte ich aus einer Liste des Verfassungsschutzes Arbeitsschwerpunkte aus und ließ mir zu diesen die entsprechenden Akten aushändigen.

5.3.3.2 Keine vollständige Aktenvorlage

Festzustellen ist, dass bei der Prüfung in mindestens einem Fall nicht die gesamte Akte vorgelegt wurde. Bei Durchsicht dieser Akte fiel auf, dass verschiedene Zusammenhänge aus der Abfolge der in der Akte gesammelten Informationen nicht erklärbar waren. Das LFV räumte am nächsten Tage ein, dass der Akte verschiedene Schriftstücke aus Geheimhaltungsgründen entnommen wurden.
Dieses Verfahren widerspricht dem in § 29 HDSG geregelten Auskunfts- und Einsichtsrecht des Datenschutzbeauftragten.

§ 29 Abs. 1 und 2 HDSG

(1) Alle Daten verarbeitenden Stellen und ihre Auftragnehmer sind verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,

2. Zutritt zu allen Diensträumen zu gewähren.

(2) Die Rechte nach Abs. 1 dürfen nur vom Hessischen Datenschutzbeauftragten persönlich ausgeübt werden, wenn die oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet. In diesem Fall müssen personenbezogene Daten eines Betroffenen, dem von der Daten verarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, auch ihm gegenüber nicht offenbart werden.

In der Vergangenheit habe ich auch in den Fällen, in denen nicht die förmliche Feststellung des Ministeriums nach § 29 Abs. 2 Satz 1 HDSG vorlag, immer die Geheimhaltung von Informationen über vertrauliche Quellen respektiert. Daran hätte ich mich selbstverständlich bei der jetzigen Prüfung wieder gehalten.

Zwischen dem LFV und mir wurde in diesem Zusammenhang noch einmal klargestellt, dass für den Fall, dass Unterlagen wegen des Quellenschutzes aus einer Akte herausgenommen werden, zukünftig Fehlblätter in die Akte einzuheften sind, aus denen der Grund für die Entnahme für mich ersichtlich ist.

5.3.3.3 Tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten der organisierten Kriminalität

Vielen der eingesehenen Akten war gemeinsam, dass der Zeitpunkt für den Beginn der Informationssammlung sehr früh angesetzt ist. Es werden nicht nur allgemeine Informationen, sondern auch personenbezogene Daten bereits zu einem Zeitpunkt erhoben und gespeichert, in dem es oftmals zweifelhaft erscheint, ob tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten der organisierten Kriminalität vorliegen. Nach meinem Eindruck ist es für die Beobachtung der organisier-

ten Kriminalität geradezu typisch, dass die Sammlung von Informationen - insbesondere auch von personenbezogenen Daten - zu einem Zeitpunkt erfolgt, in dem erst geprüft werden soll, ob Anhaltspunkte für Tätigkeiten in diesem Bereich vorliegen. Dies gilt in gleicher Weise für den Einsatz von nachrichtendienstlichen Mitteln, insbesondere von V-Männern oder auch Observationen, die zu einem sehr frühen Zeitpunkt erfolgen.

Diese Prüfungsfeststellungen und die rechtliche Einordnung waren u. a. Gegenstand längerer Erörterungen mit dem HMDIS und Vertretern des LFV, die sich bis zum Sommer hinzogen. Zwar sieht das Gesetz über das LFV in Hessen die Sammlung von Informationen im sog. Prüffall vor.

§ 4 Abs. 1 VerfSchG

Das Landesamt für Verfassungsschutz darf personenbezogene Daten aus allgemein zugänglichen Quellen erheben, um zu prüfen, ob tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen.

Allerdings knüpft das Gesetz an die ausnahmsweise zulässige Erhebung von Daten im Prüffall besondere Rechtsfolgen (beispielsweise keine Speicherung in Dateien oder keine Anlage von Personenakten, kein Einsatz nachrichtendienstlicher Mittel), die für die Arbeit des LFV im Bereich der Beobachtung der organisierten Kriminalität nicht gewollt sind. Die Datenerhebung kann deshalb nicht auf § 4 Abs. 1 VerfSchG gestützt werden. Es bleibt bei der Voraussetzung, dass tatsächliche Anhaltspunkte in der Person des Betroffenen vorliegen müssen.

Das LFV hat mir in diesem Zusammenhang zugesagt, wie folgt zu verfahren: Es wird in regelmäßigen Abständen von ca. drei Monaten geprüft, ob der ausgewählte Bearbeitungsschwerpunkt weiterverfolgt wird. Die Entscheidung, ob tatsächliche Anhaltspunkte für organisierte Kriminalität vorliegen, wird in den Vorgängen klar formuliert und dokumentiert. Sachverhalte, die einem derartigen Bearbeitungsschwerpunkt nicht zugeordnet werden können, werden nicht weiter verfolgt und die Dokumentation dazu wird vernichtet.

Ich werde demnächst prüfen, ob das Verfahren eingehalten wird.

5.3.4 Auskunft über eigene Daten beim Landesamt für Verfassungsschutz

Beim Landesamt für Verfassungsschutz ist ein aus datenschutzrechtlicher Sicht begrüßenswerter Wandel zu mehr Transparenz zu verzeichnen.

Bei allen hessischen Behörden haben Betroffene einen Anspruch auf Auskunft über die zur eigenen Person gespeicherten Daten. Im allgemeinen Datenschutzrecht ist dieses Element des informationellen Selbstbestimmungsrechtes, soweit es sich auf automatisierte Datenspeicherungen bezieht, als Recht auf gebührenfreie Auskunft u.a. über die zur eigenen Person gespeicherten Daten in § 18 Abs. 3 und, soweit es sich auf Datenspeicherungen in Akten bezieht, als Akteneinsichtsrecht in § 18 Abs. 5 HDSG normiert.

Für den Sicherheitsbereich ergibt sich das Informationsrecht aus bereichsspezifischen Regelungen, die den Belangen des jeweiligen Sachgebiets Rechnung tragen. Beispielsweise erkennt § 29 HSOG zwar ein Auskunftsrecht aber kein Akteneinsichtsrecht an. § 185 StVollzG enthält ebenso ein Auskunftsrecht, ein Akteneinsichtsrecht wird erst unter weiteren Bedingungen eingeräumt. Auch berücksichtigen alle Regelungen für den Sicherheitsbereich den Rechtsgedanken, dass durch eine Auskunftserteilung der eigentliche Zweck der Datenspeicherung nicht vereitelt werden darf. Schließlich ist klar, dass etwa ein Verdächtiger einer Straftat durch die Wahrnehmung des Auskunftsrechtes nicht auf eine bevorstehende Ermittlungsmaßnahme aufmerksam gemacht werden darf.

Auch im Bereich des Verfassungsschutzes gibt es das Recht auf Auskunft über Datenspeicherungen zur eigenen Person. § 18 VerfSchG regelt:

§ 18 VerfSchG

(1) Der betroffenen Person ist vom Landesamt für Verfassungsschutz auf Antrag gebührenfrei Auskunft über die zu ihrer Person gespeicherten Daten sowie den Zweck und die Rechtsgrundlage der Verarbeitung zu erteilen.

(2) Abs. 1 gilt nicht, soweit eine Abwägung ergibt, dass das Auskunftsrecht der betroffenen Person gegenüber dem öffentlichen Interesse an der Geheimhaltung der Tätigkeit des Landesamtes für Verfassungsschutz oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten muss. Ein Geheimhaltungsinteresse liegt dann vor, wenn
1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist,
2. durch die Auskunftserteilung Quellen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamtes für Verfassungsschutz zu befürchten ist,
3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen.

Die Entscheidung trifft der Behördenleiter oder ein von ihm besonders beauftragter Mitarbeiter.

(3) Die Auskunftsverpflichtung erstreckt sich nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen.
(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Die Gründe der Auskunftsverweigerung sind aktenkundig zu machen. Wird die Auskunftserteilung

abgelehnt, ist die betroffene Person auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass sie sich an den Hessischen Datenschutzbeauftragten wenden kann. Mitteilungen des Hessischen Datenschutzbeauftragten dürfen keine Rückschlüsse auf den Erkenntnisstand des Landesamtes für Verfassungsschutz zulassen, sofern es nicht einer weitergehenden Auskunft zustimmt.

Bei Inkrafttreten dieser Norm im Jahre 1990 bewertete mein damaliger Amtsvorgänger im 19. Tätigkeitsbericht (Ziff. 8.6) diese Regelung grundsätzlich positiv. Allerdings wurde damals ein differenziert ausgeprägtes Auskunftsrecht für wünschenswert gehalten: z.B. einmal für den Fall, dass Betroffene von Sicherheitsüberprüfungen Auskunft über eigene Daten verlangen und ein anderes Mal für den Fall, dass eine spionageverdächtige Person dasselbe geltend macht. Es wurde seitens meiner Behörde darauf hingewiesen, dass das Auskunftsrecht der sicherheitsüberprüften Person stärker sein müsse, als das des Spionageverdächtigen. Doch die Rechtslage war und blieb für beide Fälle identisch. Es stand lediglich fest, dass Abwägungen im Einzelfall Grundlage für eine Entscheidung über eine Auskunftserteilung oder -verweigerung darstellen müssen. Ein wenig skeptisch schloss die damalige Beurteilung der Auskunftsregelung mit der Feststellung, es bliebe abzuwarten, ob damit ein Stück mehr Transparenz für die Betroffenen erreicht werde.

In den Folgejahren und bis heute erreichen mich regelmäßig Eingaben von Betroffenen nach § 18 Abs. 4 VerfSchG. Die geheimhaltungsbedürftigen Aspekte der jeweiligen Einzelfälle gebieten es, auf eine nachvollziehbare Beschreibung der Einzelfallentscheidungen zu verzichten. Allerdings kann ein allgemeiner Wandel im Auskunftsverhalten des LFV festgestellt werden.

Beispielsweise wurde vor Inkrafttreten des Gesetzes nur in ganz besonders gelagerten Einzelfällen die Auskunft erteilt, dass eine Person der Behörde überhaupt nicht bekannt sei. Mit dem Argument, es könnte sich um einen Spion handeln, der nur einmal feststellen will, ob die Verfassungsschutzbehörde ihn bereits enttarnt habe, wurde oft ein Ausforschungsbemühen angenommen und die Auskunft, wonach der Anfrager der Behörde völlig unbekannt sei, verweigert. Nach Inkrafttreten des Gesetzes ergingen Einzelfallentscheidungen, und an die Annahme eines Ausforschungsbemühens wurden nach und nach höhere Anforderungen gestellt. Heute, knapp zwanzig Jahre nach Inkrafttreten des Gesetzes, erfährt regelmäßig jeder Auskunftssuchende, falls dem so ist, dass er der Behörde nicht bekannt ist. Nur noch bei deutlichen Anhaltspunkten für einen Ausforschungsversuch wird das vorstehende Argument herangezogen. Ich kann jedoch feststellen, dass sich seit Jahren niemand mehr an mich gewandt hat, dem die Auskunft aus diesem Grunde verweigert wurde.

Aber auch für den Fall, dass der Behörde Informationen zur Person vorliegen, ist ein Wandel zu mehr Transparenz zu verzeichnen. Aufgrund der Regelung in § 18 Abs. 4 darf meine Mitteilung an den Betroffenen, der sich nach einer Auskunftsverweigerung an mich gewandt hat, keine Rückschlüsse auf den Erkenntnisstand der Behörde zulassen, wenn das LFV einer weitergehenden Auskunft nicht zustimmt. So konnte ich in früheren Jahren den Betroffenen nach datenschutzrechtlicher Prüfung oft nur mitteilen, die Prüfung habe ergeben, dass die datenschutzrechtlichen Belange des Anfragers nicht verletzt wurden. Bei jeder datenschutzrechtlichen Kontrolle eines Einzelfalles habe ich - soweit ich es für angebracht hielt - das LFV um Zustimmung zu einer etwas weitergehenden Auskunft gebeten. Auch wenn den Betroffenen selbst klar sein musste, dass ihre Aktivitäten beispielsweise in einem bestimmten Extremismusbereich Anlass einer Datensammlung des LFV sein müsste, so ist es doch "ein Stück" mehr an Transparenz, wenn die Behörde den Betroffenen dies ausdrücklich unter Bezeichnung des Extremismusbereiches bestätigt. Mittlerweile - dies entnehme ich den Unterlagen, die mir Petenten nach dem Hinweis des LFV nach § 18 Abs. 4 Satz 3 zuschicken - macht das LFV selbst solche Angaben. Auch die Frage von Petenten nach konkreten Angaben - z.B. zu den gespeicherten Informationen oder an welche Stellen möglicherweise gespeicherte Informationen weitergegeben wurden - werden punktuell und im Einzelfall beantwortet. Insgesamt ist damit ein aus datenschutzrechtlicher Sicht begrüßenswerter Wandel zu verstärkter Transparenz zu verzeichnen.

5.4 Ausländerrecht

5.4.1 Prüfung von Ausländerbehörden

Anlassunabhängig habe ich im Berichtszeitraum bei der Ausländerbehörde des Hochtaunuskreises in Bad Homburg und der Ausländerbehörde der Stadt Fulda eine Datenschutzprüfung vorgenommen. Gravierende Mängel wurden nicht festgestellt. Korrekturbedarf besteht offensichtlich bei der Anwendung des neuen Freizügigkeitsgesetzes. Die Unterbringung der Ausländerbehörde der Stadt Fulda ist dringend verbesserungsbedürftig.

5.4.1.1 Anwendung des Freizügigkeitsgesetzes

Als einer von mehreren Prüfungsansätzen wurden stichprobenartig Akten eingesehen, in denen das seit 1. Januar 2005 in Kraft getretene Gesetz über die allgemeine Freizügigkeit von Unionsbürgern (FreizügG/EU) zur Anwendung kommt. Dieses Gesetz regelt die Einreise und den Aufenthalt von Staatsangehörigen anderer Mitgliedstaaten der Europäischen Union (Unionsbürger) und ihrer Familienangehörigen. § 2 des Gesetzes regelt das Recht auf Einreise und Aufenthalt und bestimmt, wer gemeinschaftsrechtlich freizügigkeitsberechtigt ist.

§ 2 FreizügG/EU

(1) Dieses Gesetz regelt die Einreise und den Aufenthalt von Staatsangehörigen anderer Mitgliedstaaten der Europäischen Union (Unionsbürger) und ihrer Familienangehörigen.

(2) Gemeinschaftsrechtlich freizügigkeitsberechtigt sind
1. Unionsbürger, die sich als Arbeitnehmer, zur Arbeitssuche oder zur Berufsausbildung aufhalten wollen,
2. …

Die vorläufigen Anwendungshinweise zum Freizügigkeitsgesetz legen abschließend fest, welche Dokumente für die Ausstellung der Freizügigkeitsbescheinigung vorzulegen sind.

Nr. 5.3.1.1.2 VAH-FreizügG/EU

Falls im Einzelfall nicht auf eine Prüfung verzichtet werden kann, können von einem freizügigkeitsberechtigten Unionsbürger nur folgende von der Freizügigkeitsrichtlinie abschließend vorgegebene Dokumente gefordert werden:

- gültiger Personalausweis oder Reisepass

- bei Erwerbstätigen: Einstellungsbescheinigung des Arbeitgebers oder Beschäftigungsbescheinigung; Nachweis der Selbständigkeit

- bei Nichterwerbstätigen: …

Für einen in Deutschland arbeitenden Unionsbürger sind also außer beispielsweise dem Nationalpass und dem Arbeitsvertrag keine sonstigen Unterlagen zu fordern. In den Akten der beiden Ausländerbehörden fanden sich aber regelmäßig weitere Dokumente, die zur Erteilung der von den Ausländerbehörden auszustellenden Freizügigkeitsbescheinigung nicht notwendig waren. Beispielsweise waren den Akten über den erforderlichen Nachweis der Erwerbstätigkeit hinaus Bescheinigungen über das Bestehen eines Kranken- oder Rentenversicherungsverhältnisses, Gesundheitserklärungen zu Krankenversicherungsanträgen, Abschriften aus Grundbüchern, Kopien von Mietverträgen und weitere Dokumente zu entnehmen. Solche Unterlagen entgegenzunehmen kann in besonders gelagerten Einzelfällen von Nichterwerbstätigen durchaus angebracht sein. Sie im Falle der Erwerbstätigkeit regelmäßig zur Akte zu nehmen war aber schlicht überflüssig, datenschutzrechtlich ausgedrückt "nicht erforderlich" und damit unzulässig.

Beide Ausländerbehörden sagten mir zu, ab sofort auf die überflüssige Datenerhebung zu verzichten. Eingereichte Unterlagen, bei denen offensichtlich ist, dass sie nicht zur konkreten Aufgabenerfüllung benötigt werden, sind nicht zu den Akten zu nehmen. Die Mitarbeiter der Ausländerbehörden wurden entsprechend informiert. Im Hochtaunuskreis wurden auch die kreisangehörigen Gemeinden informiert, weil diese alternativ die Antragsunterlagen entgegennehmen.

5.4.1.2 Weitere Prüfansätze

Weitere Kontrollansätze waren die Prüfung der Beachtung datenschutzrechtlicher Aspekte

- bei der Entgegennahme von Verpflichtungserklärungen nach § 68 des Aufenthaltsgesetz,

- bei dem Verfahren zur Ermittlung sog. Scheinehen und

- bei der Beteiligung der Sicherheitsbehörden vor Erteilung von Aufenthaltstiteln.

Die Prüfung führte bei beiden Ausländerbehörden zu keinen Beanstandungen.

5.4.1.3 Räumliche Situation der Ausländerbehörde der Stadt Fulda

In der Ausländerbehörde der Stadt Fulda findet der gesamte Publikumsverkehr in einem Raum statt. Dort sind drei Schreibtische nahezu unmittelbar nebeneinander angeordnet. Durch diese räumliche Nähe lässt es sich nicht vermeiden, dass alle an einem Arbeitsplatz geführten Gespräche an den beiden anderen Arbeitplätzen von den jeweils vorsprechenden Personen gewollt oder ungewollt mitgehört werden. Ich habe der Stadtverwaltung mehrere Vorschläge unterbreitet wie sie diese Situation verbessern kann. Letztendlich kann ich der Stadtverwaltung nicht vorschreiben, welche konkreten organisatorischen Maßnahmen zu treffen sind. Die Stadtverwaltung hat mir zugesagt, bei einer in Kürze anstehenden Umplanung der Anordnung der Arbeitsplätze in der Ausländerbehörde für Abhilfe zu sorgen. Die Umsetzung steht noch aus.

5.4.2 Elektronische Bearbeitung im Aufenthalts- und Einbürgerungsverfahren

Auch in der Ausländerverwaltung hält E-Government Einzug. Im Aufenthalts- und Einbürgerungsverfahren werden Verfahrensabschnitte elektronisch ausgestaltet. eAufenthalt und eEinbürgerung verfolgen unterschiedliche Konzepte. Ich berate das federführende Hessische Ministerium des Innern und für Sport bei der Einführung der elektronischen Systeme.

5.4.2.1 eAufenthalt

Die hessischen Ausländerbehörden sind zuständig für das Aufenthaltsverfahren bzw. die Entscheidung über eine Aufenthaltserlaubnis für einen ausländischen Bürger. Zur Erfüllung dieser Aufgaben bedarf es eines umfangreichen Datenaustauschs mit anderen Behörden.

In einer Vielzahl der Aufenthaltserlaubnisverfahren ist eine Anfrage an das HLKA und an das LFV vorgesehen mit dem Ziel dort festzustellen, ob Erkenntnisse über den Antragsteller vorliegen. Falls diese Behörden über Informationen verfügen, kann dies für die Erteilung der Aufenthaltserlaubnis eine Rolle spielen.

§ 73 Abs. 2 und 3 AufenthG

(2) Die Ausländerbehörden können zur Feststellung von Versagungsgründen gemäß § 5 Abs. 4 oder zur Prüfung von Sicherheitsbedenken vor der Erteilung oder Verlängerung eines sonstigen Aufenthaltstitels, die bei ihr gespeicherten personenbezogenen Daten der Betroffenen Person an…das Landesamt für Verfassungsschutz und das Landeskriminalamt übermitteln…

(3) Die in den Absätzen 1 und 2 genannten Sicherheitsbehörden und Nachrichtendienste teilen der anfragenden Stelle unverzüglich mit, ob Versagungsgründe nach § 5 Abs. 4 oder Sicherheitsbedenken nach Absatz 2 vorliegen…

Die gesetzliche Regelung wurde durch Erlass des HMDIS vom 10. Mai 2007 dahingehend konkretisiert, dass eine derartige Anfrage bei Personen zu erfolgen hat, die eine bestimmte in der Anlage 1 des Erlasses genannte Staatsangehörigkeit besitzen.

Nach Angaben des HMDIS erreichen die Anfragen bei dem HLKA und LFV einen jährlichen Umfang von zehn- bis zwanzigtausend. Aufgrund dieses erheblichen Arbeitsvolumens ist vorgesehen, zunächst den Austausch mit diesen beiden Behörden elektronisch auszugestalten. In einem nächsten Schritt sollen dann weitere beteiligte Behörden, wie andere Ausländerbehörden, Meldebehörden, die Staatsanwaltschaft in Hessen, Generalbundesanwalt - Bundeszentralregister, Bundesamt für Migration und Flüchtlinge angeschlossen werden.

Im Rahmen von eAufenthalt sollen die bisherigen Informations- und Kommunikationswege zwischen den beteiligten Stellen nicht geändert werden; nur in technischer Hinsicht wird die Kommunikation per Postweg durch die elektronische Kommunikation über eine EDV-gestützte Plattform ersetzt. Insgesamt verspricht man sich dadurch eine Beschleunigung des Verfahrens und eine Entlastung für die Verwaltung.

Die technische Realisierung soll mit einem BizTalk-Server erfolgen, der als Kommunikationsserver eingehende Nachrichten entgegennimmt, diese nach den technischen Schnittstellenanforderungen des Empfängers konvertiert und für den Empfänger in einem "Empfangsbriefkasten" bereithält. Der Empfänger kann die Nachrichten dann nach seinen Erfordernissen abholen. Bei der Konvertierung werden nur Datenformate, bzw. das Schema für die Darstellung, angepasst. In der Nachricht selbst werden keine Daten verändert, gelöscht oder hinzugefügt. Jede Nachricht gelangt in genau einen Empfangsbriefkasten. Deshalb muss die Ausländerbehörde für jede Zielbehörde eine eigene Anfrage (automatisch) generieren.

Um unbefugte Zugriffe zu verhindern, wurden eine Reihe von Maßnahmen ergriffen:

- Die Kommunikation zu den Ausländerbehörden und anderen teilnehmenden Behörden, z. Z. LFV und HLKA, erfolgt SSL-verschlüsselt über HTTPS.

- Der Kommunikationsaufbau wird von den Versendern bzw. Empfängen aufgebaut. Das BizTalk-System spielt keine aktive Rolle.

- Die Verbindungen der verschiedenen Systeme (ekom21, LKA, LFV) zum BizTalk-Server werden explizit definiert. Andere Verbindungen sind nicht zugelassen.

- Die zentralen Systeme der eAufenthalt-Plattform sind in besonders gesicherten Rechnerräumen untergebracht.

- Es findet keine dauerhafte Datenspeicherung auf dem BizTalk-Server statt, und Datensicherungen werden nicht vorgenommen. Die Anfrage-Daten werden nur für die Dauer einer Anfrage vorgehalten. Die Log-Dateien zum Kommunikationsfluss werden maximal drei Wochen gespeichert. Es werden keine Sicherungen der SQL-Datenbank des BizTalk-Servers gemacht. D.h. sobald eine Sicherheitsüberprüfungsanfrage erfolgreich beantwortet wurde und drei Wochen vergangen sind, sind keine Daten über die Anfrage mehr in eAufenthalt vorhanden.

- Die gesamte Plattform ist ein eigenständiges System mit eigener Benutzerverwaltung. Benutzer beteiligter Verwaltungen können nur auf die eigenen "Briefkästen" zugreifen. Diese und die Zugriffe der Administration werden protokolliert und stehen für Revisionszwecke zur Verfügung.

Wenn die Maßnahmen richtig und konsequent umgesetzt werden, sind die datenschutzrechtlichen Anforderungen an die IT-Sicherheit der eAufenthalt-Plattform erfüllt. Im Gesamtzusammenhang spielen allerdings auch die angeschlossen Systeme der teilnehmenden Behörden eine wichtige Rolle. So müssen die Fachverfahren sicherstellen, dass nur die einzelnen Behörden und deren Mitarbeiter Anfragen für sich stellen können und auch nur sie die Antworten zur Kenntnis erhalten.

Bei der Beteiligung des HLKA und des LFV geht es in einzelnen Fällen um sehr sensible Daten, beispielsweise um Ausführungen zu Straftaten oder Erkenntnisse über die Mitgliedschaft in verfassungsfeindlichen Organisationen. Wichtig war mir deshalb die Festlegung, dass vom LFV keine inhaltlichen Aussagen übermittelt werden, sondern nur die Feststellung "es liegt etwas vor". Weitere Ausführungen zur Speicherung müssen deshalb - wie bisher auch - in Briefform erfolgen. Auf diese Weise wird zweierlei erreicht: Für den Betroffenen sensible Informationen werden nicht in das elektronische System eingestellt. Darüber hinaus ist sichergestellt, dass keine automatisierte Übernahme von Informationen erfolgen kann, sondern es immer der Zusammenstellung und Wertung durch einen Behördenmitarbeiter bedarf.
Beim HLKA werden im Rahmen von eAufenthalt zwar Informationen über die Art der Straftat übermittelt, z.B. Anzeige wegen zu schnellen Fahrens. Alles Weitere - wie etwa Angaben zum Ausgang des jeweiligen Strafverfahrens - hat konventionell zu erfolgen. Es gibt allerdings Pläne, die Abfrage beim HLKA weiter zu automatisieren. An der Diskussion beteilige ich mich.

eAufenthalt soll bei der Ausländerbehörde der Stadt Frankfurt ab Dezember d.J. in Betrieb gehen, die weiteren Ausländerbehörden werden dann im Laufe des nächsten Jahres folgen.

5.4.2.2 eEinbürgerung

Auch am Einbürgerungsverfahren sind eine Vielzahl von Behörden beteiligt. Hinzu kommt, dass sich das Einbürgerungsverfahren über verschiedene Verwaltungsstufen erstreckt: Die unteren Verwaltungsbehörden (Gemeinden über 7.500 Einwohner ansonsten die Landkreise) nehmen die Einbürgerungsanträge entgegen, vervollständigen sie und führen beispielsweise auch den erforderlichen Test über ausreichende Deutschkenntnisse des Ausländers durch. Sie händigen ggf. auch die Einbürgerungsurkunde aus. Die Entscheidung über die Einbürgerung obliegt den Regierungspräsidien als Einbürgerungsbehörden. Vor der Entscheidung sind Stellungnahmen verschiedener Behörden über den Einbürgerungsbewerber einzuholen, beispielsweise von den Ausländerbehörden, die für den Betroffenen zuständig waren, vom LFV, vom HLKA, vom BZR. Dem HSL ist nach positiver Entscheidung über die Einbürgerung Mitteilung für die Einbürgerungsstatistik zu machen. Auf der dritten Stufe koordiniert das HMDIS den Verwaltungsvollzug und übt Aufsichtsbefugnisse aus.

Die Zahl der Einbürgerungsfälle in Hessen schwankt, pro Jahr sind es etwa 20.000. eEinbürgerung soll zum einen die Dauer des Verfahrens verkürzen und damit auch Anreize für die Einbürgerung schaffen sowie die beteiligten Behörden entlasten.

Da es sich bei eEinbürgerung um ein sehr komplexes System handelt, wurde im Gesetz zur Bestimmung der zuständigen Behörden in Staatsangehörigkeitsangelegenheiten vom 21. März 2005 (GVBl. I S. 229, 234) ein gemeinsames automatisiertes Verfahren gewählt.

§ 3 Abs. 2 Gesetz zur Bestimmung der zuständigen Behörden in Staatsangehörigkeitsangelegenheiten

Das für das Staatsangehörigkeitsrecht zuständige Ministerium kann ein gemeinsames automatisiertes Verfahren für die Bearbeitung von Einbürgerungsverfahren einrichten. Es kann die nach § 2 Abs. 1 zuständigen Behörden verpflichten, das gemeinsame automatisierte Verfahren zu nutzen. § 15 Abs. 1 Satz 2-4, Abs. 2 HDSG gilt entsprechend.

Das Verfahren eEinbürgerung unterscheidet sich von dem unter Ziff. 5.4.2.1 beschriebenen Verfahren eAufenthalt. Mit eAufenthalt werden nur Anfragen an andere Behörden und die dazugehörigen Antworten übertragen; es findet keine dauerhafte Datenspeicherung statt, und jede beteiligte Stelle greift nur auf Daten zu, die ausschließlich ihr zugeordnet sind.

Demgegenüber wird in dem Verfahren eEinbürgerung für jeden Antrag eine elektronische Akte angelegt, die der für die Einbürgerung zuständigen Behörde, dem Regierungspräsidium, zugeordnet ist. Andere Behörden wie beispielsweise Kommunen, Polizei oder Verfassungsschutz übermitteln Daten und Dokumente über einen Formularserver in die Akte. Sie haben lesenden Zugriff in den Akten auf die Dokumente, in deren Bearbeitung sie eingebunden sind. Es handelt sich daher um ein gemeinsames Verfahren nach § 15 HDSG.

Das Verfahren eEinbürgerung bedient sich für die Führung der elektronischen Akte des Dokumentenmanagement-Systems DOMEA. Beschäftigte verschiedener Behörden haben schreibenden oder lesenden Zugriff auf die elektronische Akte. Die Daten werden bis zur Löschung, also für lange Zeiträume, gespeichert. In dieser Zeit werden Datensicherungen vorgenommen und andere für den Betrieb des Verfahrens nötige Arbeiten durchgeführt. Die Daten können daher von den beteiligten Stellen und auch vom Personal des Betreibers, der HZD, zur Kenntnis genommen werden. Zugriffe unbefugter Personen müssen durch die Datensicherheitsmaßnahmen der HZD und die verfahrensspezifischen Sicherheitsvorkehrungen verhindert werden. Für die Übertragung ist eine Verschlüsselung mittels SSL vorgesehen, während für die Anwendung die Zugriffskontrolle des Dokumentenmanagementsystems greift. Die HZD verhindert mit räumlichen und technischen Maßnahmen auf Ebene des Servers unbefugte Zugriffe.

Die Vorteile für den Anwender liegen auf der Hand: Die beteiligten Behörden auf allen drei Verwaltungsstufen arbeiten mit derselben elektronischen Einbürgerungsakte und können sich also auch jederzeit über den Stand des Verfahrens informieren.

Auch hier habe ich Wert darauf gelegt, dass Informationen aus den Datenspeicherungen des LFV nicht in die elektronische Datei eingespeist, sondern konventionell verschickt und bearbeitet werden.

Das Verfahren wurde von den drei Regierungspräsidien, der Stadt Frankfurt, der Gemeinde Büttelborn, der Stadt Gießen und dem Schwalm-Eder-Kreis als Pilotprojekt getestet. In der Ausländerbehörde der Stadt Frankfurt läuft das Verfahren seit März 2007 im Echtbetrieb.

5.5 Verkehrswesen

5.5.1 Verfahrensprotokolle beim Kraftfahrt-Bundesamt helfen wirksamen Datenschutz herzustellen

Auch für die Polizei sind Abrufe im automatisierten Verfahren aus dem Verkehrszentralregister nur im Rahmen der gesetzlichen Zweckbestimmung zulässig.

Ein Bürger bat mich, eine vermutete Datenschutzverletzung aufzuklären, die ihn sehr beunruhigte. Der Petent hatte während einer mehrtägigen Abwesenheit seinen Pkw in der Nähe seiner Wohnung auf einem ausgewiesenen öffentlichen Parkplatz abgestellt. Während dieser Zeit wurde sein Vermieter von einem ihm unbekannten Mann befragt, ob der Petent in seinem Haus wohne, da dessen Pkw vom Abstellort entfernt werden müsse. Er habe die Daten des Petenten bei der Polizei erfragt. Der Petent war im Nachhinein über diesen Vorfall sehr betroffen, da er und seine Lebensgefährtin in der Vergan-

genheit wiederholt Belästigungen eines sog. Stalkers ausgesetzt waren und nun erneute Zudringlichkeiten befürchteten. Für ihn war nicht nachvollziehbar, warum die Polizei Auskunft über seine Daten erteilt hatte.

Mit Hilfe von Protokolldateien konnte der Sachverhalt aufgeklärt werden. Die Auswertung der Protokollierungen des Zentralen Verkehrsinformationssystem (ZEVIS) beim Kraftfahrt-Bundesamt ergab, dass die Abfrage vom Mitarbeiter einer Polizei-Einsatzzentrale in Mittelhessen veranlasst wurde. Von dort erfolgte schließlich die Erklärung: Ein Nachbar hatte das parkende Fahrzeug des Petenten als angebliche Verkehrsbehinderung für seine Hofeinfahrt angezeigt. Da das Fahrzeug ordnungsgemäß geparkt war, konnte eine polizeiliche Maßnahme wie Abschleppen/Umsetzen nicht erfolgen. Eine Funkstreife, die den Sachverhalt vor Ort hätte aufklären können, war nicht verfügbar. Der Mitarbeiter veranlasste eine Abfrage beim Kraftfahrt-Bundesamt. Da der Halter in der Nähe des Nachbarn wohnsitzmäßig gemeldet war, bat der Mitarbeiter der Einsatzzentrale den Nachbarn, mit dem Halter selbst Kontakt aufzunehmen und gab ihm dafür die entsprechenden Daten bekannt. Der Nachbar traf jedoch nur den Vermieter an.

Gemäß §§ 35, 36 Abs. 1 Nr. 1b StVG kann die Polizei Halterabfragen aus ZEVIS tätigen, wenn es um die Verfolgung von Verkehrsordnungswidrigkeiten oder um die Abwendung von Gefahren für die öffentliche Sicherheit geht. Da das Fahrzeug des Petenten ordnungsgemäß geparkt war, lag weder ein Verstoß gegen die Straßenverkehrsordnung vor noch bestand eine öffentliche Gefährdung. Die Datenabfrage war nicht vom Gesetzeszweck gedeckt und daher unzulässig.

Zwar konnten die Folgen der Datenschutzverletzung nicht rückgängig gemacht werden. Mit der Aufklärung des Falles konnte der Petent aber zumindest von der Sorge einer befürchteten Belästigung durch den Stalker befreit werden. Darüber hinaus veranlasste die betroffene Behördenleitung eine innerdienstliche Aufklärung über die datenschutzrechtlichen Belange im Zusammenhang mit Abfragen aus dem Verkehrszentralregister. Ich gehe deshalb davon aus, dass dort zukünftig Verstöße nicht mehr vorkommen werden.

5.5.2 Keine Auskünfte aus den örtlichen Fahrzeugregistern an die Gebühreneinzugszentrale zur Ermittlung der Gebührenpflicht für Autoradios

Die GEZ hat keinen Anspruch auf Auskunft aus den Fahrzeugregistern, um säumige Gebührenzahler zu ermitteln. Auch bei der Suche nach nicht angemeldeten Autoradios fehlt der für eine Datenübermittlung notwendige Bezug zur Teilnahme am Straßenverkehr.

Im Berichtszeitraum erhielt ich eine Anfrage von einem hessischen Landesverband, ob die Übermittlung von Zulassungsdaten aus den Fahrzeugregistern an die GEZ zulässig sei. Ferner erging ein Rundschreiben des HMWVL an die hessischen Kfz-Zulassungsstellen zum gleichen Thema. Dies veranlasste mich, auch gegenüber dem Hessischen Rundfunk die Voraussetzungen klarzustellen, unter denen die Landesrundfunkanstalten bzw. die GEZ Auskünfte aus den örtlichen Fahrzeugregistern erhalten können. Danach gilt Folgendes:

1. Nach § 35 Abs. 1 Nr. 4 StVG können Fahrzeug- und Halterdaten zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung übermittelt werden. Im Zusammenhang mit der Feststellung von Gebührenschuldnern, die ihrer Anzeigepflicht gemäß § 3 des Rundfunkgebührenstaatsvertrages nicht nachgekommen sind, kann von einer Gefährdung der die öffentlichen Sicherheit und Ordnung nicht gesprochen werden, so dass § 35 Abs. 1 Nr. 4 StVG keine Anwendung findet.

2. Nach § 39 Abs. 3 Nr. 1a StVG muss der Empfänger glaubhaft machen, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung von öffentlich-rechtlichen Ansprüchen in Höhe von jeweils mindestens 500 Euro benötigt. Diese Bestimmung setzt danach eine bereits bestehende öffentlich-rechtliche Forderung in Höhe von mindestens 500 Euro voraus. Die Vorschrift bietet deshalb keine Rechtsgrundlage für eine Auskunftserteilung zur Prüfung der Frage, ob überhaupt eine Forderung besteht.

3. Nach § 35 Abs. 1 Nr. 3 StVG kann eine Datenübermittlung erfolgen, wenn dies zur Verfolgung von Ordnungswidrigkeiten erforderlich ist. Zum einen sind die Rundfunkanstalten für die Verfolgung von Ordnungswidrigkeiten nicht zuständig, zum anderen geht es hier auch nicht um die Verfolgung einer Ordnungswidrigkeit, sondern (zunächst) um die Klärung der Frage, ob überhaupt der Verdacht einer Ordnungswidrigkeit besteht.

4. Nach § 39 Abs. 1 StVG ist eine Datenübermittlung zur Verfolgung von Rechtsansprüchen möglich, wenn es sich um einen Anspruch im Zusammenhang mit der Teilnahme am Straßenverkehr handelt. Gemeint sind hier z.B. Schadensersatzansprüche aus Verkehrsunfällen. Bei Auskunftsersuchen von Rundfunkanstalten, um Schuldner von Rundfunkgebühren (Autoradio) ausfindig zu machen, fehlt dieser Zusammenhang.

Daraus ergibt sich, dass für den Hessischen Rundfunk (HR) und die GEZ keine rechtliche Möglichkeit besteht, Auskünfte aus den örtlichen Fahrzeugregistern zu erhalten, um Gebührenschuldner zu ermitteln, die ihrer Anzeigepflicht gemäß § 3 des Rundfunkgebührenstaatsvertrages nicht nachkommen. Ich habe den HR aufgefordert, künftig den Versuch zu unterlassen, bei den Zulassungsbehörden unberechtigterweise Halterdaten zu erfragen und gebeten, die GEZ entsprechend anzuweisen.

Der HR hat zwischenzeitlich reagiert und seine Außendienstmitarbeiter angewiesen alle Anfragen an die Kfz-Zulassungsstellen in Hessen einzustellen. Er behielt sich jedoch vor, eine eigene Prüfung der Rechtslage durchzuführen, deren Ergebnis bei Redaktionsschluss jedoch noch nicht vorlag.

5.6 Schulen und Schulverwaltung

5.6.1 LUSD - Zentrale Lehrer- und Schülerdatenbank

Die Einführung der zentralen Lehrer- und Schülerdatenbank (LUSD), eines der großen E-Government-Projekte der Hessischen Landesregierung, ist komplex und gestaltet sich schwierig; insbesondere gilt es neben technischen auch eine Vielzahl von datenschutzrechtlichen Problemen zu bewältigen. In die Problembewältigung bin ich frühzeitig eingebunden worden, so dass datenschutzrechtliche Beratung und antizipierende Kontrolle ineinander fließen.

Mit der Einführung der zentralen LUSD verfolgt das HKM die Ziele, die Verwaltungsarbeit an den Schulen zu vereinfachen, den Informationsfluss zwischen Schulen, Schulämtern und Ministerium durch ein landesweites Schulnetz zu verbessern und durch stets aktuelle Daten die Planung der Unterrichtsabdeckung und der Schulentwicklung zu optimieren. In der Lehrer- und Schülerdatenbank sollen die Daten von rund 50.000 Lehrern und 660.000 Schülern an ca. 2.000 Schulen verwaltet werden.

5.6.1.1 Verfahren

5.6.1.1.1 Die alte LUSD

Bereits in meinem 24. Tätigkeitsbericht habe ich mich mit dem bis zur Umstellung im Schuljahr 2006/2007 eingesetzten dezentralen Verfahren LUSD beschäftigt. Vom Hessischen Institut für Bildungsplanung und Schulentwicklung wurde Mitte der 90er Jahre in Zusammenarbeit mit der HZD ein Nachfolgesystem zur "Schüler-Individual-Datei" (SID) und dem Verwaltungsprogramm "Gymnasiale Oberstufe (GO)" entwickelt. Dieses Programm LUSD war eine landesweit eingesetzte Schulverwaltungssoftware für hessische Schulen fast aller Schulformen. Es handelte sich um eine Datenbank, in der die Daten von Schülerinnen und Schülern, deren Erziehungsberechtigten und denjenigen, denen die Erziehung oder Pflege anvertraut ist, über die besuchten Unterrichtsveranstaltungen sowie den dort erzielten Leistungen (Noten) und den Unterrichtseinsatz der Lehrkräfte gespeichert und verarbeitet wurden. Das Produkt wurde ab dem Schuljahr 1995/96 an den Schulen eingesetzt und in den folgenden Jahren regelmäßig aktualisiert.

Seit 2002 liefern die Schulen ihre Statistik-Daten per Diskette über die jeweiligen Schulämter an die HZD. Die Daten sind anonymisiert und werden im Kultus-Data-Warehouse (KDW) für Planungs- und Entwicklungszwecke ausgewertet und dem HKM zur Verfügung gestellt. Weitere Daten erhält das Landesamt für Statistik für seine jährlichen Auswertungen.

5.6.1.1.2 Die neue LUSD

Mit der neuen Version der LUSD werden die gleichen Daten in einer operativen Datenbank zusammengeführt, die auf einem Server in der HZD angelegt ist und dort betreut wird. Die personenbezogenen Schülerindividualdatensätze werden von der Schule angelegt und gepflegt, die die Schülerinnen und Schüler jeweils besuchen. Auf diesen Datensatz hat grundsätzlich auch nur die Schule Zugriff, der die Schülerinnen bzw. die Schüler angehören. Bei einem geplanten Schulwechsel kann die zur Aufnahme vorgesehene Schule einen Blick auf die zur Aufnahmeentscheidung notwendigen Schülerdaten erhalten. Dies wird durch die Zuordnung eines Kandidatenstatus ermöglicht. Erst mit der endgültigen Aufnahmeentscheidung übergibt die abgebende Schule die Zugriffsberechtigung an die aufnehmende Schule.

Auswertungen und Berichte in der LUSD sind nur schulbezogen und nur von den berechtigten Mitarbeiterinnen und Mitarbeitern der Schulen erstellbar. Es handelt sich im Wesentlichen um Serienbriefe, Klassen- und Kurslisten.

5.6.1.1.3 Unterschiede alte LUSD/neue LUSD

Der wesentliche Unterschied der neuen zur alten LUSD-Anwendung liegt darin, dass alle Schulen - im Rahmen ihrer Zugriffsrechte - auf dieselbe Datenbank zugreifen. Die bisherige LUSD-Anwendung wurde an jeder Schule individuell installiert, hatte nur ihren eigenen Datenbestand und auch nur Zugriff auf diesen. Mit der übergreifenden Speicherung der Daten in einer zentralen Datenbank wurden auch nachfolgende Änderungen bzw. Erweiterungen vorgenommen:

- Zentrale Pflege und Bereitstellung von Basisdaten
  Es handelt sich um nicht personenbezogene Daten (bisher als Katalogdaten bezeichnet), die für alle Schulen gleich sind, z.B. Listen von Orten, Schulämtern, Fächern, Schulformen, Stundentafeln oder Aufzählungen wie amtliche Bezeichnungen für Dienst, Lehramt, Funktion oder einfache Wertelisten für Anrede, Kursart, Kursoption.

- Schulspezifische, nicht personenbezogene Basisdaten
  Sie können wie in der alten LUSD pro Schule verwaltet werden. Sie sind in der neuen LUSD-Anwendung nur für die jeweilige Schule sichtbar. Dies betrifft im weitesten Sinn das schulische Umfeld von den Schulen der Umgebung bis zur Raumsituation der Schule.

- Schulübergreifende Verwaltung von Schülerdaten
  Die Daten zu jedem Schüler werden nicht mehrfach (d.h. einmal pro besuchte Schule) vorgehalten. Zu jedem Schüler wird nur ein Datensatz schulübergreifend in der Datenbank gespeichert. Dabei gehört die Datenhoheit über die Daten eines Schülers immer jeweils der Schule, die er besucht.

- Schulübergreifende Unterrichtsformen und Kooperationen
  Bei schulübergreifenden Unterrichtsformen (z.B. gemeinsame Leistungskurse benachbarter Gymnasien) werden Schülerdaten in beiden beteiligten Schulen genutzt. Der Schulleiter der Schule, an der der Unterricht stattfindet, benötigt für die Unterrichtsorganisation einen Teil der Daten der Schüler der Stammschule (z.B. für namentliche Klassenliste, Kontakt zu Schülern). Schreibenden Zugriff hat er nur auf die Unterrichts- und Leistungsdaten, für die seine Schule Verantwortung trägt. Die Gesamtverantwortung verbleibt bei der Stammschule.

- Differenzierung der Zugriffsberechtigung innerhalb der Schule
  Die Konzeption des Berechtigungskonzeptes folgt dem Grundsatz, dass den Anwendern der Zugriff ausschließlich auf diejenigen Daten eingeräumt wird, die ihnen elektronisch oder schriftlich bereits auch schon jetzt zur Erfüllung ihrer Aufgaben zur Verfügung stehen, und zwar ausschließlich im Rahmen der dienstlichen Erforderlichkeit. Über die Zugriffsrechte an der Schule entscheiden die Schulleiterinnen und Schulleiter. Das alte LUSD-Programm ließ die Profile "Schulleiter" (Zugriff auf alle Daten) und "Sekretärin" (nur Zugriff auf Schülerdaten) zu. Hinzu kam die Rolle des Administrators bzw. der Administratorin. In der neuen LUSD wurde das Konzept um die Rollen Abteilungsleiter/in und Schulzweigleiter/in sowie Lehrer bzw. Lehrerin erweitert. Die Zugriffsberechtigung bzw. Beschränkung ergibt sich aus den jeweiligen Zuständigkeiten. Soweit die Schulleitung Aufgaben delegiert, kann sie auch die entsprechende Rolle delegieren.

5.6.1.2 Einführungsstrategie in Stufen

Die Einführung der zentralen LUSD erfolgt in mehreren Stufen:

1. Migration aller Schulen in die zentrale LUSD (s. Ziff. 5.6.1.2.1)
2. Anbindung der LUSD an das KDW (s. Ziff. 5.6.1.2.2)
3. Elektronische Übermittlung der Daten aus den Meldeämtern (s. Ziff. 5.6.1.2.3)
4. Anbindung der LUSD an SAP R/3 HR (s. Ziff. 5.6.1.2.4)
5. Zugriffsmöglichkeiten des HKM und der Staatlichen Schulämter (s. Ziff. 5.6.1.2.5)

5.6.1.2.1 Migrationen aller Schulen

Mit der Implementierung der neuen Software wurde im Oktober 2006 begonnen. Die ersten Migrationen fanden ohne erkennbare größere Probleme statt. Im Laufe des Schuljahres 2006/2007 wurden alle Daten aller Schulen auf die zentrale Datenbank übernommen. Die Situation eskalierte Ende des Schuljahres 2006/2007 und Anfang des Schuljahres 2007/2008, als besonders viele Datenbankzugriffe zugleich erfolgten. Die Sekretariate klagten zunehmend über Datenverluste und Leitungsprobleme. Im Laufe des Entwicklungsprojektes wurde Prozess- bzw. Business-Logik auf dem Datenbank-Server statt auf dem Application-Server abgebildet. Bei hoher Beanspruchung war die Datenbank überlastet, dies ergab Wartezeiten. Diese Wartezeiten führten zu einem Abbruch der Datenverarbeitung mit der Folge des Verlusts der eingegebenen Daten. Zur Problemlösung muss die gesamte Struktur der Datenbank überarbeitet werden. Mit einem neuen Programm ist erst Mitte 2008 zu rechnen.

5.6.1.2.2 Anbindung der LUSD an das Kultus-Data-Warehouse

Die Statistikdaten sollen direkt durch Datenabzug an das KDW elektronisch übermittelt und von dort an das Landesamt für Statistik weitergeleitet werden. Der bisher praktizierte Versand von Disketten entfällt. Bei Erstellung dieses Berichts waren allerdings die davon betroffenen Datenkataloge und die notwendigen Änderungen der diesbezüglichen Rechtsgrundlagen noch nicht derart konkretisiert, dass sie an dieser Stelle dargestellt werden könnten. Man kann festhalten, dass das Verfahren selbst eine Änderung erfahren wird, da bundesweit der Vergleich von Schülerkarrieren geplant ist. Hierfür wird eine eigene Vorabkontrolle erforderlich. Ob die bestehenden Rechtsgrundlagen ausreichen, wird zurzeit noch geprüft. Auch die technische Gestaltung ist noch nicht abschließend geklärt.

5.6.1.2.3 Daten aus den Meldeämtern

Zur Überprüfung der Erfüllung der Schulpflicht wurden bisher die Daten der einzuschulenden Kinder über die staatlichen Schulämter an die Schulen übermittelt. Die geplante Änderung der Meldedatenübermittlungsverordnung sieht hier eine Vereinfachung vor (s. auch Ziff. 5.6.2): Die Daten der betroffenen Kinder sollen aus den Meldeämtern direkt in die LUSD-Datenbank eingespeist werden. Folgende Daten werden übermittelt:

1. Familienname
2. Vorname
3. Tag und Ort der Geburt
4. Geschlecht
5. Gesetzlicher Vertreter/Vertreterin (Vor- und Zuname, Doktergrad, Tag der Geburt)
6. Staatsangehörigkeiten
7. Gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch die frühere Anschrift aus dem Inland

5.6.1.2.4 Anbindung der LUSD an SAP R/3 HR

Die Stammdaten von Lehrkräften und Daten über ihren Unterrichtseinsatz sollen gespeichert und verarbeitet werden. Es ist geplant, die schulrelevanten Stammdaten direkt über eine Schnittstelle aus dem Verfahren SAP R/3 HR zu importieren. Folgende Daten sind vorgesehen:

1. Name, Vorname
2. Geburtsort
3. Lehrbefähigung
4. Lehrämter
5. Nationalität
6. sonstige Qualifikationen
7. Unterrichtserlaubnisse
8. SAP-Personalnummer
9. amtliche Funktionsbeschreibung
10. Adresse

5.6.1.2.5 Zugriffsmöglichkeiten des HKM und der Staatlichen Schulämter

In einem späteren Release ist geplant, dass die staatlichen Schulämter, die Schulträger und das HKM Inforollen erhalten. Hierdurch soll ein Zugriff auf Berichte und Reports aus der LUSD ermöglicht werden.

5.6.1.3 Datenschutzrechtliche Bewertung

Die datenschutzrechtliche Bewertung bezieht sich nur auf die Stufe 1 der Einführungsstrategie, die weiteren Stufen sind noch nicht so weit konkretisiert, dass eine Bewertung möglich ist.

5.6.1.3.1 Gemeinsames Verfahren nach § 15 HDSG

Wenn mindestens zwei Daten verarbeitende Stellen gemeinsam und automatisiert auf dieselben Datenbestände oder Teile davon zugreifen können, bin ich nach § 15 Abs. 1 HDSG vor Einführung des Verfahrens anzuhören. Dabei sind mir die in Satz 4 erwähnten Angaben und Unterlagen zu überlassen.

Eine Besonderheit bei der Einführung der zentralen LUSD machte ein solches Beteiligungsverfahren notwendig.

§ 15 Abs. 1 HDSG

Die Einrichtung eines automatisierten Verfahrens, das mehreren Daten verarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Benutzung des Verfahrens ist im Einzelfall nur erlaubt, wenn hierfür die Zulässigkeit der Datenverarbeitung gegeben ist. Vor der Einrichtung oder Änderung eines gemeinsamen Verfahrens ist der Hessische Datenschutzbeauftragte zu hören. Ihm sind die Festlegungen nach Abs. 2 Satz 1, das Verfahrensverzeichnis nach § 6 Abs. 1 und das Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3 vorzulegen.

Wie oben unter Ziff. 2.3 dargestellt, können beim sog. Kandidatenverfahren mehrere Schulen auf bestimmte Schülerdaten zumindest lesend zugreifen. Neben der Stammschule sind dies die Schulen, bei denen sich die Schülerinnen bzw. Schüler vor einem beabsichtigten Schulwechsel als Interessent anmelden. Das Verfahren lässt nur den Zugriff auf diejenigen Schülerdaten zu, die die Schulleitung für ihre sachgerechte Entscheidung über die Übernahme der Schülerin bzw. des Schülers benötigt, also auf Schülerdaten, die für die anstehende Entscheidung erforderlich sind. Statt eines solchen Lesezugriffs wäre es zwar auch möglich gewesen, die relevanten Auskünfte bei den Betroffenen selber einzuholen oder sich die Schülerakte zusenden zu lassen und diese einzusehen. Der Online-Zugriff stellt demgegenüber die schnellere und - da nicht auf alle Daten zugegriffen werden kann - auch die datenschutzfreundlichere Variante dar. Die in § 15 Abs. 1 HDSG notwendige Abwägung mit den schutzwürdigen Interessen der Schülerinnen und Schüler ergab deshalb die Feststellung, dass das Verfahren datenschutzrechtlich angemessen ist. Ansonsten stand im Mittelpunkt der datenschutzrechtlichen Bewertung der Unterlagen die in § 15 Abs. 1 Satz 4 erwähnte Vorabkontrolle.

5.6.1.3.2 Die Vorabkontrolle (Stufe 1)

§ 7 Abs. 6 HDSG verlangt für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung eine gutachtliche Bewertung der einzelnen Gefahren für das informationelle Selbstbestimmungsrecht unter den Aspekten der rechtlichen Zulässigkeit sowie der technischen und organisatorischen Datensicherheit (Vorabkontrolle).

§ 7 Abs. 6 HDSG

Wer für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist, hat vor dem Beginn der Verarbeitung zu untersuchen, ob damit Gefahren für die in § 1 Abs. 1 Nr. 1 geschützten Rechte verbunden sind; dies gilt in besonderem Maße für die in § 7 Abs. 4 genannten Daten. Das Verfahren darf nur eingesetzt werden, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen

verhindert werden können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten.

Durchzuführen ist die Vorabkontrolle von demjenigen, der für den Einsatz oder die wesentliche Änderung des Verfahrens zuständig ist. Die LUSD soll in den Schulen landeseinheitlich eingeführt werden. Die Konzeption und die Gesamtsteuerung lagen und liegen beim HKM. Gleichwohl bleiben die Schulen aber für ihren Bereich die nach dem HDSG verantwortlichen Daten verarbeitenden Stellen. Bei der Konzeption der Vorabkontrolle in § 7 Abs. 6 HDSG waren solche Szenarien, wie sie bei landeseinheitlichen Verfahren anzutreffen sind, bereits absehbar. Deshalb trifft die Pflicht zur Erstellung der Vorabkontrolle denjenigen, der für den Einsatz zuständig ist. Insoweit das HKM zentrale Vorgaben für den Einsatz des Verfahrens macht, hat es folglich auch die Vorabkontrolle zu erstellen. Da es sich bei der LUSD um ein gemeinsames Verfahren nach § 15 HDSG handelt, trifft den Federführer hier die Pflicht, die Vorabkontrolle durchzuführen, sofern sie nicht durch IT-technische und organisatorische Detailvorgaben der jeweiligen Schulen für ihren Bereich ergänzt werden muss. Dies wurde mit der Erstellung eines **Musters** bewältigt, in dem die generellen Vorgaben behandelt und die von den Schulen zu ergänzenden Angaben gekennzeichnet sind, die jeweils in die Schlussbewertung einzubeziehen sind. Dieses Muster gibt den Rahmen für die einzelnen Schulen, überlässt es ihnen aber, die bei ihnen jeweils zu bewertenden Gefahren und die Gegenmaßnahmen detailliert im Rahmen ihrer eigenen Ergänzung zu beschreiben. Außerdem müssen die Schulen, soweit die einzelnen Vorgaben die dort vorhandene IT-Sicherheitsstruktur verändern, ihr eigenes nach § 10 Abs. 2 HDSG und entsprechend Nr. 5.2 der IT-Sicherheitsleitlinie notwendiges Sicherheitskonzept erstellen bzw. fortschreiben. Das Muster der Vorabkontrolle hat das HKM wegen der zahlreichen, teils neuen datenschutzrechtlichen Fragestellungen mit mir abgestimmt.

5.6.1.3.3 Umsetzung der Datenschutzmaßnahmen

Bereits im Oktober 2004 hat mich das HKM über die Planung der LUSD informiert, seit diesem Zeitpunkt begleite ich das Projekt datenschutzrechtlich.

Im Februar 2005 lag mir der erste Entwurf der Vorabkontrolle für die Migration der Schulen vor. Er war noch unzureichend und ich hatte folgende Forderungen formuliert:

1. Durchführung des Beteiligungsverfahren nach § 15 HDSG
2. Überarbeitung der Vorabkontrolle und des Verfahrensverzeichnisse
3. Transparenz für den Nutzer über seine gespeicherten Daten
4. klare Beschreibung aller technischer Details des Verfahrens
5. Beschreibung und Festlegung der rechtlichen Daten-Übermittlungen.

Die überarbeitete Vorabkontrolle lag mir am 12. Juli 2006 im Rahmen des § 15 HDSG zur Stellungnahme vor. Sie war umfangreich und bestand aus folgenden Elementen:

1. Vorabkontrolle
2. Sicherheitskonzept LUSD
3. Sicherheitskonzept Netz
4. Sicherheitskonzept Internetzugang
5. Sicherheitskonzept E-Mail
6. Gesamtverzeichnis nach § 15 HDSG
7. Erlassentwurf Einführung der neuen LUSD und Vorgaben zur IT-Sicherheit und Datenschutz
8. Schnittstelle SAP R/3 HR und LUSD
9. Formblatt zur Ergänzung der Vorabuntersuchung durch die Schule
10. Überblick über die in der LUSD verarbeiteten Daten
11. Zuordnung von Rollen und Masken.

Insbesondere die technischen Konzepte waren detailliert und durchdacht. Da im Juli 2006 die Migrationen der Schulen auf die zentrale LUSD noch nicht begonnen hatte, konnte ich die beschriebenen Maßnahmen nicht überprüfen. Dennoch stellte ich in den Unterlagen einige Unstimmigkeiten fest und bestand auf Nachbesserung der nachstehenden Punkte:

1. Erstellung von Muster-Sicherheitskonzepten für die Datenverarbeitung in den Schulen
2. Präzisierung und Umsetzung der in den Sicherheitskonzepten "LUSD" und "Netzanbindung" beschriebenen Maßnahmen

2.1 Sicherheitskonzept LUSD, insbesondere IT-Sicherheitsmanagement, Notfallplanung, Behandlung von Sicherheitsvorfällen, Festlegung der verantwortlichen Personen, vertragliche Festlegungen

2.2 Sicherheitskonzept Netzanbindung Schulen, insbesondere des IT-Sicherheitsmanagements

3. Fertigstellung der Entwürfe der Sicherheitskonzepte "E-Mail" und "Internetzugang"

Bei Redaktionsschluss war der Stand der datenschutzrechtlichen Unsetzung wie folgt:

Zu 1.
Erstellung von Sicherheitskonzepten für Schulen
Die Notwendigkeit "Muster-Sicherheitskonzepte" zu erstellen und umzusetzen, ist seit langem unumstritten. Bisher mangelte es an den fachlichen und personellen Ressourcen. Im Rahmen der zentralen LUSD hat das HKM für diese Aufgabe ab

dem 1. August 2007 für ein Jahr eine Kraft vom Schulamt abgeordnet. Diese wird eine Arbeitsgruppe leiten, die sich mit der Erstellung mit "Muster-Sicherheitskonzepten" befasst. Mit diesen ist im Frühsommer 2008 zu rechnen.

Zu 2.
Präzisierung und Umsetzung der Sicherheitsmaßnahmen in den Sicherheitskonzepten "LUSD" und "Netzanbindung"

Hierbei handelt es sich im Wesentlichen um organisatorische Maßnahmen. Deshalb sah die ursprüngliche Planung vor, diese Präzisierung und Umsetzung während des "Roll-Outs" (Migration der Schulen) durchzuführen.

Aufgrund der schwerwiegenden technischen Probleme blieb hierfür leider keine Zeit. Hier muss im Zuge der Überarbeitung der LUSD erheblich nachgebessert werden.

Zu 3.
Fertigstellung der Entwürfe der Sicherheitskonzepte "E-Mail" und "Internetzugang"

Die Sicherheitskonzepte sind fertiggestellt, liegen mir seit März 2007 vor und sind nicht zu beanstanden.

Wie in Ziff. 5.6.1.4.2 beschrieben, müssen die Schulen eine eigene Vorabkontrolle vornehmen. Das HKM hat im Dezember 2006 den Erlass "Einführung der neuen LUSD und Vorgaben zur Gewährleistung der IT-Sicherheit und Datenschutz an staatlichen hessischen Schulen" vom 23. November 2006 I. 7-640.000.010-27 im Amtsblatt 12/06 veröffentlicht und darin angekündigt, dass die Schulen die Muster-Vorabkontrolle in Form einer CD erhalten, damit sie auf dieser Basis die abschließende Vorabkontrolle selbst vornehmen können.

Der Versand der Disketten erfolgte im Juni 2007. Die Vorabkontrolle durch die Schulen wurde, soweit ich ersehen konnte, bisher nicht durchgeführt.

5.6.1.4 Ergebnisse weiterer Prüfungen

Im Laufe des Jahres 2007 habe ich mehrere Prüfungen durchgeführt. Bei der Einführung kam es zu einigen datenschutzrechtlichen Pannen.

5.6.1.4.1 Umsetzung durch die Schulträger

Bei der Einführung der zentralen LUSD wurden die Schulträger vor die Aufgabe gestellt, die notwendige technische Infrastruktur bis zum ersten Router der Zentralanbindung zur Verfügung zu stellen und darauf zu achten, dass die lokalen Systemkonfigurationen keine Sicherheitslücken enthalten, die einen unbefugten Zugang zu den Daten der zentralen LUSD bzw. zu den Systemen erlauben würden.

Dabei haben sich die Schulträger, die die Sachmittelausstattung der Schulen bereitstellen, dieser Aufgabe landesweit auf sehr unterschiedliche Weise angenommen. Auf Grund ihrer unterschiedlichen strukturellen Voraussetzungen, zum Teil bereits bestehender Netze und dem auch noch nach Schultyp und Ausstattungszeitpunkt sehr differierenden heterogenen Gerätebestand ergaben sich verschiedenste Lösungen. Es wurden sowohl einzelne Arbeitsplätze, die nicht mit dem eigentlichen Schulverwaltungsnetz verbunden sind, für das Arbeiten mit der zentralen LUSD bereitgestellt als auch komplette, bereits bestehende Schulverwaltungsnetze nach einigen Anpassungen insgesamt angebunden.

Drei Schulträger haben den Anschluss der Schulverwaltungsrechner zum Anlass genommen, gemeinsam alle Rechner ihres Zuständigkeitsbereichs auf ein einheitliches technisches Niveau zu bringen. Die einheitliche Ausstattung von Hard- und Software sollte insbesondere den in den kommenden Jahren zu leistenden Support-Aufwand minimieren und gewährleisten, dass die lokalen Systeme dauerhaft in einer sicheren Konstellation betrieben werden. Bei der Umsetzung wurde aber nicht berücksichtigt, dass die Schule Daten verarbeitende Stelle im Sinne des § 2 Abs. 3 HDSG ist und damit die Verantwortung für die Verarbeitung der Schüler- und Lehrerdaten auch über die LUSD hinaus bei der Schulleitung liegt.

§ 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.

Den Schulen wurde in den bereitgestellten Systemumgebungen alle Möglichkeiten zur Wahrnehmung ihrer Aufgaben entzogen. Sie hatten keinerlei Einsicht in die Systemprotokolle und konnten auch die System-Einstellungen von Betriebssystem und Anwendungen nicht überprüfen.

Grundsätzlich hat eine Behördenleitung sonst auch keine unmittelbaren Zugriffsrechte auf der beschriebenen Systemebene. Aber sie kann ständig eigenes Personal oder einen Auftragnehmer anweisen, die Systemzustände stichprobenhaft oder anlassbezogen zu kontrollieren und die entsprechenden Systembereiche zur Kontrolle sogar unmittelbar zugänglich zu machen bzw. notwendige Änderungen sofort umzusetzen. In der hier gegebenen Konstellation - die Schulleitungen haben gegenüber dem Personal des Schulträgers keinerlei Weisungsbefugnis - war das nicht mehr möglich.

Ich habe die Schulträger aufgefordert, die Handlungsfähigkeit der Schulleitungen durch eine Änderung der Systemeinstellungen wieder herzustellen. Da sich die notwendigen Kontrollfunktionen nicht ohne weiteres mit den Berechtigungen eines normalen Systembenutzers verbinden lassen, wird den Schulen zunächst wieder ein Konto mit administrativen Rechten

einzurichten sein. In einem weiteren Schritt kann ein Konzept zu einer aufgabengerechten Rechtezuweisung an die Schulleitungen erarbeitet werden.

Außer diesem grundsätzlichen Konzeptfehler zeigten sich neben weiteren Details noch zwei wichtige Problembereiche:

- Durch die Vereinheitlichung der Hardware wurde es erforderlich, die Festplatten der Altrechner vor einer Wiederverwendung oder Entsorgung der Geräte sicher zu löschen. Die Schulträger hatten zwar ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziertes Verfahren dafür vorgesehen, aber nicht bedacht, dass dieser Vorgang bei älteren Geräten deutlich länger als 24 Stunden dauern kann. Das hätte bei den mehreren hundert Geräten der drei Schulträger einen immensen personellen Aufwand erfordert. Daher wurden neue Überlegungen angestellt, wie man die Festplatten, deren weitere Verwendung nicht wirtschaftlich ist, mit geringerem Aufwand bzw. zu geringeren Kosten entsorgen kann. Ich habe die Schulträger darauf hingewiesen, dass dafür nur noch eine physikalische, thermische oder magnetische Zerstörung der Datenträger in Frage kommt, die in jedem Fall dazu führt, dass die Magnetisierungsschicht der einzelnen Festplatten-Scheiben nicht mehr lesbar ist. Eine solche Dienstleistung wird fachgerecht in aller Regel nur durch spezialisierte Entsorgungsfirmen erbracht.

- Einsatz einer Fernzugriffs-(Remote-Support-)Software in einer nicht zulässigen Konfiguration
  Um innerhalb einer Schule möglichst effizient die einzelnen Verwaltungsrechner administrieren zu können, hatten die erwähnten drei Schulträger mit der Neukonzeption der LUSD-Arbeitsplatzrechner die Verwendung einer Software zum Fernzugriff vorgesehen, bei der das Monitorbild eines entfernten Rechners über das interne Netzwerk an das lokale System übertragen wird und die lokalen Mausbewegungen und die Tastaturanschläge zur Steuerung des anderen Gerätes eingesetzt werden. Man kann dann mit wenigen Einschränkungen so arbeiten, wie an einem lokalen Gerät.

  Die hier eingesetzte Variante der Software VNC (Virtual Network Computing) wurde allerdings nicht richtig konfiguriert. Remote-Controle-Software darf nur eingesetzt werden, wenn der Benutzer des fernadministrierten Rechners aktiv einer Abfrage zur Aufschaltung zugestimmt hat und danach ständig durch einen entsprechenden optischen Hinweis auf die Aktivität des Programms aufmerksam gemacht wird. Er muss ferner jederzeit die Möglichkeit haben, die Verbindung zum administrierenden Rechner zu unterbrechen. Darüber hinaus sollten die Einstellungen und die anfallenden Anwendungsprotokolle der Software nach Möglichkeit in einem geschützten Bereich hinterlegt werden, der idealerweise nur nach dem Vier-Augen-Prinzip zugänglich ist. Insbesondere die Frage nach dem Schutz der Einstellungen und der Protokolle ist nur mit zusätzlichem Aufwand zu realisieren. Die Schulträger haben sich nach meiner Kritik dazu entschlossen, die Software komplett auf allen ausgelieferten Rechnern zu deinstallieren.

  Am geschilderten Beispiel wird deutlich, dass die Schulen und Schulträger auf die Fragestellungen, wie die Sicherheit der LUSD-Arbeitsplätze insgesamt auszugestalten ist, nur unzureichend vorbereitet waren und in diesen Punkten einer stärkeren allgemeinen Hilfestellung durch das federführende HKM bedurft hätten. Ich gehe davon aus, dass sich mit der Erstellung der bereits in Ziff. 5.6.1.4.3, letzter Absatz angesprochenen Mustersicherheitskonzepte die Situation landesweit auch für verschiedenste Vor-Ort-Konstellationen auf ein einheitliches Niveau heben lässt.

5.6.1.4.2 Unberechtigte Zugriffe auf die Daten der LUSD

Im August des vergangenen Jahres unterrichtete mich das HKM über einen Programmfehler im Modul "Passwortmanagement". Bei Namensgleichheiten sei ein unberechtigter Zugriff auf die Datenbank möglich gewesen. Der Fehler sei erkannt und bereits behoben.

Im September wurde ich mit dem Problem abermals konfrontiert, als sich ein Schulleiter an mich wandte. Zwei Kollegen anderer Schulen hatten ihm mitgeteilt, dass es ihnen möglich wäre, von ihren Schulen auf die Daten seiner Schule zuzugreifen. Die Vorfälle seien unverzüglich dem zentralen LUSD-Support, den zuständigen staatlichen Schulämtern und dem HKM zur Kenntnis gegeben worden, aber noch nicht abgestellt. Ich wandte mich an das HKM und bat um sofortige Aufklärung. Es ergab sich folgender Sachverhalt:

- Entgegen ursprünglicher Konzeptüberlegungen wurde auf Grund netzwerktechnischer Gegebenheiten darauf verzichtet zu prüfen, ob eine Benutzeranmeldung an die zentrale LUSD und der Standort des Rechners, von dem diese Anmeldung erfolgt, zueinander passen. Dadurch können die Benutzerkennungen landesweit an allen schulischen Arbeitsplätzen mit LUSD-Anbindung zum Zugang benutzt werden, sofern das entsprechende Passwort bekannt ist. Dies ist in Fällen, in denen Bedienstete für mehrere Schulen tätig sind, u.U. auch von praktischer Bedeutung, birgt aber Risiken, die ich bei der Fortentwicklung des Verfahrens noch gesondert betrachten werde.

- Bei der Festlegung des Standards für die Benutzerkennungen hat die Projektleitung entschieden, den Benutzernamen nicht mit dem Schulnamen bzw. einer Referenznummer zu verbinden, wie das in anderen landesweiten Systemen der Fall ist, bei denen die Dienststellennummer dem Benutzernamen vorangestellt ist. Da zusätzlich in den Anmeldenamen nur der erste Buchstabe des Vornamens einfließt, kommt es bei häufig vertretenen Nachnamen zu Namensdubletten, wie z.B.: AMustermann, AMustermann1, AMustermann2, AMustermann11, AMustermann12.

  Die zur Unterscheidung vom System ergänzte, laufende Ziffer verhindert nicht, dass es bei einer Fehleingabe relativ schnell zum Aufruf einer falschen Benutzerkennung kommt (z.B. wenn AMustermann11 versehentlich nur AMustermann1 eintippt).
- Diese Rahmenbedingungen allein würden aber bei einem korrekt funktionierenden Verfahren nur dann zu einem unberechtigten Zugriff führen, wenn zu einer irrtümlich aufgerufenen Benutzerkennung das richtige Passwort bekannt ist.

Die Gewährung des Zugriffs auf fremde Datenbestände kam letztendlich zu Stande, weil ein Fehler im Ablauf der Passwort-Wechselroutinen beim Testen und Freigeben nicht aufgefallen war. Dadurch wurde bei einer Kennung, deren Passwort fristgemäß abgelaufen war, die Passwortwechselroutine ausgeführt, ohne dass der Benutzer durch das Altpasswort am System authentifiziert wurde. Der versehentliche Aufruf einer Benutzerkennung, deren Passwort abgelaufen war, führte also mit dessen Neuvergabe zu einem umfassenden Zugriff.

Wie uns das Hessische Kultusministerium mitgeteilt hat, wurde dieser Fehler durch eine Programmänderung am 27. August 2007 behoben. Leider bestand das Problem über diesen Zeitpunkt fort bei allen Benutzerkennungen, deren Passwort vorher durch einen anderen Benutzer geändert wurde. Der jeweils zuständige schulische Administrator musste bei allen Kennungen, von denen er nicht sicher sein konnte, dass sie von den jeweils Berechtigten seiner Schule eingesetzt wurden, das Passwort überschreiben.

Auch wenn mir bis Redaktionsschluss keine weiteren Fälle bekannt geworden sind, die auf dem geschilderten Programmfehler beruhen, werde ich bei der Fortentwicklung der Anwendung darauf hinwirken, dass in das Verfahren eine Plausibilitätskontrolle integriert wird, mit der die landesweite Verwendung der Anwenderkennungen eingeschränkt werden kann, und die zu einer auswertbaren Protokollierung im zentralen Verfahren führt.
Auffälligkeiten können dann schneller erkannt und hinterfragt werden.

5.6.1.4.3 Internet-Nutzung

Mit der Einführung der LUSD und dem Aufbau eines landesweiten Schulnetzes ist es allen Schulen möglich, den gesicherten Internetzugang über die HZD zu nutzen. In dem Sicherheitskonzept "Internetzugang" ist den Schulnetzen ein weiterer ungesicherter Netzzugang untersagt. Bei meinen Prüfungen musste ich aber feststellen, dass diese Vorgabe nicht eingehalten wurde.

5.6.1.5 Ausblick

Die vorliegenden technischen Konzepte sind nicht zu beanstanden. Wenn alle dort beschriebenen Maßnahmen umgesetzt werden und die Ergebnisse und Forderungen meiner Prüfungen berücksichtigt werden, bestehen keine datenschutzrechtlichen Bedenken gegen den Einsatz der LUSD in der 1. Stufe.

5.6.2 Änderung der Meldedatenübermittlungsverordnung zur Überwachung der Schulanmeldungen

Zur effektiven Kontrolle der rechtzeitigen Anmeldung schulpflichtig werdender Kinder durch die Schulen, soll der Datenaustausch zwischen den Meldeämtern und den Schulen in eine datenschutzrechtlich korrekte und überwiegend automatisierte Verfahrensweise überführt werden.

Das HMDIS beteiligte mich bei dem Entwurf zur Änderung des § 17 Abs. 1 der MeldDÜVO. Diese Vorschrift erlaubt die Datenübermittlung zwischen den Meldeämtern und den Schulen zur Überwachung der Schulanmeldung schulpflichtig gewordener Kinder durch die Schulen. Nach § 58 HSchulG tritt die Schulpflicht grundsätzlich mit Vollendung des sechsten Lebensjahres ein, und zwar zum 1. August des jeweiligen Jahres. Die Eltern haben entsprechend die Schulanmeldung vorzunehmen. Dies ergibt sich aus § 67 Abs. 1 HSchulG.

§ 67 Abs. 1 HSchulG

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

Soweit die Eltern diesen schulrechtlichen Pflichten nicht nachkommen, kann dies zu einem Bußgeldtatbestand führen nach § 181 Abs. 1 Nr. 2 HSchulG.

Die Erfüllung dieser Pflicht muss von der jeweils örtlich zuständigen Grundschule überwacht werden. Dies wurde bisher ermöglicht, indem die Meldeämter den zuständigen Schulen über die staatlichen Schulämter digitalisierte Datensätze zu den betroffenen Kindern überließen, die in das schulische Standardverwaltungsprogramm LUSD dort eingespielt wurden.

Im Zuge der generellen Aktualisierung der MeldDÜVO war beabsichtigt, den hier betroffenen § 17 Abs. 1 den neuen IT-Strukturen in der Schulverwaltung anzupassen.

Im Rahmen meiner Stellungnahme zum Entwurf nahm ich zugleich die Gelegenheit wahr, den Weg des Datentransfers datenschutzrechtlich zu korrigieren. Der letzte Satz des Abs. 1 sah bisher nämlich vor, dass die Datensätze über die jeweils zuständigen staatlichen Schulämter an die Schulen weitergeleitet wurden. Da das Schulgesetz im Zusammenhang mit der Überwachung der Erfüllung der Schulpflicht nur der örtlich jeweils zuständigen Grundschule, nicht aber den staatlichen Schulämtern Aufgaben zuweist, ist der Datenweg über diese Ämter datenschutzrechtlich nicht zulässig. Nach § 58 Abs. 1 sind schulpflichtige Kinder bei der örtlich zuständigen Grundschule, nicht beim Schulamt anzumelden. Die ursprünglich vom HKM in der Neufassung des § 17 Abs. 1 geforderte Variante, dass der Datenweg über das HKM gehen solle, habe ich aus diesem Grund abgelehnt.
Im Zuge der Neufassung des § 17 Abs. 1 prüfte ich auch die Frage der Erforderlichkeit der insgesamt sieben Einzeldaten zum betroffenen Kind:

- Familiennamen

- Vornamen
- Tag und Datum der Geburt
- Geschlecht
- gesetzliche Vertreterin/gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt)
- Staatsangehörigkeiten
- gegenwärtige und frühere Anschriften. Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch die letzte frühre Anschrift im Inland.

Zu diskutieren war u.a. die Frage, inwieweit auch die Angabe der Haupt- und Nebenwohnung eines Kindes erforderlich ist. Das HKM erläuterte dazu, dass die Schulleitung danach beurteilen könne, wo sich der räumliche Lebensmittelpunkt des Kindes befindet. Dieser ist nach § 60 Abs. 4 HSchulG relevant für die Frage der örtlich zuständigen Grundschule, weshalb die Übermittlung erforderlich ist.

Im Gegensatz zur bisherigen Regelung soll der neue § 17 Abs. 1 nicht mehr Weg und Technik der Datenübermittlung festlegen. Bei den Erörterungen erhielt ich die Auskunft, dass dieser Datentransfer künftig direkt erfolgen soll, über eine Einspielung der jeweiligen Datensätze pro Schule in die bei der HZD zentral verarbeiteten LUSD-Daten der Schulen (vgl. Ziff. 5.6.1). Die Meldeämter haben insoweit künftig eine entsprechende Lieferpflicht gegenüber der HZD, die allerdings noch programmtechnisch zu entwickeln ist. Den datenschutzrechtlichen Erfordernissen ist dadurch entsprochen.

5.6.3 Verfahren zum Nachteilsausgleich für schwerbehinderte Lehrkräfte gemäß der Pflichtstundenverordnung

Das förmliche Verfahren zur Beantragung einer Pflichtstundenermäßigung für schwerbehinderte Lehrkräfte ist datenschutzrechtlich nicht zu beanstanden. Allerdings war das von einem Staatlichen Schulamt verwendete Formular einer Erklärung der Entbindung von der ärztlichen Schweigepflicht unpräzise bzw. missverständlich formuliert. Meinen Vorschlag zur Änderung der Erklärung hat das Schulamt übernommen.

5.6.3.1 Die Eingabe eines schwerbehinderten Lehrers

Ein schwerbehinderter Lehrer wandte sich an mich, weil er im Zusammenhang mit einer beantragten Stundenermäßigung vom Gesundheitsamt ein Formular zur Unterschrift vorgelegt bekommen hatte, wonach er seine Zustimmung zur Aufhebung der ärztlichen Schweigepflicht geben solle, um medizinische Informationen zu seiner Person an das RP Gießen übermitteln zu können. Der Betroffene verweigerte dies mit dem Hinweis, seinen Arbeitgeber bzw. das RP gingen diese Informationen nichts an. Mich bat er hierzu um eine datenschutzrechtliche Stellungnahme.

5.6.3.2 Das Verfahren zur Ermäßigung der Pflichtstundenzahl

Gemäß § 17 der Verordnung über die Pflichtstunden der Lehrkräfte, über die Anrechnung dienstlicher Tätigkeiten und über Pflichtstundenermäßigungen (Pflichtstundenverordnung) vom 20. Juli 2006 (ABl. Nr. 08/2006, S. 631) kann das Staatliche Schulamt auf Antrag eine Pflichtstundenermäßigung von zwei Wochenstunden gewähren, wenn die Notwendigkeit dieses Nachteilsausgleichs vom Gesundheitsamt bescheinigt wird.

§ 17 Verordnung über die Pflichtstunden der Lehrkräfte

Lehrkräften sowie Sozialpädagoginnen und Sozialpädagogen, die Schwerbehinderte nach § 2 Abs. 2 SGB IX sind, kann das Staatliche Schulamt auf Antrag eine Pflichtstundenermäßigung von zwei Wochenstunden gewähren, wenn die Notwendigkeit dieses Nachteilsausgleichs vom Gesundheitsamt bescheinigt wird. Wenn das Gesundheitsamt eine höhere Pflichtstundenermäßigung empfiehlt und der Medizinaldienst des Regierungspräsidiums Gießen dieser Empfehlung zustimmt, kann eine weitere Ermäßigung von bis zu drei Wochenstunden gewährt werden. Die Pflichtstundenermäßigungen sind je nach Art der Behinderung zu befristen. Jede Änderung des Gesundheitszustandes oder der dienstlichen Voraussetzungen ist dem Staatlichen Schulamt zu melden; dieses kann seine Entscheidung jederzeit ändern oder aufheben.

Die Beantragung durch den Betroffenen erfolgt formlos und gegenüber dem Schulamt. Dieses erteilt einen Untersuchungsauftrag beim Gesundheitsamt mit der Maßgabe, Mitteilung darüber zu machen, ob und in welchem Umfang eine Pflichtstundenermäßigung in Frage kommt. Wird vom Gesundheitsamt eine Reduzierung von mehr als zwei Stunden empfohlen, soll es den Betroffenen eine Erklärung zur Entbindung von der Schweigepflicht unterschreiben lassen, damit eine Weiterleitung der Unterlagen an die dann zuständige Medizinalaufsicht beim RP Gießen erfolgen kann.

Der Antragsteller erhält vom Schulamt vor dem Untersuchungstermin ein Schreiben, in dem auf die Einschaltung des Gesundheitsamtes hingewiesen wird. Auch wird ihm mitgeteilt, welche Unterlagen vom Gesundheitsamt benötigt werden. Außerdem wird auf die Schweigepflichtentbindungserklärung mit dem Hinweis verwiesen, diese zu unterschreiben, wenn die Ermäßigung drei Stunden betragen solle.

Ist dies nämlich der Fall, gehen die Unterlagen zusammen mit der Empfehlung des Gesundheitsamtes zur Medizinalaufsicht beim RP Gießen, die hessenweit zuständig ist. Dort wird im weiteren Verlauf des Verfahrens in der Regel nach Aktenlage entschieden. Zur Beurteilung des Sachverhaltes fordert die Medizinalaufsicht folgende Daten vom Betroffenen an, soweit sich diese nicht bereits in den vom Gesundheitsamt gelieferten Unterlagen befinden:

- Anzahl der Stunden
- Art der Fächer

- Kopie des Schwerbehindertenausweises
- Kopie des Bescheides des Versorgungsamtes.

In Einzelfällen kann es dennoch zu Rückfragen der Medizinalaufsicht beim Gesundheitsamt kommen.

5.6.3.3 Die Schweigepflichtentbindung

Das Schulamt hatte ein Formular mit folgendem Inhalt konzipiert:
"Hiermit entbinde ich das Stadtgesundheitsamt von seiner Schweigepflicht gegenüber dem RP Gießen, was die medizinischen Unterlagen und Auskünfte zu meinem Antrag auf Reduzierung der Stundenzahl betrifft."

Für die Antragsteller, das hatte auch die Beschwerde des Lehrers gezeigt, ist die Information darüber wesentlich, wer zu welchem Zeitpunkt bzw. Stadium des Antragsverfahren welche Daten erhält. Es macht in der Tat einen Unterschied, ob bei einem Antrag gemäß § 17 der Pflichtstundenverordnung ausschließlich das Schulamt selbst sowie das zuständige Gesundheitsamt eingeschaltet sind oder darüber hinaus auch der Medizinaldienst eingeschaltet wird, soweit die vom Gesundheitsamt vorgeschlagene Reduzierung mehr als zwei Stunden wöchentlich umfasst.

An dieser Stelle setzte auch mein Verbesserungsvorschlag zur Präzisierung der Erklärung ein:
"Da die Gewährung von mehr als zwei Wochenstunden Pflichtstundenermäßigung gemäß § 17 Pflichtstundenverordnung die Zustimmung des Medizinaldienstes des RP Gießen erfordert, bin ich damit einverstanden, dass das Gesundheitsamt meine Antragsunterlagen an den Medizinaldienst weitergibt und erforderliche Auskünfte hierzu erteilt."

Mit dieser Formulierung wird den Betroffenen deutlicher als bislang klargemacht, dass im Falle einer höheren Pflichtstundenermäßigung die Medizinalaufsicht einzuschalten ist und dies eine entsprechende Datenübermittlung zur Folge hat.

5.6.3.4 Reaktion des Schulamtes

Das Schulamt hat als Reaktion auf meinen Vorschlag hin zugesichert, künftig den von mir formulierten Text zu verwenden. Damit lassen sich Missverständnisse hinsichtlich einer geplanten bzw. erforderlichen Übermittlung medizinischer Daten vermeiden.

5.6.4 Datenschutzfragen bei der Erstellung und Behandlung von Schülerfotos

Das Fotografieren von Schülerinnen, Schülern und Lehrkräften in der Schule durch einen professionellen Fotografen und der Verkauf der Fotos hat lediglich in einer Rechtsbeziehung zwischen diesem und den Fotografierten zu erfolgen. Die Schulverwaltung stellt nur den organisatorischen Rahmen zur Verfügung.

Der Datenschutzbeauftragte einer Schule bat mich, zu einem Sachverhalt Stellung zu nehmen, der in zahlreichen Schulen immer wieder vorkommt:

Ein bundesweit tätiges Unternehmen bietet Schulen an, von Lehrkräften und Schülern, sowohl einzeln als auch in der Klassengemeinschaft, Fotos anzufertigen und den Betroffenen die Bilder dann zum Kauf anzubieten. Auch seine Schule habe dieses Angebot erhalten und sie sei gebeten worden, die notwendigen organisatorischen Vorbereitungen zu übernehmen. Insbesondere sollten die Schüler, Eltern und Lehrkräfte über dieses Angebot informiert werden. Die Schülerfotos sollten der Schule auf Wunsch auch zum Anfertigen von Schülerausweisen zur Verfügung gestellt werden.

Die Frage des schulischen Datenschutzbeauftragten war insbesondere, welche rechtliche Rolle die Schule in diesen Abläufen spielen sollte und welche datenschutzrechtliche Verantwortung sie dabei übernehmen würde.

Zu einer datenschutzrechtlich korrekten Gestaltung habe ich ihm die folgenden Hinweise zu den wichtigsten Aspekten gegeben.

Die Erstellung der Fotos ist eine Speicherung personenbezogener Daten nach § 2 Abs. 2 Nr. 2 HDSG.

§ 2 Abs. 2 Nr. 2 HDSG

…
Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zu Zwecke ihrer weiteren Verarbeitung,
…

Für die Beantwortung der Frage, wer unter welchen Voraussetzungen diese Datenverarbeitung durchführen darf, sind die Daten verarbeitenden Stellen zu unterscheiden. Die Schule besitzt kein Recht am Bild der Schüler bzw. Schülerinnen und diese haben deshalb auch nicht die Pflicht, das Foto zu dulden. Bilder von Schülerinnen und Schülern gehören nicht zum Katalog der Schülerdaten, die die Schule für Schulverwaltungsaufgaben nach Anlage 1 Nr. 1 der "Verordnung über die Verarbeitung personenbezogener Daten in Schulen" vom 30. November 1993 (ABl. Nr. 4/1994, S. 206) speichern darf. Lediglich Daten aus diesem Katalog darf die Schulverwaltung erheben, und Schülerinnen und Schüler bzw. Eltern müssen nach § 83 Abs. 3 HSchulG die Datenerhebung unterstützen.

§ 83 Abs. 3 HSchulG

Schülerinnen und Schüler, deren Eltern und Lehrerinnen und Lehrer sind verpflichtet, die erforderlichen Angaben zu machen.
Die Verarbeitung von Daten, die nicht im Datenkatalog der Schulverordnung genannt sind, kann allerdings zulässig sein, wenn sie zu einem der in der sog. Generalklausel des § 83 Abs. 1 Satz 1 HSchulG genannten Zweck erforderlich ist.

§ 83 Abs. 1 Satz 1 HSchulG

Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags der Schule und für einen jeweils damit verbunden Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. …

Selbst die Verwendung der Schülerfotos für die Erstellung eines Schülerausweises fällt nicht unter diese Vorschrift. Denn der Ausweis bescheinigt nur, dass die ihm im Bild erkennbare Person Schüler der Schule ist, die Vorlage des Bildes für den Ausweis ist Sache des Schülers und bleibt freiwillig. Die Schule und auch Lehrkräfte dürfen Bilder von Schülern und Schülerinnen auch nicht für weitere Zwecke verwahren und nutzen. So dürfen z.B. Lehrkräfte nicht von "ihren" Schülern Fotos erstellen, um ihrem schlechten Namensgedächtnis nachhelfen zu können.

Aus diesen Erwägungen folgte meine Empfehlung, in den Informationen an die Schüler, Eltern und Lehrkräfte rechtlich klarzustellen, dass das Anfertigen der Fotos keinesfalls im Auftrag der Schule erfolge und die Schule für diese Zwecke nur die organisatorischen Hilfsdienste leiste. Die Schule wird auch nicht als Erfüllungsgehilfe für den Fotografen im Verhältnis zum Schüler tätig. Damit entfällt insgesamt eine datenschutzrechtliche Verantwortung der Schule.

Da der Fotograf keine öffentliche Stelle ist, wird der datenschutzrechtliche Rahmen durch die Vorschriften des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen vorgegeben. Obwohl ich für die Kontrolle und Beratung dieses Rechtsbereiches sachlich nicht zuständig bin, sei hier Folgendes angemerkt:

Das Anfertigen der Fotos stellt auch nach § 3 Abs. 4 Nr. 1 BDSG eine Datenerhebung dar.

§ 3 Abs. 4 Nr. 1 BDSG

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
…

Diese ist nach § 28 BDSG insbesondere zulässig im Rahmen eines Vertragsverhältnisses mit dem Betroffenen.

§ 28 Abs. 1 Nr. 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,
….

Daraus folgt zwingend, dass Fotografen nur Fotos machen dürfen, wenn zwischen ihnen und den fotografierten Personen bzw. deren Erziehungsberechtigten ein Rechtsverhältnis besteht.

Auch wenn dies an sich nicht in meine Kontrollkompetenz fällt, hielt ich den Hinweis für sinnvoll, dass der Fotograf den Fotografierten zusagt, die Speichermedien nach Druck und Ausgabe der Fotos vollständig zu löschen, um eine Weiterverwendung der Fotos jedenfalls auszuschließen.

5.7 Umwelt und Geologie

5.7.1 Veröffentlichung von Standort-, Funktions- und Eigenschaftskarten

Die Veröffentlichung von flurstücksbezogenen Standort-, Funktions- und Eigenschaftskarten im Internet ist nur auf einer besonderen gesetzlichen Grundlage oder mit Einwilligung der Grundstückseigentümer zulässig.

Das Hessische Landesamt für Umwelt und Geologie (HLUG) bat mich, die datenschutzrechtliche Zulässigkeit der Veröffentlichung von Standort-, Funktions- und Eigenschaftskarten zu überprüfen. Solche Karten stellen z.B. potenzielle Kompensationsflächen für Eingriffe in Natur und Landschaft oder Weinanbaugebiete mit ihren Bodeneigenschaften dar. Zur topographischen Orientierung sind in den großmaßstäbigen Fachkarten die Flurstücksgrenzen der automatisierten Liegenschaftskarte eingezeichnet.

Je nachdem, ob die Veröffentlichung von Standort-, Funktions- und Eigenschaftskarten als Druckwerk oder elektronisch im Internet erfolgt, gelten unterschiedliche rechtliche Anforderungen.

5.7.1.1 Veröffentlichung in gedruckter Form

Die Veröffentlichung der Standort-, Funktions- und Eigenschaftsdaten in Karten ist eine Übermittlung personenbezogener Daten an Personen und Stellen außerhalb des öffentlichen Bereichs. Das HDSG definiert personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 2 Abs. 1 HDSG). Unter welchen Bedingungen Daten als anonymisiert angesehen werden können und damit keinen datenschutzrechtlichen Bestimmungen unterliegen, bestimmt das Gesetz nicht. Ein Maßstab hierfür lässt sich dem BDSG entnehmen. Gemäß § 3 Abs. 6 BDSG gelten personenbezogene Daten als anonymisiert, wenn sie derart verändert worden sind, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können. Mit Hilfe von Angaben aus dem Liegenschaftskataster, die jeder ohne großen Aufwand erlangen kann (§ 16 HVG), sind die Angaben aus den Standort-, Funktions- und Eigenschaftskarten einzelnen Grundstückseigentümern zuzuordnen und somit Einzelangaben über sachliche Verhältnisse einer bestimmbaren Person.

§ 16 Abs. 1 und 2 HVG

(1) Jede Person oder Stelle kann das Liegenschaftskataster und seine Unterlagen sowie die Ergebnisse der Landesvermessung einsehen, Auskunft und auf Antrag Auszüge daraus erhalten.

(2) Die Einsicht in die personenbezogenen Daten sowie das Erteilen von entsprechenden Auskünften und Auszügen ist nur zulässig, wenn der Nutzer ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft macht. Personenbezogene Daten im Sinne dieses Gesetzes sind die Namen von natürlichen Personen, deren Geburtsdatum und deren Anschrift.

Soweit die Angaben in den Karten natürliche Personen unter den Grundstückseigentümern betreffen, sind daher die Übermittlungsvorschriften des HDSG zu beachten. Selbst ohne Flurstücksgrenzen in den Karten lassen sich die Gebietsangaben einzelnen Grundstücken und über die Katasterangaben einzelnen Eigentümern zuordnen.

Die Veröffentlichung des Kartenmaterials ist nicht zur Aufgabenerfüllung des Hessischen Landesamtes für Umwelt und Geologie erforderlich, so dass § 11 Abs. 1 HDSG als Rechtsgrundlage für die Veröffentlichung ausscheidet.

§ 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.

Die Veröffentlichung der Karten lässt sich auf § 16 Abs. 1 HDSG stützen, obgleich diese Vorschrift nicht gerade für Veröffentlichungen (d.h. Massenübermittlungen, die nicht auf Veranlassung eines bestimmten Empfängers erfolgen) konzipiert ist. Der Empfänger muss nach § 16 Abs. 1 HDSG ein berechtigtes Interesse glaubhaft machen und es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können. Ein berechtigtes Interesse der Allgemeinheit an dem Kartenmaterial ist zu bejahen. An Standort-, Funktions- und Eigenschaftskarten besteht ein vielfältiges wirtschaftliches, wissenschaftliches und allgemeines Interesse. Liegt das berechtigte Interesse nach Überzeugung der Behörde vor, muss es nicht noch zusätzlich von einem Datenempfänger glaubhaft gemacht werden.

Die Abwägung zwischen berechtigtem Informationsinteresse der Datenempfänger und den schutzwürdigen Belangen der Betroffenen setzt zwar in der Regel eine Einzelfallprüfung voraus. Wenn kein Einzelfall denkbar ist, in dem schutzwürdige Belange eines Betroffenen beeinträchtigt werden können, ist jedoch auch eine pauschale Prüfung zulässig. Das ist hier der Fall. Grundstückseigentümer müssen generell hinnehmen, dass öffentliche oder private Stellen Daten über die geologische Beschaffenheit oder sonstige Eigenschaften oder die wirtschaftliche und sonstige Nutzung bestimmter Gebiete veröffentlichen, selbst wenn die Daten mittelbar auf ihr Grundstück beziehbar sind. Andernfalls dürften selbst Stadtpläne oder Landkarten nicht mehr veröffentlicht werden, da aus ihnen häufig auch wertbestimmende Informationen für einzelne Grundstücke entnommen werden können. Möglicherweise haben einzelne Grundstückseigentümer ein Interesse, dass eine Veröffentlichung der Beschaffenheit ihres Grundstücks unterbleibt, das Interesse ist jedoch nicht schutzwürdig.

§ 16 Abs. 1 HDSG

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.

5.7.1.2 Veröffentlichung im Internet

Eine Veröffentlichung im Internet ist eine Datenübermittlung an Personen und Stellen außerhalb des Geltungsbereichs der EG-Datenschutz-Richtlinie und damit auch an Empfänger, bei denen kein angemessener Datenschutz gewährleistet ist. Da die Übermittlung nicht ausschließlich im Interesse der Grundstückseigentümer erfolgt, ist sie nur unter den Bedingungen des § 17 Abs. 2 Satz 3 HDSG zulässig. Das Gesetz enthält vier Erlaubnistatbestände, von denen drei hier nicht erfüllbar sind. Die Übermittlung an Personen oder Stellen außerhalb des EU-Bereichs ist nicht für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforder-

lich (Nr. 2). Sie erfolgt nicht zur Wahrung lebenswichtiger Interessen der Grundstückseigentümer (Nr. 3) und auch nicht aus einem öffentlichen Register (Nr. 4). Selbst wenn man in dem beim HLUG geführten Bodeninformationssystem, aus dessen Daten die Karten erstellt werden, ein für die Öffentlichkeit bestimmtes Register i.S.v. § 17 Abs. 2 Satz 3 Nr. 4 HDSG sehen würde, ließe sich die Veröffentlichung der Karten im Internet nicht auf diese Regelung stützen, da sie im Gegensatz zu § 16 Abs. 1 HDSG ausdrücklich nur auf Einzelübermittlungen und nicht auf Massenübermittlungen abstellt. Als Rechtsgrundlage für die Übermittlung bleibt daher nur die Einwilligung der Grundstückseigentümer (Nr. 1).

§ 17 Abs. 2 HDSG

Eine Übermittlung an Empfänger außerhalb des in Abs. 1 genannten Bereichs ist aufgrund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt oder beim Empfänger ein angemessener Datenschutz gewährleistet ist. Vor der Entscheidung über die Angemessenheit ist der Hessische Datenschutzbeauftragte zu hören. Sofern beim Empfänger kein angemessener Datenschutz gewährleistet ist, dürfen personenbezogene Daten übermittelt werden, wenn

1. der Betroffene seine Einwilligung gegeben hat,

2. die Übermittlung für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder

4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Der Empfänger, an den die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu Zwecken verarbeitet werden dürfen, die mit den Zwecken zu vereinbaren sind, zu deren Erfüllung sie ihm übermittelt werden.

Eine Alternative zur Vermeidung dieser wenig praktikablen Konsequenz wäre, Zugriffe auf das Internetangebot des HLUG nur aus dem EU-Gebiet und aus Ländern, die ein von der EU-Kommission gemäß Art. 25 Abs. 6 der Richtlinie 95/46 EG (EG-Datenschutzrichtlinie) festgestelltes angemessenes Schutzniveau aufweisen, zuzulassen. In diesem Fall gilt als Beurteilungsmaßstab für die Zulässigkeit der Veröffentlichung der Karten im Internet allein § 16 Abs. 1 HDSG.

Der andere Weg, den die Landesregierung auf mein Anraten auch beschritten hat, ist die Schaffung einer gesetzlichen Befugnis, die es erlaubt, Datenbestände aus dem Bodeninformationssystem im Internet zu veröffentlichen (vgl. § 10 Abs. 3 Gesetzentwurf der Landesregierung für ein Hessisches Gesetz zur Ausführung des Bundes-Bodenschutzgesetzes und zur Altlastensanierung vom 24. April 2007 - LTDrucks. 16/7240).

5.8 Gesundheitswesen

5.8.1 Hessisches Gesetz über den öffentlichen Gesundheitsdienst

Der Landtag hat das Hessische Gesetz über den öffentlichen Gesundheitsdienst verabschiedet. Das Gesetz enthält einige detaillierte Regelungen zur Verarbeitung personenbezogener Daten. Einige weitergehende Konkretisierungen wären wünschenswert gewesen. Ergänzend ist weiterhin das Hessische Datenschutzgesetz anzuwenden.

Am 28. September 2007 hat der Hessische Landtag ein Gesetz über den öffentlichen Gesundheitsdienst verabschiedet (HGöGD, GVBl. I S. 659). Das Gesetz hat insbesondere auch das Ziel, die wesentlichen Aufgaben des öffentlichen Gesundheitsdienstes in einem Gesetz zusammenzufassen. Mit dem Gesetz werden u.a. das Gesetz über die Vereinheitlichung des Gesundheitswesens vom 3. Juli 1934 (VereinheitlichungsG 1934) und die dazu erlassenen drei Durchführungsverordnungen aufgehoben. Eine spezialgesetzliche Regelung des öffentlichen Gesundheitsdienstes liegt in anderen Bundesländern bereits seit längerer Zeit vor. Auch aus datenschutzrechtlicher Sicht war eine Aufhebung der drei Durchführungsverordnungen dringend erforderlich. Meine Dienststelle wurde von dem Hessischen Sozialministerium in die Diskussion des Vorentwurfs einbezogen. Im Rahmen einer schriftlichen Anhörung des Sozialpolitischen Ausschusses des Hessischen Landtags zu dem Gesetzentwurf (LTDrucks. 16/7236) hat meine Dienststelle Stellung genommen. Einige Vorschläge zur Regelung der Verarbeitung personenbezogener Daten wurden in das Gesetz aufgenommen, in einigen Punkten wäre jedoch aus datenschutzrechtlicher Sicht eine weitergehende Konkretisierung der Vorschriften wünschenswert gewesen.

5.8.1.1 Klarstellung der Unterscheidung zwischen Aufgabenzuweisungen und Befugnissen zur Verarbeitung personenbezogener Daten

In zahlreichen Vorschriften sind Aufgaben des öffentlichen Gesundheitsdienstes formuliert, z.B. in § l Abs. 3 (Zusammenarbeit mit anderen Behörden und Stellen), § 3 Abs. 5 (Zusammenarbeit der Behörden des öffentlichen Gesundheitsdienstes), § 6 Abs. 2 (u.a. Beobachtung und Bewertung der Impfsituation in der Bevölkerung), § 7 Abs. 4 (Beratung und Unterstützung anderer Stellen), § 7 Abs. 5 (Beitragung zur Versorgungsstruktur für ältere Menschen), § 13 (Beobachtung und Bewertung der gesundheitlichen Situation der Bevölkerung). Nicht thematisiert wird, ob und ggf. in welchem Umfang für diese Aufgaben auch personenbezogene (medizinische) Daten verarbeitet werden sollen. Hinzuweisen ist daher darauf, dass diese Aufgabenzuweisungen keine Befugnis zur Verarbeitung personenbezogener Daten enthalten und für die Frage der Befugnis zur Verarbeitung personenbezogener Daten die speziellen Regelungen zur Verarbeitung personenbezogener Daten

im Hessischen Gesetz über den öffentlichen Gesundheitsdienst, insbesondere die Regelung zum Datenschutz in § 18, sowie ergänzend die Bestimmungen des HDSG maßgeblich und im Einzelfall zu prüfen sind.

5.8.1.2 Regelung zur Kinder- und Jugendgesundheit (§ 10)

In § 10 Abs. l ist die Durchführung der ärztlichen Einschulungsuntersuchungen durch die Gesundheitsämter geregelt, und es sind konkrete Festlegungen zur Verarbeitung der Daten getroffen. Eine Verpflichtung der Kinder zur Teilnahme ergibt sich aus § 71 HSchulG.

§ 10 Abs. 1 HGöGD

Die Untersuchung hat den Zweck, gesundheitliche Einschränkungen der Schulfähigkeit oder die Teilnahme am Unterricht betreffende gesundheitliche Einschränkungen festzustellen. Die dabei erhobenen personenbezogenen Daten dürfen für die Zwecke nach Satz 3 verarbeitet werden. Sie dürfen in anonymisierter Form für Zwecke der Gesundheitsberichterstattung verwendet werden. Bei Übermittlungen an Stellen außerhalb des Gesundheitsamtes ist vorher eine Anonymisierung vorzunehmen. …

In § 10 Abs. 2 ist darüber hinausgehend festgelegt, dass die Gesundheitsämter zur Früherkennung von Krankheiten, Behinderungen, Entwicklungs- und Verhaltensstörungen weitere ärztliche Untersuchungen durchführen können. Auf welcher Rechtsgrundlage, in welchem Umfang, zu welchem Zweck und durch welche Stellen im Einzelfall derartige Untersuchungen durchgeführt werden sollen, ist weder im Gesetz noch in der Begründung ersichtlich. Auch hier gilt: Hinsichtlich der Verarbeitung personenbezogener Daten sind evtl. im konkreten Fall vorhandene spezialgesetzliche Regelungen zu prüfen oder die Vorschriften des Hessischen Datenschutzgesetzes.

5.8.1.3 Regelung zum Datenschutz (§ 18)

In das Gesetz wurde - zusätzlich zu einigen speziellen Regelungen zur Datenverarbeitung - eine allgemeine Vorschrift zum Datenschutz aufgenommen (§ 18).

5.8.1.3.1 Verfahren bei der Erstellung von Gutachten (Abs. 1)

In § 18a der 1. DVO zum Gesetz über die Vereinheitlichung des Gesundheitswesens wurde vor einigen Jahren in Abstimmung mit meiner Dienststelle ein Stufenverfahren festgelegt, das aus meiner Sicht sachgerecht ist und sich bewährt hat. Nach der Übermittlung des Gesundheitszeugnisses in dem festgelegten (begrenzten) Umfang ist die auftraggebende Stelle bei konkreten Zweifeln an der Vollständigkeit oder Aussagefähigkeit des Gesundheitszeugnisses oder dem darin festgestellten Ergebnis der Beurteilung berechtigt, Aufklärung von dem untersuchenden Arzt zu verlangen, soweit sie dies unter Beachtung der Verhältnismäßigkeit für erforderlich hält. Das Gesundheitsamt ist in diesem Fällen verpflichtet, ihr die für das Gesundheitszeugnis maßgeblichen Einzeldaten zu übermitteln. Eine entsprechende Regelung wurde in § 18 Abs. 1 aufgenommen:

§ 18 Abs. 1 HGöGD

Bei ärztlichen Untersuchungen ist die zu untersuchende Person vor Beginn der Untersuchung auf deren Zweck und die Übermittlungsbefugnis hinzuweisen. Der die Untersuchung veranlassenden Stelle darf nur das Ergebnis der Untersuchung übermittelt oder weitergegeben werden. Abweichend von Satz 1 dürfen die Anamnese und einzelne Untersuchungsergebnisse übermittelt oder weitergegeben werden, soweit deren Kenntnis zur Entscheidung über die konkrete Maßnahme, zu deren Zweck die Untersuchung durchgeführt worden ist, erforderlich ist.

Im Interesse aller Beteiligten sollte der Hinweis i.S.v. Satz 1 schriftlich erfolgen oder zumindest in der Akte dokumentiert werden, damit im Fall eines nachträglichen Konflikts der Ablauf und der Inhalt der Information nachvollziehbar ist.

Als Satz 3 hatte ich zusätzlich die folgende bisher ebenfalls in § 18a der l. DVO zum Gesetz über die Vereinheitlichung des Gesundheitswesens enthaltene spezielle Regelung für Bewerbungsverfahren vorschlagen, die sicherstellt, dass medizinische Daten über Bewerber nicht unnötig breit gestreut werden:

Bei Untersuchungen anlässlich der Einstellung eines Bewerbers in den öffentlichen Dienst darf das Ergebnis der Untersuchung nur übermittelt werden, wenn der untersuchende Arzt oder die untersuchende Ärztin die untersuchte Person über Inhalt und Umfang der gutachterlichen Feststellungen aufgeklärt und diese sich mit der Übermittlung des Ergebnisses einverstanden erklärt hat.

Der Vorschlag hätte eine Klarstellung der Rechtslage für alle mit Bewerbungsverfahren befassten Mitarbeiterinnen und Mitarbeiter bedeutet. Er wurde leider nicht aufgenommen. Auch ohne eine solche Regelung im Hessischen Gesetz über den öffentlichen Gesundheitsdienst gebietet die Rechtslage diese Verfahrensweise, weil eine rechtswirksame Einwilligung in die Übermittlung nur erteilt werden kann, wenn der Inhalt der Übermittlung, das Untersuchungsergebnis, dem Bewerber bekannt ist.

5.8.1.3.2 Pauschale Befugnis zur Erhebung der Meldedaten aller Neugeborenen (Abs. 2)

In Abs. 2 wurde folgende Erhebungsbefugnis aufgenommen:

§ 18 Abs. 2 HGöGD

Für die Aufgaben nach den §§ 10 und 11 erheben die Gesundheitsämter von den Meldebehörden Namen, Geburtstag, Anschrift und Staatsangehörigkeit aller Neugeborenen oder aller Kinder eines festzulegenden Jahrgangs.

Hierbei handelt es sich um eine schrankenlose Blankett-Eingriffsbefugnis. Die Formulierung ist ein Einfallstor für beliebige Datenzugriffe. Die Kombination einer allgemeinen Aufgabenzuweisungsnorm mit einer korrespondierenden Befugnisnorm macht die Befugnisnorm zu einer konturenlosen Generalklausel. Speziell die Daten aller Neugeborenen stellen aus datenschutzrechtlicher Sicht eine sehr sensitive Datensammlung dar. Dem Hessischen Datenschutzbeauftragten ist keine einzige Maßnahme bekannt, zu deren Durchführung alle Gesundheitsämter diese Daten benötigen könnten. In § 17 Abs. 2 der Meldedaten-Übermittlungsverordnung ist bereits vorgesehen, dass die Meldebehörden den Gesundheitsämtern zur Erfüllung ihrer Aufgaben nach §§ 71 und 149 des HSchulG die Daten schulpflichtiger Kinder übermitteln. Für eine Kontrolle der Teilnahme an den durch das Kindergesundheitsschutz-Gesetz neu geregelten Früherkennungsuntersuchungen wurde ebenfalls eine spezielle Regelung in die Meldedaten-Übermittlungsverordnung aufgenommen (s. Ziff. 5.8.2).

Aus der Gesetzesbegründung erschließt sich die Notwendigkeit dieser Regelung nicht. Dort heißt es nur:

Abs. 2 regelt spezielle Erhebungsbefugnisse der Gesundheitsämter bei Maßnahmen der Kinder- und Jugendgesundheit und der Zahngesundheit.

Auch das Hessische Sozialministerium konnte in der Diskussion über diese Vorschrift keine Maßnahme nennen. Soweit künftig konkrete Maßnahmen gestützt auf diese Vorschrift eingeführt werden sollen, zählt es zu meinen Aufgaben, die Erforderlichkeit und Geeignetheit der Datenerhebungen zu prüfen.

5.8.1.3.3 Gewährleistung der Geheimhaltungspflichten und der Zweckbindung der personenbezogenen Daten in den Gesundheitsbehörden

Abs. 3 thematisiert die innerbehördliche Organisation der Gesundheitsbehörden. Insbesondere für die Datenverarbeitung in den Gesundheitsämtern ist dies eine zentrale Frage:

Nach dem Entwurf haben die Gesundheitsämter umfassende Beratungsaufgaben, s. z.B. § 6 Abs. l, § 7 Abs. l bis 3, § 10 Abs. 3. Die Beratungen sollen wie bisher auf freiwilliger Basis wahrgenommen werden. Soweit personenbezogene Daten verarbeitet werden, ist es angesichts der vielfältigen Aufgaben der Gesundheitsämter für die Beratung Suchenden von zentraler Bedeutung, dass die Einhaltung der gesetzlich normierten Schweigepflichten, insbesondere der ärztlichen Schweigepflicht, und eine **strikte Zweckbindung** der Daten bei Beratungen in den Gesundheitsämtern gewährleistet werden. Ein Gesundheitsamt ist keine informationelle Einheit. Personenbezogene Daten unterliegen auch im Gesundheitsamt einer grundsätzlichen Zweckbindung. Insbesondere dürfen auch Daten, die Bürgerinnen und Bürger dem Gesundheitsamt zum Zwecke der freiwilligen Gesundheitsberatung anvertraut haben, grundsätzlich nur zweckgebunden für den von den Bürgerinnen und Bürgern intendierten Zweck verwendet und nicht darüber hinausgehend für die Ausübung von Überwachungs- und Zwangsmaßnahmen genutzt werden. Wer freiwillig Beratungshilfe in Anspruch nimmt, muss beim Gesundheitsamt die gleiche Vertraulichkeit erwarten können wie bei einem freien Träger. Er soll sich darauf verlassen können, dass ihm Angaben aus einem solchen Beratungsgespräch nicht im Verwaltungsvollzug entgegengehalten werden. Ausnahmen davon müssen eng begrenzt und klar festgelegt werden. Dies liegt auch im Interesse des Gesundheitsamtes selbst, dessen Beratungstätigkeit vom Vertrauen der Ratsuchenden in die Beratungstätigkeit getragen sein muss. Nur so können die Gesundheitsämter ihre Beratungstätigkeit auch effektiv wahrnehmen. Ein Bürger wird zögern, die Beratungsdienste in Anspruch zu nehmen, wenn er damit rechnen muss, dass die dem Gesundheitsamt in diesem Zusammenhang bekannt werdenden Daten unter Umständen zu einem späteren Zeitpunkt in ganz anderen Zusammenhängen und zu seinem Nachteil verwandt werden können.

In Abs. 3 wurde nunmehr folgende Regelung hierzu aufgenommen:

Die innerbehördliche Organisation der Gesundheitsbehörden ist so zu gestalten, dass gesetzliche Geheimhaltungspflichten, insbesondere die ärztliche Schweigepflicht, gewahrt werden.

Diese Regelung ist inhaltlich korrekt. Der Aspekt ist von zentraler Bedeutung. Eine weitergehende Konkretisierung wäre jedoch wünschenswert gewesen. Die Schweigepflichten, insbesondere die ärztliche Schweigepflicht, und der Grundsatz der Zweckbindung der Daten sind bereits bei der Aktenführung zu beachten, da sonst eine Einhaltung der rechtlichen Vorgaben in der Praxis sehr schwierig ist. Die Anlage einer umfassenden "Gesundheitsakte" über eine Person, in der z.B. Vorgänge wie freiwillige Beratungen und die Durchführung von Überwachungs- und Zwangsmaßnahmen zusammen abgelegt sind, muss unterbleiben. Wenn z.B. ohne Rücksicht auf den konkreten Untersuchungsauftrag bzw. Kontext und den Abschluss der einzelnen Vorgänge alle Vorgänge in einer Akte über viele Jahre hinweg aufbewahrt werden, führt dies im Ergebnis regelmäßig dazu, dass bei einem neuen, dieselbe Person betreffenden Untersuchungsauftrag bzw. Vorgang, die gesamte Akte ohne fachliche Notwendigkeit dem mit dem neuen Vorgang befassten Bearbeiter zur Kenntnis gegeben wird. Ich hatte daher eine entsprechende klarstellende Konkretisierung im Gesetz vorgeschlagen. Die Regelung des Abs. 3 muss in dem dargelegten Sinn vor Ort entsprechend umgesetzt werden.

5.8.1.3.4 Vorgaben zur Dauer der Datenspeicherung

Leider ist entgegen meinen Vorschlägen in § 18 keine Regelung zur Datenlöschung aufgenommen worden. Bei stichprobenhaften Prüfungen der Datenverarbeitung in Gesundheitsämtern hat sich gezeigt, dass zum Teil erhebliche Unklarheiten bzgl. der Aufbewahrungsdauer von Unterlagen bestehen; Klärungsbedarf wird u.a. auch beim RP Darmstadt gesehen (s. Ziff. 5.8.4)

5.8.1.3.5 Verweis auf das Hessische Datenschutzgesetz (Abs. 4)

Für weitere Details der Datenverarbeitung wird auf das HDSG verwiesen. Dies ist ausreichend. Insbesondere ist eine Regelung zur Forschung wie sie in verschiedenen Gesundheitsdienstgesetzen anderer Bundesländer enthalten ist aus meiner Sicht entbehrlich, da § 33 HDSG hinreichend präzise Vorgaben auch für die Durchführung von Forschungsvorhaben mit medizinischen Daten enthält. Die Vorschrift findet gem. § 12 Abs. 1 HKHG i.V.m. § 33 HDSG auch für die Krankenhäuser Anwendung und hat sich auch insoweit in der Praxis als angemessen erwiesen. Entsprechendes gilt für die Datenverarbeitung im Auftrag. Auch im HKHG (§ 12 Abs. 1) wird auf die Regelung über die Datenverarbeitung im Auftrag im HDSG verwiesen. Die Regelung schließt die Möglichkeit ein, hinsichtlich der Verarbeitung medizinischer Daten ein erhöhtes Schutzniveau zu fordern. Es kann daher auch für den öffentlichen Gesundheitsdienst auf das HDSG verwiesen werden.

5.8.2 Kindergesundheitsschutz-Gesetz

Der Landtag hat ein Gesetz zur Verbesserung des Gesundheitsschutzes für Kinder beschlossen. Die Einführung einer Verbindlichkeit der Früherkennungsuntersuchungen und die Einrichtung eines Kindervorsorgezentrums bringt auch in erheblichem Umfang neue Verarbeitungen personenbezogener Daten der Kinder und Eltern mit sich. Meine Vorschläge zur Ausgestaltung des Datenschutzes wurden in das Gesetz übernommen.

Am 14. Dezember 2007 hat der Hessische Landtag das Kindergesundheitsschutz-Gesetz beschlossen (GVBl. I S. 856). Mit dem Gesetz wird eine Verbesserung des Gesundheitsschutzes von Kindern und ihres Schutzes vor Vernachlässigung, Misshandlung und Missbrauch angestrebt. Zentraler Bestandteil des Gesetzes ist die Einführung einer Verbindlichkeit der Früherkennungsuntersuchungen. Zum einen wird die Teilnahme an den Früherkennungsuntersuchungen U4 bis U9 (s. Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Früherkennung von Krankheiten bei Kindern bis zur Vollendung des 6. Lebensjahres, sog. Kinder-Richtlinien, http://www.g-ba.de/informationen/richtlinien/15/) verbindlich (§ 1 Abs. 1). Zum anderen wird auch die Teilnahme an den Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen, das sog. Neugeborenen-Screening (s. Anlage 2 der o.a. Kinder-Richtlinien), verbindlich (§ 1 Abs. 2). Das Gesetz sieht vor, dass die Kinder, die nicht innerhalb der vorgesehenen Frist an den jeweiligen Früherkennungsuntersuchungen teilgenommen haben, durch Datenabgleiche herausgefunden werden, die Eltern (bzw. Personensorgeberechtigten) dieser Kinder über die erforderlichen Früherkennungsuntersuchungen informiert und an die Teilnahme erinnert werden und - sofern weiterhin keine Teilnahme gemeldet wird - das zuständige Jugendamt eingeschaltet wird, um den Hintergrund der Nichtteilnahme an den Früherkennungsuntersuchungen aufzuklären.

Darüber hinaus ist im Gesetz festgelegt, dass den Eltern auch weitere, zusätzliche Früherkennungsuntersuchungen angeboten werden können und die Daten über diese Untersuchungen auf der Basis einer Einwilligung der Eltern ebenfalls im Kindervorsorgezentrum verarbeitet werden.

5.8.2.1 Neue Verarbeitungen personenbezogener Daten der Kinder und Personensorgeberechtigten

Zur Kontrolle der Durchführung der nunmehr verbindlichen Früherkennungsuntersuchungen sind neue Datenübermittlungen sowie Datenspeicherungen und Datenabgleiche im neu zu errichtenden Kindervorsorgezentrum vorgesehen.

Früherkennungsuntersuchungen U4 bis U9
Bezüglich der in § 1 Abs. 1 des Gesetzes vorgeschriebenen Verpflichtung zur Teilnahme an den U4 bis U9 werden vorgesehen

- die Übermittlung der Daten aller Neugeborenen und ihrer Eltern (bzw. Personensorgeberechtigten) durch die Meldebehörden an das Kindervorsorgezentrum (§ 18a MeldDÜVO)
  Übermittelt werden Familienname, Vorname, Tag und Ort der Geburt, Geschlecht, gesetzliche Vertreterin/gesetzlicher Vertreter und gegenwärtige Anschrift, Tag des Einzugs, Tag des Auszugs, Datum des Wohnungsstatuswechsels, evtl. Sterbetag und evtl. Übermittlungssperren.

- Datenübermittlungen der die Früherkennungsuntersuchungen durchführenden Personen an das Kindervorsorgezentrum (§ 4 Abs. 1)
  Übermittelt werden Familienname, Vorname, Geschlecht, Tag und Ort der Geburt, Name und Anschrift des Personensorgeberechtigten sowie Bezeichnung und Datum der Früherkennungsuntersuchung.

- ein Abgleich der Meldedaten und der Meldungen i.S.v. § 1 Abs. 1 im Kindervorsorgezentrum zur Feststellung, welche Kinder nicht an den vorgesehenen Früherkennungsuntersuchungen teilgenommen haben und

- die Versendung von Information und Erinnerung an die Eltern (§ 3 Abs. 1) sowie

- bei Bedarf Datenübermittlungen an das zuständige Jugendamt (§ 3 Abs. 1): Sofern die Eltern einer Aufforderung zur Teilnahme des Kindes an der erforderlichen Früherkennungsuntersuchung nicht Folge leisten, wird das Jugendamt über die Nichtteilnahme an der erforderlichen Früherkennungsuntersuchung informiert.

Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen
Bezüglich der in § 1 Abs. 2 des Gesetzes vorgeschriebenen Verpflichtung zur Teilnahme an Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen werden vorgesehen

- die Übermittlung der personenbezogenen Blutproben aller Neugeborenen an das Kindervorsorgezentrum (§ 4 Abs. 2 Satz 1)

- Datenübermittlungen über alle Neugeborenen und ihre Eltern (bzw. Personensorgeberechtigten) an das Kindervorsorgezentrum, sofern die Eltern eine Teilnahme an der Früherkennungsuntersuchung ablehnen (§ 4 Abs. 2 Satz 2)
  Übermittelt werden Familienname, Vorname, Geschlecht, Tag und Ort der Geburt, Name und Anschrift der Personensorgeberechtigten sowie Bezeichnung und Datum der erforderlichen Früherkennungsuntersuchung.

- ein Abgleich der Meldedaten und Meldungen im Kindervorsorgezentrum zur Feststellung, welche Kinder nicht an den Untersuchungen teilgenommen haben; das Kindervorsorgezentrum hat dann die Aufgabe, durch Beratung auf eine Teilnahme hinzuwirken (§ 3 Abs. 2).

Zusätzlich angebotene freiwillige Früherkennungsuntersuchungen
Darüber hinausgehend sieht das Gesetz in § 1 Abs. 4 vor, dass den Eltern über die in Anlage 2 der o.a. Kinder-Richtlinien genannten Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen weitere Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen auf freiwilliger Basis angeboten werden können. Eltern in Hessen wird bereits seit einiger Zeit über die in der Kinderrichtlinie genannten Untersuchungen hinaus ein erweitertes kostenfreies Screening ihrer Neugeborenen auf weitere behandelbare Erkrankungen angeboten, die in der Elterninformation konkret und abschließend genannt wurden. Bei diesen Erkrankungen wird angenommen, dass eine frühe Diagnose den Kindern eine bessere Lebensqualität ermöglicht. Die hierbei gewonnenen Daten und Restblutproben sollen nach Information und Einwilligung der Eltern ebenfalls im Kindervorsorgezentrum gespeichert bzw. aufbewahrt werden. Den Umfang dieser zusätzlichen Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen legt gem. § 3 Abs. 6 der Beirat des Kindervorsorgezentrums fest.

5.8.2.2 Datenschutzrechtliche Forderungen

Bei der Frage der Einführung einer Verpflichtung zur Teilnahme an Früherkennungsuntersuchungen handelt es sich um eine vom Hessischen Datenschutzbeauftragten nicht zu bewertende gesundheitspolitische Entscheidung.

Die umfangreiche neue Verarbeitung personenbezogener Daten muss jedoch aus datenschutzrechtlicher Sicht für die festgelegten Zwecke erforderlich und geeignet sein. Vor diesem Hintergrund war es mein zentrales Anliegen, dass

- die neue Verarbeitung personenbezogener Daten im Gesetz präzise und konsistent festgelegt wird,

- das Kindervorsorgezentrum im Rahmen der Mitteilungen über die Teilnahme an der U4 bis U9 keine medizinischen Details zur Kenntnis erhält,

- eine strikt zweckgebundene Verwendung der Daten und Restblutproben sichergestellt wird,

- die Daten der Kinder und Personensorgeberechtigten in einer **öffentlichen** Stelle verarbeitet werden und

- nach einem angemessenen Zeitraum effektiv evaluiert wird, ob die umfangreichen Datenverarbeitungen für den Kinderschutz erforderlich und geeignet sind.

So wäre etwa eine reine Datensammlung ohne zeitnahe Aufklärung des im Einzelfall vorliegenden Hintergrunds einer fehlenden Früherkennungsuntersuchung dem Kinderschutz nicht dienlich und könnte damit datenschutzrechtlich auch nicht gerechtfertigt werden. Die Personensorgeberechtigten dürfen auch nicht längerfristig mit nicht abgeklärten Informationen über eine evtl. Kindeswohlgefährdung gespeichert werden. Stellt sich heraus, dass das Kindeswohl im Einzelfall nicht gefährdet ist, müssen die gespeicherten Informationen umgehend dementsprechend aktualisiert bzw. gelöscht werden.

5.8.2.3 Datenschutzrechtliche Regelungen im Gesetz

Meine Dienststelle wurde von der Sozialministerin bereits bei der Erarbeitung des Entwurfs beteiligt. Das Gesetz enthält detaillierte Regelungen zur Datenverarbeitung, in die meine Vorschläge aufgenommen worden sind:

- Das Gesetz sieht vor, dass durch Rechtsverordnung eine **öffentliche** Stelle als Hessisches Kindervorsorgezentrum bestimmt wird (§ 3 Abs. 7). Es ist geplant, das Kindervorsorgezentrum am Universitätsklinikum Frankfurt einzurichten.
- Die dem Kindervorsorgezentrum übermittelten personenbezogenen Daten dürfen nur zu den im Gesetz festgelegten Zwecken in dem dafür erforderlichen Umfang verarbeitet werden (§ 5 Abs. 1). Die Zwecke sind im Gesetz präzise festgelegt, insbesondere sind auch zeitliche Vorgaben für die vorgesehenen Maßnahmen in dem Gesetz vorgegeben:

- Die Ärztinnen und Ärzte müssen das Kindervorsorgezentrum über eine erfolgte Früherkennungsuntersuchung i.S.v. § 1 Abs. 1 "spätestens 5 Werktage nach der Untersuchung" informieren.

- Das Kindervorsorgezentrum stellt jeweils "unmittelbar nach Ablauf der für die jeweilige Früherkennungsuntersuchung nach § 1 Abs. 1 vorgesehenen Frist" fest, welche Kinder nicht an den vorgesehenen Untersuchungen teilgenommen haben.

- Wenn die Eltern der Aufforderung zur Teilnahme nicht Folge leisten, informiert das Kindervorsorgezentrum "unverzüglich" das zuständige Jugendamt.

- Personenbezogene Daten über die Gesundheit eines Kindes dürfen vom Kindervorsorgezentrum nur mit Einwilligung der Personensorgeberechtigten an Dritte übermittelt werden (§ 5 Abs. 1).

- Personenbezogene Daten sind im Kindervorsorgezentrum spätestens sechs Jahre nach der Geburt des Kindes zu löschen (§ 5 Abs. 2).

- Die bei den Untersuchungen angefallenen Restblutproben dürfen

- nur mit Einwilligung der Personensorgeberechtigten und

- nur in verschlüsselter Form

aufbewahrt werden.

Die zur Wiederherstellung des Personenbezugs erforderlichen Zuordnungsregeln sind getrennt bei einer Treuhandstelle zu verwahren, die durch Rechtsverordnung bestimmt wird. Die Wiederherstellung des Personenbezugs ist nur mit gesondert zu erteilender Einwilligung der Personensorgeberechtigten zulässig. Die Personensorgeberechtigten können jederzeit die Herausgabe der Restblutprobe verlangen. Restblutproben sind spätestens nach zehn Jahren zu vernichten, soweit die Berechtigten einer längeren Aufbewahrung nicht ausdrücklich zustimmen (§ 5 Abs. 3).

- Bei dem Kindervorsorgezentrum wird ein Beirat gebildet, der u.a. auch aus einem Vertreter des HDSB besteht. Der Beirat wirkt darauf hin, dass das Kindervorsorgezentrum seine Aufgaben ordnungsgemäß wahrnimmt und legt im Einvernehmen mit dem Kindervorsorgezentrum Grundsätze für den Umgang mit Daten und Untersuchungsmaterial fest. Darüber hinaus legt er den Umfang der zusätzlichen Früherkennungsuntersuchungen fest (s.o.).

Einzelheiten zur Evaluation wurden im Gesetz nicht festgelegt. Im Hinblick auf die umfangreiche neue zentrale Datensammlung sehe ich es als wünschenswert an, dass nach einem angemessenen Zeitraum effektiv überprüft wird, ob diese Datensammlung tatsächlich für den angestrebten Zweck erforderlich und geeignet ist. Es sollte geklärt und festgelegt werden, welche Daten hierfür in welchem Verfahren dokumentiert werden. Über das Konzept hat eine Besprechung zwischen dem Hessischen Sozialministerium und mir stattgefunden. Das Hessische Sozialministerium plant eine Festlegung per Erlass.

5.8.2.4 Weitere Schritte für 2008

- Das Universitätsklinikum Frankfurt am Main wurde durch Verordnung vom 21. Dezember 2007 (GVBl. I S. 962) zum Hessisches Kindervorsorgezentrum bestimmt. Der Aufbau des Kindervorsorgezentrums am Universitätsklinikum Frankfurt wird von meiner Dienststelle aus datenschutzrechtlicher Sicht betreut. Eine erste Besprechung zwischen dem Hessischen Sozialministerium, dem Universitätsklinikum und mir hat bereits stattgefunden, und daraufhin wurde meiner Dienststelle bereits ein Teil des geplanten Datenschutzkonzepts übersandt. Die Diskussion wird fortgesetzt. Dabei besteht insbesondere Konsens darüber, dass der Datenbestand des Kindervorsorgezentrums abzuschotten ist von dem im Universitätsklinikum vorhandenen Patientendatenbestand und auf die Daten des Kindervorsorgezentrums nur diejenigen Mitarbeiterinnen und Mitarbeiter zugreifen dürfen, die diese Daten für die Durchführung ihrer Aufgaben benötigen. Weitere Einzelheiten, namentlich zur Sicherstellung der Zweckbindung der Daten und zum Schutz gegen unbefugten Zugriff werden noch geklärt.

- Die im Gesetz vorgeschriebene getrennte Aufbewahrung der Zuordnungsinformationen für die Restblutproben bei einem Treuhänder muss umgesetzt werden.

- Soweit der Beirat zusätzliche freiwillige Früherkennungsuntersuchungen beschließt, muss der Text des Einwilligungsformulars für zusätzliche freiwillige Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen infolge der im Gesetz geregelten geänderten Verfahrensweisen und der geänderten Rechtslage überarbeitet werden. Hierfür habe ich dem Sozialministerium meine Unterstützung angeboten.

5.8.3 Forschungsprojekt CIMECS zur einrichtungsübergreifenden elektronischen Fallakte

Zum digitalen Austausch von Patientendaten zwischen verschiedenen Behandlungseinrichtungen wird in Hessen ein Forschungsprojekt durchgeführt. Meine Dienststelle berät die Projektleitung. Eine Reihe datenschutzrechtlicher Fragen bedürfen noch der Klärung.
Von der Universität Gießen wird derzeit in Kooperation mit der Landesregierung Hessen, der Landesärztekammer Hessen, dem Ärzteverbund ANR, T-Systems und einigen Klinken das Forschungsprojekt CIMECS (Central Interdisciplinary Medicare System) durchgeführt. Gegenstand des Forschungsprojekts ist die einrichtungsübergreifende elektronische Fallakte, die einen schnellen, einfachen und sicheren Austausch von Patientendaten (Arztbriefe, Befunde, Laborergebnisse, CTs, MRTs

etc.) zwischen Haus- und Fachärzten sowie Kliniken ermöglichen soll. CIMECS ist eine internetbasierte Kommunikationsplattform, die über ein gesichertes Netzwerk (Branchennetzwerk Gesundheit von T-Systems) berechtigten Ärzten Patientendaten zur Verfügung stellen soll. Dabei soll jeder Behandler nach wie vor unverändert seine eigene nach Berufsrecht vorgeschriebene Dokumentation seiner Behandlung führen. Die elektronische Fallakte soll auf der Basis einer Einwilligung des Patienten eingerichtet und genutzt werden. Die Einwilligung des Patienten bezieht sich auf einen konkreten Behandlungsfall.

Mit der elektronischen einrichtungsübergreifenden Fallakte soll die Qualität der Behandlung verbessert werden. Auch aus datenschutzrechtlicher Sicht ist es allerdings von zentraler Bedeutung, dass zuvor verbindlich geklärt und festgelegt wird, welche Stelle für welche Aufgaben bzw. Inhalte verantwortlich ist.

Nach einer ersten allgemeinen Besprechung mit den Projektbeteiligten habe ich in einer schriftlichen Stellungnahme die aus datenschutzrechtlicher Sicht noch klärungsbedürftigen Punkte für die Projektbeteiligten zusammengestellt. Hierzu zählen insbesondere die folgenden Punkte:
- Wer ist die für die zentrale elektronische Fallakte verantwortliche Daten verarbeitende Stelle?
- Welchen Inhalt haben die Patienteninformation und Patienteneinwilligung?
- Wie wird die Nutzung der Fallakte protokolliert? Es muss nachvollziehbar sein, wer welche Dokumente oder Links einstellt und/oder abruft, d.h. welcher Arzt bzw. welche Institution welche Informationen bei der Behandlung zur Verfügung hatte.
- Wie sieht das Verfahren aus, mit dem die Zugriffsberechtigungen für behandelnde Ärzte vergeben werden?
- Wie sind die Patientenrechte im Verfahren ausgestaltet?
- Welche Datensicherheitsmaßnahmen sollen ergriffen werden? Liegt ein Datensicherheitskonzept vor?
- Wie werden Integrität und Authentizität der in CIMECS zur Verfügung gestellten Befunde gewährleistet?

5.8.4 Prüfung der Datenverarbeitung ausgewählter Gesundheitsämter

Die Prüfung der Archive in fünf ausgewählten Gesundheitsämtern hat ergeben, dass die Lagerung der Akten, der Zugang zu den Unterlagen sowie die getroffenen Maßnahmen zur Vernichtung einzelner Aktenbestände im Wesentlichen den datenschutzrechtlichen Vorgaben entsprachen. In wenigen Einzelfällen waren die Speicherfristen einzelner Unterlagen nicht ausreichend berücksichtigt worden. Nach wie vor mangelt es jedoch an einem Gesamtkonzept für Speicherfristen von medizinischen Unterlagen im Gesundheitsamt.

5.8.4.1 Vorbemerkung

Im Jahr 2006 habe ich mit der Prüfung von Archiven in fünf ausgewählten Gesundheitsämtern begonnen, die im Jahr 2007 abgeschlossen wurde. Zum Zeitpunkt der Prüfung gab es das Gesetz über den öffentlichen Gesundheitsdienst (HGöGD) noch nicht. Die Vorgaben der seinerzeit gültigen Rechtsgrundlagen waren aber ähnlich (vgl. Ziff. 5.8.1). In dem Beitrag sind gleichwohl auch die Vorschriften des HGöGD zitiert, soweit diese statt bisheriger Rechtsgrundlagen künftig anzuwenden sind.

5.8.4.2 Art der in Gesundheitsämtern gelagerten Akten

Unterlagen, die in Gesundheitsämtern anfallen, sind in der Regel medizinischer Natur und zum größten Teil personenbezogen. Einem Kontakt mit dem Gesundheitsamt kann man sich kaum entziehen. Ob Schuleingangsuntersuchung, amtsärztliche Begutachtung im Zusammenhang mit der Einstellung in den öffentlichen Dienst oder bei privaten Arbeitgebern, dem Infektionsschutz, Beurteilung der Voraussetzung zur Erteilung von Waffenscheinen oder Sammlung der Leichenschauscheine, um nur einige Beispiele zu nennen. Die Rechtsgrundlagen für die Datenverarbeitung sind ebenso vielfältig: so ist z.B. für die Schuleingangsuntersuchung die Verordnung über die Zulassung und Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege einschlägig, für Maßnahmen zum Infektionsschutz das Infektionsschutzgesetz, für ärztliche Untersuchungen das Gesetz über den öffentlichen Gesundheitsdienst (HGöGD) vom 28. September 2007 (GVBl. I S. 659).

In vielen Fällen ist das Gesundheitsamt selbst aktiv oder wird von anderen Stellen eingeschaltet. Kein Wunder also, dass hier eine Fülle papierner und elektronischer Daten anfallen, die zu einem bestimmten Zeitpunkt auch wieder vernichtet bzw. gelöscht werden müssen.

5.8.4.3 Rechtliche Grundlagen für die Speicherung

Die Aufbewahrungsvorschriften für medizinische Unterlagen sind in einigen Bereichen - wenn überhaupt - allenfalls rudimentär geregelt. In anderen speziellen Vorschriften wie z.B. der Verordnung über die Zulassung und Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege (StAnz. 2000 S. 752, verlängert durch VO vom 9. August 2004, StAnz. 2004 S. 2852) hingegen gibt es klare Vorgaben für die Aufbewahrungsdauer der personenbezogenen Unterlagen der Schülerinnen und Schüler (hier: bis zur Vollendung des 23. Lebensjahres). Ein anderes Beispiel für eine eindeutige Speicherfrist ergab sich zum Prüfzeitpunkt für die Aufzeichnungen des amtsärztlichen Dienstes, die im Zusammenhang mit dienst- und arbeitsrechtlichen Angelegenheiten erstellt wurden. Nach § 18a der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens waren diese bis zur Vollendung des 70. Lebensjahres der untersuchten Person, im Falle ihres Todes oder Ausscheidens vor Vollendung des 65. Lebensjahres noch fünf Jahre aufzubewahren. Dies entspricht im Wesentlichen den Fristen, die auch im Personalaktenrecht (§§ 107 ff. HBG) und im Hessischen Archivgesetz geregelt sind.

Die Aufbewahrung anderer personenbezogener Unterlagen ist nicht durch besondere Aufbewahrungsvorschriften geregelt. Dies betrifft insbesondere die Leichenschauscheine oder aber die Akten des sozialpsychiatrischen Dienstes, soweit er amt-

lich, also durch andere öffentliche Stellen beauftragt, tätig wird. Das Regelungsdefizit führt deshalb bei den betroffenen Stellen immer wieder zu Unsicherheiten. Leider sind die Aufbewahrungsfristen auch im neuen HGöGD nicht konkretisiert worden (s. Ziff. 5.8.1).

5.8.4.4 Zugang zu den Archiven

In allen Ämtern werden nicht mehr benötigte Unterlagen in Räumen eingelagert, die als Archiv dienen. Während im Gesundheitsamt des Schwalm-Eder-Kreises die Akten einzelner Bereiche in jeweils getrennten Räumen eingelagert wurden, sind bei den anderen Stellen einzelne, große Räume oder mehrere zusammenhängend begehbare Lagerstätten eingerichtet. Wesentliches Kriterium bei einer gemeinsamen Einlagerung ist, dass die Aktenbestände übersichtlich voneinander getrennt sind. Dies war in allen Fällen gewährleistet.

Der Zugang zu den verschlossenen Archiven erfolgt grundsätzlich über eine zentrale Stelle, welche in der Regel die Schlüsselabholung protokolliert. In einigen Stellen gibt es mehrere Schlüssel, über welche die für das Archiv zuständigen Mitarbeiterinnen und Mitarbeiter verfügen.

5.8.4.5 Aufbewahrung einzelner Unterlagen

5.8.4.5.1 Leichenschauscheine

Mit jedem Todesfall erhält das Gesundheitsamt eine Kopie der von einem Arzt ausgestellten Bescheinigung. In der Regel werden diese Unterlagen in den Ämtern über einen Zeitraum von 30 Jahren hinweg gespeichert. Dies ist keine gesetzlich festgelegte Frist, sondern eine von den Gesundheitsämtern vereinbarte Dauer, die in einem Arbeitspapier der Verwaltungsleiter fixiert ist. Bei einigen Stellen war dieser Zeitraum überschritten, zwei Ämter hatten noch nie derartige Unterlagen vernichtet, weil man sich nicht darüber im Klaren war, über welchen Zeitraum hinweg eine Aufbewahrung zu erfolgen hat.

5.8.4.5.2 Pockenschutzimpfungen

In fast allen Ämtern waren personenbezogene Unterlagen zu den Impfungen in Form von Listen vorhanden. Die Angaben zu den Betroffenen reichten bis in die fünfziger Jahre hinein. Seit 1970 werden keine Säuglinge mehr gegen Pocken geimpft, seit 1982 ist das Gesetz über die Verpflichtung zur Teilnahme an einer Pockenschutzimpfung außer Kraft gesetzt. In diesem Bereich gibt es keine rechtlichen Vorgaben zur Speicherdauer. Deshalb hat sich die Speicherdauer hier nach den allgemeinen Vorgaben des HDSG auszurichten. Nach § 19 Abs. 3 HDSG sind personenbezogen Daten unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist. Demzufolge sind diese Akten zu vernichten.

5.8.4.5.3 Aufzeichnungen des amtsärztlichen Dienstes

Diese Akten, die im Zusammenhang mit dienst- und arbeitsrechtlichen Angelegenheiten erstellt wurden, waren bislang nach § 18a der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens bis zur Vollendung des 70. Lebensjahres der untersuchten Person, im Falle ihres Todes oder Ausscheidens vor Vollendung des 65. Lebensjahres noch fünf Jahre aufzubewahren. In den meisten Fällen wurde dieser Vorgabe Rechnung getragen. Mittlerweile ist jedoch diese Rechtsgrundlage entfallen, weil das Gesetz über die Vereinheitlichung des Gesundheitswesens aus dem Jahre 1934 und die darin genannten Durchführungsverordnungen durch das HGöGD ersetzt wurden. Konkrete Aufbewahrungsfristen sind im HGöGD nicht genannt. Allerdings habe ich gefordert, dass in absehbarer Zeit durch Erlass neben anderen Bereichen auch der des amtsärztlichen Dienstes hinsichtlich der Speicherfristen geregelt werden muss.

5.8.4.5.4 Unterlagen des sozialpsychiatrischen Dienstes

Die Aufbewahrungsdauer von Unterlagen, die "von Amts wegen" - also durch die Beauftragung anderer öffentlicher Stellen - erstellt worden sind, sollte sich mangels spezialgesetzlicher Vorschriften an den Vorgaben des § 10 Abs. 3 der ärztlichen Berufsordnung orientieren. Darin ist festgelegt, dass ärztliche Aufzeichnungen zehn Jahre aufzubewahren sind. Nicht alle Stellen haben sich an dieser Frist orientiert. So kam es teilweise zu erheblichen zeitlichen Überschreitungen.

5.8.4.6 Zusammenfassung

Grundsätzlich sind die Archive der geprüften Gesundheitsämter in einem respektablen Zustand, was die Aufbewahrung personenbezogener Unterlagen anbelangt. Auch bedingt durch fehlende gesetzliche Regelungen wurden einige wenige Unterlagen nicht rechtzeitig gelöscht bzw. vernichtet. Die Löschung muss nach § 19 Abs. 3 HDSG erfolgen, sobald die Daten für die Aufgabenerfüllung nicht mehr erforderlich sind. In Bereichen mit klaren spezialgesetzlichen Normen - wie etwa den Schuluntersuchungen oder den Hepatitis-C-Unterlagen aus dem Bereich des Infektionsschutzes - waren die Vorgaben umgesetzt. Mit dem neuen HGöGD ist jetzt eine rechtliche Grundlage geschaffen, um auf dem Erlassweg die Aufbewahrungsfristen festzulegen. Einen entsprechenden Hinweis habe ich gegenüber dem Sozialministerium abgegeben. Auch das Regierungspräsidium Darmstadt hat in einem Brief an das Ministerium auf die Erforderlichkeit von klaren Fristen für die Datenspeicherung hingewiesen.

5.8.4.7 Weitere Ergebnisse der Prüfung

5.8.4.7.1 Aktenführung

Kein Anlass zur Kritik in den geprüften Gesundheitsämtern ergab deren Aktenführung. Datenschutzbeauftragte anderer Bundesländer haben auch in der jüngeren Vergangenheit festgestellt, dass einzelne Ämter eine gemeinsame Akte zu Betroffenen führen. In einer solchen Akte werden Untersuchungsergebnisse, Gutachten u.a. verschiedener Fachbereiche zentral geführt. Dies ist jedoch nicht zulässig. Die datenschutzrechtliche Problematik besteht darin, dass bei einer zentralen Aktenführung sämtliche Kontakte eines Betroffenen mit dem Gesundheitsamt von allen Mitarbeiterinnen und Mitarbeitern eingesehen werden können. Von der Schuleingangsuntersuchung bis hin zum Leichenschauschein, also von der Wiege bis zur Bahre, würde zu dem Betroffenen eine einzige Akte geführt. Dies widerspricht den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und der Zweckbindung im Hinblick auf Kenntnisnahme und Verarbeitung personenbezogener (medizinischer) Daten.

In den von mir aufgesuchten Gesundheitsämtern war der Grundsatz einer dezentralen, fachbereichsbezogenen Aktenführung gewährleistet: es gab eine getrennte Aktenführung durch die jeweils zuständigen Stellen.

Verbesserungsbedürftig ist aber fast durchweg die gezielte Kontrolle und Aussonderung von Akten. Nur im Bereich der Schuluntersuchungen, die jahrgangsweise abgelegt werden, ist eine schnelle und gezielte Aussonderung einfach durchführbar und die Aussonderung war deshalb auch vollzogen. In allen anderen Bereichen bereitet es Probleme, eine fristenorientierte Aussonderung vorzunehmen, da in der Vergangenheit keine Kennzeichnungen der Aktenbestände vorgenommen wurden. In verschiedenen Ämtern hat man jedoch angefangen, klare Strukturen hierfür zu schaffen.

5.8.4.7.2 Posteingang

Bis auf ein Gesundheitsamt wurde bei allen anderen die Post ungeöffnet und direkt dem Amt zugestellt. Teilweise treten die Ämter in der Öffentlichkeit als eigenständige Behörde auf, teilweise sind sie als Teil der Kreis- oder Stadtverwaltung klassifiziert. Unabhängig davon muss gewährleistet sein, dass die Kommunikation mit dem Gesundheitsamt, insbesondere der Schriftverkehr, weitgehend vertraulich bleibt.

Beim Gesundheitsamt der Kreises Bergstraße war dies nicht gewährleistet. Die für das Amt eindeutig adressierte Post, die u.a. ärztliche Gutachten oder Betreuungsangelegenheiten zum Inhalt haben kann, wurde in der zentralen Posteingangsstelle geöffnet und mit einem Eingangsstempel versehen. Die gleiche Prozedur wurde im Gesundheitsamt selbst vollzogen. Die geöffnete Post konnte im Bereich der zentralen Annahme in der Kreisverwaltung und auf dem Weg von dort zum Gesundheitsamt hin von Unbefugten eingesehen werden.
Meiner Forderung, diese Praxis einzustellen und die Post ungeöffnet dem Gesundheitsamt zu übermitteln, wurde unmittelbar nachgekommen.

5.8.4.7.3 Sozialpsychiatrischer Dienst

In den vergangenen Jahren gab es immer wieder Diskussionen darüber, in welcher Form der Sozialpsychiatrische Dienst (SpD) als Organisationseinheit in die Strukturen des Gesundheitsamtes einzubeziehen ist. Hintergrund dieser Fragestellung ist die heterogene Aufgabenstellung des Dienstes. Einerseits steht er Hilfesuchenden für freiwillige Beratungen zur Verfügung. Andererseits wird der SpD auch amtlich tätig, insbesondere dann, wenn er von einem anderen Amt beauftragt wird, mit vermeintlich oder tatsächlich auffällig gewordenen Personen Kontakt aufzunehmen. Bei dieser Fallkonstellation wird eine Akte angelegt, die in der Regel zehn Jahre aufbewahrt wird.

In allen Ämtern war Sorge getragen, dass freiwillige Beratungen nicht in die Aktenführung des Amtes Eingang finden und die amtlichen Akten nur mit Einwilligung der Betroffenen anderen Organisationseinheiten des Amtes zugänglich gemacht werden.

5.8.4.7.4 Betreuungsstelle

In welcher Behörde die Betreuungsstelle angesiedelt wird, obliegt grundsätzlich der kommunalen Organisationshoheit. In vielen Fällen erfolgt dies beim Gesundheitsamt. Dies ist dann unproblematisch, wenn eine sachliche und personelle Trennung zu anderen Bereichen innerhalb des Gesundheitsamts umgesetzt ist. Vor allem personelle Sachzwänge haben es in einzelnen Ämtern erforderlich gemacht, dass Mitarbeiter des SpD auch in der Betreuungsstelle tätig sind. Das kann die Konstellation zur Folge haben, dass ein Mitarbeiter zunächst im Wege einer psychologischen Beratung Kontakt zu einem oder einer Betroffenen erhält, um im Anschluss für dieselbe Person eine Betreuung einzuleiten. Hier verquicken sich unterschiedliche Aufgabenstellungen. Auch in diesen Fällen ist eine strikte Trennung der Aktenbestände zu gewährleisten. Es muss jederzeit erkennbar sein, in welchem Kontext ein Mitarbeiter oder eine Mitarbeiterin für den SpD tätig werden und wann dieselbe Person in der Funktion als Beschäftigte der Betreuungsstelle aufgetreten ist. Damit wird auch transparent, welche Daten für welche Aufgabenstellung verwendet werden und es ist nachvollziehbar, ob die vorgegebene Zweckbindung eingehalten wurde.

5.8.5 Prüfung beim MDK Sachsen-Anhalt

Die Auftragsdatenverarbeitung des MDK Sachsen-Anhalt für den MDK Hessen, welche die elektronische Aufbereitung von Akten des MDK Hessen über Begutachtungen im Krankenhaus beinhaltet, entspricht im Wesentlichen den Vorgaben des § 80 SGB X i.V.m. § 78a SGB. Allerdings fehlte es an den erforderlichen Verfahrensverzeichnissen.
Die fristgerechte Vernichtung von Akten aus einem anderen Auftragsdatenverarbeitungsverhältnis war nicht erfolgt.

5.8.5.1 Art und Umfang des Datenverarbeitungsauftrages

Seit einigen Jahren lässt der MDK Hessen personenbezogene Daten im Auftrag durch den MDK Sachsen-Anhalt bzw. dessen Tochterunternehmen MedFlex GmbH verarbeiten. Über die rechtlichen Rahmenbedingungen einer Auftragsdatenverarbeitung sowie die inhaltlichen Aspekte der einzelnen Aufträge habe ich mich ausführlich geäußert (s. 33. Tätigkeitsbericht, Ziff. 5.8.2 und 34. Tätigkeitsbericht, Ziff. 5.8.7). Wohl kaum eine andere öffentliche Stelle des Landes Hessen hat neben dem MDK Hessen in derartigem Umfang Datenverarbeitungsprozesse ausgelagert. Dies beinhaltet die Führung eines Papierarchivs und der elektronischen Aufbereitung von Akten daraus ebenso wie das Schreiben von Briefen und Berichten, die per E-Mail als Sprachdatei von hessischen Geschäftsstellen des MDK nach Sachsen-Anhalt zum dortigen MDK in Magdeburg verschickt werden.

Anfang 2007 kam ein weiterer Auftrag hinzu. Dabei handelt es sich um die fallabschließende Archivierung von Unterlagen der Krankenhausbegutachtungen des MDK Hessen sowie auf Anforderung durch hessische MDK-Geschäftsstellen deren digitale Aufbereitung. Der Umfang des Verarbeitungsauftrages beträgt schätzungsweise 80.000 Akten jährlich.

5.8.5.2 Transport und Verarbeitung der Akten

Der Datenschutzbeauftragte des MDK war in die Planungsphase des DV-Projekts eingeschaltet. Er wies an, die medizinischen Unterlagen für den Transport, der von einem Paketdienst durchgeführt wird, zu versiegeln. Hierfür wird ein Sicherheitsklebeband benutzt, um etwaige Öffnungsversuche am Paket auf dem Transportweg zu erkennen.

Die Pakete werden direkt in das Archiv des MDK Sachsen-Anhalt geliefert und dort geöffnet. Danach werden die Unterlagen sortiert. Schließlich werden diese, entsprechend dem Verfahren bei dem Auftrag "Pflegebegutachtungen", auf Anforderung digitalisiert und über die vorhandene Standleitung von Magdeburg auf den Server des MDK Hessen in Oberursel weitergeleitet.

5.8.5.3 Ergebnis der Prüfung

Der Verfahrensablauf dieses Projektes war nach dem damaligen Kenntnisstand datenschutzrechtlich ohne erkennbare Mängel. Allerdings gab es sowohl zu diesem Datenverarbeitungsauftrag wie zu den anderen Projekten keine Verfahrensbeschreibungen bzw. Verfahrensverzeichnisse. Dieses Defizit habe ich ebenso bemängelt wie die Tatsache, dass die Aktenvernichtung aus dem Archivierungsauftrag für die Pflegegutachten zeitlich im Rückstand war. Akten aus dem Papierarchiv des Jahres 2001 waren noch nicht entsprechend der fünfjährigen Aufbewahrungsfrist des § 276 Abs. 2 SGB V vernichtet.

§ 276 Abs. 2 SGB V

Der Medizinische Dienst darf Sozialdaten nur erheben und speichern, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen nach § 275 und für die Modellvorhaben nach § 275a erforderlich ist; haben die Krankenkassen nach § 275 Abs. 1 bis 3 eine gutachtliche Stellungnahme oder Prüfung durch den Medizinischen Dienst veranlasst, sind die Leistungserbringer verpflichtet, Sozialdaten auf Anforderung des Medizinischen Dienstes unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist. … Die Sozialdaten sind nach fünf Jahren zu löschen. …

Der kommissarische Geschäftsführer des MDK Hessen hat mir nach Kenntnisnahme des Prüfberichtes zugesichert, die Defizite umgehend beheben zu lassen. Verfahrensverzeichnisse wurden gefertigt und dem Datenschutzbeauftragten des MDK Hessen vorgelegt. Die Vernichtung der vom Fristablauf betroffenen Akten des Papierarchivs wurde zugesagt und ist mittlerweile erfolgt.

5.8.6 Prüfung beim Klinikum Fulda

Eine stichprobenartige Prüfung im Klinikum Fulda hat nur in einigen wenigen Einzelfragen Anlass zur Kritik gegeben. Allerdings sind in dem vom Krankenhaus verwendeten Formulartext des Behandlungsvertrags einige datenschutzrechtliche Aspekte nicht hinreichend beachtet.

Das Klinikum Fulda ist mit fast 1.000 Betten in 29 Kliniken und Instituten das größte Krankenhaus in Osthessen und gehört der höchsten Versorgungsstufe an. In einem Einzugsgebiet von etwa 500.000 Einwohnern versorgen 2.600 Mitarbeiterinnen und Mitarbeiter jährlich ca. 38.000 stationäre Patienten. In diesem Zusammenhang fallen zahlreiche personenbezogene, medizinische Daten an, die vom Krankenhaus vor dem unbefugten Zugriff Dritter angemessen geschützt werden müssen.

Die im Klinikum durchgeführte Prüfung war zeitlich und inhaltlich begrenzt; oft musste der erste Augenschein genügen. Dies vorausgeschickt, brachte die Prüfung die nachfolgend erläuterten Ergebnisse.

5.8.6.1 Rechtliche Aspekte

5.8.6.1.1 Formulartext des Behandlungsvertrags

Im Formulartext des Behandlungsvertrags sind einige datenschutzrechtliche Aspekte nicht hinreichend beachtet. Die Erhebung von sog. Pflichtangaben, die zur Durchführung der Behandlung erforderlich sind, und von freiwilligen Angaben, die nach Information über den Zweck der Datenerhebung und die Weiterverarbeitung der Daten zusätzlich vom Patienten erhoben werden können, ist nicht klar getrennt. Dadurch werden die rechtliche Grundlage und der Zweck der Datenerhebungen

nicht ausreichend für die Patienten klar. Freiwillige Angaben sind insbesondere Angaben zum Familienstand, der Konfession, dem Beruf, dem Hausarzt und evtl. zu benachrichtigenden Angehörigen.

In dem Formular werden die freiwilligen Angaben zum Teil nicht als solche gekennzeichnet. Bei dem Datum Konfession steht die Erläuterung des Zwecks der Erhebung an einer anderen, späteren Stelle als das Datenfeld. Unklar ist insbesondere auch der Punkt Auskunft über den Aufenthalt: Im Formular ist der Satz enthalten "Darüber hinaus bin ich damit einverstanden, dass Privatpersonen, die mit mir in Verbindung treten wollen, Auskunft über meinen Aufenthalt im Klinikum Fulda erhalten". Diese Formulierung erweckt den Eindruck, dass eine Einwilligung eingeholt wird, in dem Formular wird aber keine Möglichkeit gegeben, eine Auskunftserteilung abzulehnen. Der Patient muss den Behandlungsvertrag insgesamt einschließlich dieser Formulierung unterschreiben. Ein separates zusätzliches Formular zur Einrichtung einer Auskunftssperre wurde später offenbar entwickelt und wird den Patienten ausgehändigt. Damit liegen dann aber zwei sich widersprechende Erklärungen des Patienten vor.

5.8.6.1.2 Hinweise zur Datenverarbeitung im Behandlungsvertrag

Das Formular enthält einen Hinweis auf die Datenverarbeitung. Dieser Hinweis ist allerdings sehr pauschal formuliert und für Patienten schwer verständlich. Hinzu kommt, dass die Rechtslage bei den erwähnten Konstellationen sehr unterschiedlich ist und zum Teil eine Einwilligung des Patienten eingeholt werden muss. Für die Krankenhäuser in Hessen gilt gemäß § 12 HKHG ergänzend zur Regelung des § 12 das HDSG. Gemäß § 12 Abs. 4 HDSG ist der Patient in geeigneter Weise über den Zweck der Datenverarbeitung aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Die Information sollte daher überarbeitet werden, wobei uns der Wunsch, den Patienten nicht mit zu vielen Informationen zu überfordern, durchaus nachvollziehbar ist. Ergänzend kann und sollte daher für Einzelfragen zum Datenschutz ein Ansprechpartner im Klinikum genannt werden.

5.8.6.1.3 Medizinisches Versorgungszentrum

Im Klinikum befindet sich als rechtlich selbständige Organisationseinheit ein Medizinisches Versorgungszentrum. Dies versorgt u.a. Patienten des Klinikums ambulant. Das Medizinische Versorgungszentrum und das Klinikum Fulda sind aus datenschutzrechtlicher Sicht zwei zu unterscheidende Daten verarbeitende Stellen. Hinsichtlich der wechselseitigen Nutzung der Datenbestände der beiden Stellen haben sich datenschutzrechtliche Fragen ergeben, die im nächsten Berichtszeitraum einer Klärung unterzogen werden müssen.

5.8.6.2 Technische und organisatorische Aspekte

Meine Prüfung hat hinsichtlich der Datensicherheit keinen Anlass zur Beanstandung gegeben. Die Aktenaufbewahrung garantierte in den geprüften Bereichen - dies waren einige Ambulanzen sowie eine Krankenstation - den Schutz vor unbefugter Kenntnisnahme bzw. Zugriff. Die Standorte der Telefaxgeräte waren sorgsam ausgewählt.

5.8.6.2.1 Pforte und Telefonzentrale

Ein Klinikum ist keine informationelle Einheit. Jeder Mitarbeiter darf nur die Patientendaten zur Kenntnis erhalten, die tatsächlich für die Aufgabenerfüllung benötigt werden. Der Datensatz, den die Pforte bzw. Telefonzentrale vom Patienten erhält, ist in seinen einzelnen Merkmalen hinreichend begrenzt.

5.8.6.2.2 Videoüberwachung

Bestimmte Zonen des Klinikums werden videoüberwacht. Allerdings gab es nur einen allgemein gehaltenen Hinweis hierzu im Eingangsbereich. Eine konkrete Benennung eines hiervon betroffenen Bereiches fehlte.

5.8.6.2.3 Betriebsvereinbarung zur Nutzung von Internet und E-Mail

Die Regelungen in der Betriebsvereinbarung entsprechen den Anforderungen hinsichtlich der erforderlichen Transparenz gegenüber den Nutzern, wenn diese Nutzung für private Zwecke erfolgt.

5.8.6.2.4 Unzureichende Zugangskontrolle zum Technikraum

Zur EDV-Abteilung muss der Besucher einen davor gelagerten Raum passieren, in dem wesentliche Teile der Haustechnik untergebracht sind. Die Tür hierzu war offen und zudem ohne Schloss. Unbefugte hatten so die Möglichkeit, den Raum unbeobachtet zu betreten und möglichen Schaden anzurichten.

5.8.6.3 Fazit

Gravierende datenschutzrechtliche Defizite waren bei dieser stichprobenhaften Prüfung im Klinikum Fulda nicht festzustellen. Einzelne Unzulänglichkeiten hinsichtlich der Videoüberwachung oder des Zutritts in der Technik-/DV-Bereich sind abgestellt worden. Verbesserungswürdig ist das Patientenaufnahmeformular. Diesbezüglich gibt es weitere Kontakte mit dem Klinikum. Auch besteht noch weiterer Klärungsbedarf beim Medizinischen Versorgungszentrum.

5.8.7 Unzulässiges Einwilligungsformular der AOK Hessen

Bei Anträgen auf Pflegeleistungen kann im Einzelfall eine Einsichtnahme in bereits vorhandene Pflegedokumentationen zur Entscheidung über die Leistungsberechtigung erforderlich sein. Hierfür muss eine rechtswirksame Einwilligung der Betroffenen eingeholt werden. Ein von mir bereits vor längerer Zeit beanstandetes unklares Einwilligungsformular wurde auch 2007 noch von verschiedenen AOK-Geschäftsstellen verwendet.

Ebenso wie 2006 habe ich auch 2007 Beschwerden bezüglich eines von der AOK Hessen im Zusammenhang mit Anträgen auf Pflegeleistungen nach dem SGB XI (Soziale Pflegeversicherung) verwendetes Einwilligungsformular erhalten. Dieses Formular habe ich bereits vor längerer Zeit gegenüber der AOK Hessen beanstandet. Die AOK Hessen hat meine Rechtsauffassung geteilt und zugesagt, dass dieses Formular nicht mehr verwendet wird. Dessen ungeachtet ist das Formular in verschiedenen Geschäftsstellen der AOK weiterhin verwendet worden.

Einverständniserklärung

Überprüfung der Qualität der Leistungserbringung nach § 37 SGB V und § 80 SGB XI

Name, Vorname: _____

Geburtsdatum: _____

KV-Nr.: _____

Anschrift: _____

Hiermit erkläre ich mein Einverständnis, dass die AOK Hessen/AOK Hessen Pflegekasse zur Überprüfung der Qualität der Leistungserbringung in dem erforderlichen Umfang Einblick in meine Patientendokumentation des Pflegedienstes und Arztes nehmen und ggf. Fotokopien meiner Unterlagen anfertigen kann. Dies gilt auch für Dokumentationsunterlagen, die beim Pflegedienst oder Arzt aufbewahrt werden. Insoweit entbinde ich den Pflegedienst und den Arzt von seiner Schweigepflicht.

_____

Ort, Datum, Unterschrift

Datenschutzhinweis (§ 67a Abs. 3 Sozialgesetzbuch X):
Die hier erhobenen Daten unterliegen den Bestimmungen des Sozialgesetzbuches (§ 35 SGB I). Sie werden nur im Rahmen der gesetzlichen Aufgabenerfüllung der AOK Hessen/AOK Hessen Pflegekasse verwendet (§ 37 SGB V, §§ 36, 80 SGB XI).
Die Entbindung von der Schweigepflicht ist zweckgebunden und beruht auf Freiwilligkeit. Sofern die Einwilligung nicht erteilt wird, hat dies keine Auswirkung auf die Leistungserbringung.
Diese Einverständniserklärung kann jederzeit widerrufen werden.

5.8.7.1 Datenschutzrechtliche Vorgaben

Eine Erhebung und Weiterverarbeitung personenbezogener Daten durch die AOK ist nur zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist und die Datenerhebung aufgrund einer Rechtsvorschrift oder einer Einwilligung der Betroffenen erfolgt (§§ 67a ff. SGB X). Konkret bedeutet dies, dass bei einer Antragsprüfung nur die für die Bearbeitung des Antrags tatsächlich erforderlichen Daten erhoben werden dürfen. Insbesondere darf nicht routinemäßig Einblick in Pflegedokumentationen genommen werden. Soweit im Einzelfall ein Einblick in die Pflegedokumentation zur abschließenden Klärung des Leistungsanspruchs tatsächlich erforderlich ist, ist eine Einwilligung des Betroffenen einzuholen, denn Pflegedokumentationen enthalten besonders sensitive persönliche Daten und sie werden grundsätzlich nur für die Durchführung der Pflege erstellt. In der Einwilligungserklärung sind der Zweck der Einsichtnahme und die weitere Verfahrensweise mit den Daten sowie die rechtlichen Rahmenbedingungen (Mitwirkungspflicht des Antragsstellers nach §§ 60 Abs. 1, 65 SGB I) für die Betroffenen klar darzulegen.

5.8.7.2 Defizite der Verfahrensweise der AOK

Diese rechtlichen Vorgaben werden mit der Verwendung dieses Formulars nicht eingehalten:

- Das Formular wird offensichtlich **routinemäßig** bei jeder Antragstellung vorgelegt.

- Zudem wird der Zweck und Umfang der geplanten Datenverarbeitung den Betroffenen nicht zutreffend mitgeteilt: In dem Formular wird die **Überprüfung der Qualität der Leistungserbringung** als Zweck der geplanten Datenverarbeitung genannt. Das Formular wird aber den Betroffenen stets ausgehändigt im Zusammenhang mit der **Prüfung eines Antrags auf eine Pflegeleistung**, also in einem ganz anderen rechtlichen Zusammenhang.

- Das Formular enthält auch darüber hinausgehend Unklarheiten:
  Wenn Daten im Rahmen der Antragsprüfung erhoben werden, sind die Vorschriften der §§ 60 Abs. 1 und 65 SGB I einschlägig, d.h. konkret, dass der Antragsteller alle leistungserheblichen, für den Pflegebedarf relevanten Informationen angeben muss und er eine Mitwirkungspflicht hat. In dem Formular wird hingegen darauf hingewiesen, dass die Einwilligung freiwillig ist und die Ablehnung keine Auswirkung auf die Leistungserbringung hat. Wenn Letzteres zutrifft, sind die Daten offensichtlich nicht für die Antragsprüfung und damit auch nicht für die Aufgabenerfüllung der AOK in diesem Zusammenhang erforderlich. Die Erhebung der Daten mit dem Einwilligungsformular ist daher auch aus diesem Grund unzulässig: Nicht erforderliche Daten dürfen nicht erhoben werden.

Es entspricht leider der allgemeinen Erfahrung meiner Dienststelle, dass Einwilligungsformulare im Zusammenhang mit Leistungsanträgen oft von den Antragstellern unterschrieben werden - auch dann, wenn sie unklar und damit unzulässig sind -, weil die Betroffenen verunsichert sind und eine Ablehnung ihres Leistungsantrags fürchten.

Die AOK Hessen habe ich um Überprüfung gebeten, wie es dazu kommt, dass dieses Formular, mit dem keine rechtswirksamen Einwilligungen eingeholt werden können, von den verschiedensten AOK-Geschäftsstellen nach wie vor verwendet wird. Die AOK Hessen hat mir nach Überprüfung geantwortet, dass nach dortiger Feststellung das Einwilligungsformular tatsächlich versehentlich weiterhin vom zuständigen Fachbereich versandt wurde. Passiert sei dies dadurch, dass innerhalb des Textsystems das Einwilligungsformular stets zusammen mit dem Antragsformular automatisch ausgedruckt wurde. Es wurde versäumt, das Einwilligungsformular aus dem Textsystem herauszunehmen. Aufgrund meines Schreibens seien zum einen alle Mitarbeiter informiert worden, dass das Formular nicht mehr verwendet werden darf. Zum anderen sei das Formular aus dem Textsystem gelöscht worden, sodass der Vordruck auch nicht mehr ausgedruckt werden könne.

5.8.8 Bilder von Neugeborenen auf der Homepage von Krankenhäusern

Viele Krankenhäuser veröffentlichen inzwischen Bilder der bei ihnen geborenen Kinder im Internet. Zuvor müssen die Eltern über die Art und Weise und die Konsequenzen einer Veröffentlichung informiert und um Einwilligung gebeten werden. Zusätzlich zu dem Bild sollten keine personenbezogenen Daten über das Kind und/oder die Eltern im Internet zur Verfügung gestellt werden, die Dritten eine Identifizierung ermöglichen.

Immer mehr Krankenhäuser stellen auch in Hessen auf ihrer Homepage Bilder der Neugeborenen zur Verfügung. Für die Krankenhäuser ist dies eine Möglichkeit, mit einem positiven Anlass für ihr Haus zu werben und gleichzeitig den Eltern einen Service anzubieten, der offenbar zumindest von einem Teil der Eltern sehr geschätzt wird. Für die Eltern ist dies eine Möglichkeit, Verwandten und Freunden - wo immer sie sich aufhalten - schnell und mit wenig Aufwand ein Bild ihres Neugeborenen zukommen zu lassen.

Nach meinen stichprobenartigen Feststellungen und Nachfragen ist die Art und Weise der Veröffentlichung sehr unterschiedlich. Die Krankenhäuser veröffentlichen die Babybilder in der Regel mit dem Geburtsdatum des Kindes, darüber hinaus zum Teil
- nur mit dem Vornamen des Kindes,
- mit dem Vor- und Nachnamen des Kindes,
- mit dem Vor- und Nachnamen der Eltern und
- mit Vor- und Nachnamen sowie (Teil-)angaben zum Wohnort.

Die Einwilligung der Eltern wird soweit ersichtlich in der Regel eingeholt.

Gegen eine Veröffentlichung eines Bildes des Neugeborenen auf der Homepage des Krankenhauses mit Einwilligung der Eltern bestehen keine grundsätzlichen Bedenken. Es sollten jedoch die datenschutzrechtlichen Rahmenbedingungen vor einer Veröffentlichung angemessen berücksichtigt und festgelegt werden:

- Schriftlichkeit der Einwilligung
  Die Veröffentlichung eines Bildes des Neugeborenen bedarf der Einwilligung der Eltern. Die Einwilligung sollte schriftlich eingeholt werden, damit z.B. im Fall eines evtl. späteren Streits im Interesse aller Beteiligten der Ablauf nachvollzogen werden kann.

- Vorherige Information
  Rechtswirksam ist eine Einwilligung in die Datenverarbeitung nur dann, wenn die Betroffenen zuvor über die vorgesehene Datenverarbeitung hinreichend informiert wurden. Konkret bedeutet dies, dass die Eltern - z.B. in einem allgemeinen Merkblatt - insbesondere darüber informiert werden müssen, welche Daten des Kindes und/oder der Eltern zusammen mit dem Bild ins Internet gestellt werden sollen und wann Bild und Daten von der Homepage gelöscht werden. Darüber hinaus müssen die Eltern über die grundsätzlichen Konsequenzen einer Veröffentlichung im Internet informiert werden. Auch wenn die Eltern mit der Veröffentlichung (nur) die Absicht verbinden, dass ihre Verwandten und Freunde das Bild ansehen und herunterladen, so eröffnet die Veröffentlichung die technische und rechtliche Möglichkeit (auch) für unbekannte Dritte weltweit, das Bild und die Daten zur Kenntnis zu nehmen, herunterzuladen, zu speichern und für eigene Zwecke zu verwenden. Das Krankenhaus kann lediglich die Löschung von Bild und Daten auf seiner Homepage zu einem bestimmten Zeitpunkt zusagen und steuern. Auf die Frage, welche Dritte Bild und Daten zu welchem Zweck

herunterladen und weiter speichern, hat das Krankenhaus keinen Einfluss. Über diesen Sachverhalt sollten die Eltern informiert werden, bevor sie nach ihrer Einwilligung gefragt werden.

- Keine Veröffentlichung von personenbezogenen Daten, mit denen die Eltern identifiziert werden können
  Mit dem Bild sollten keine zusätzlichen Daten über Kind und/oder Eltern veröffentlicht werden, die es Dritten ermöglichen, die Eltern zu identifizieren und sie (z.B. für Werbezwecke oder aber auch mit kriminellen Absichten) anzuschreiben oder zuhause aufzusuchen. Über die Eingabe der Suchbegriffe "Babybilder" oder "Babygalerie" und "Krankenhaus" in Internetsuchmaschinen können den Eltern unbekannte Dritte schnell und mühelos Zugang zu den Babybildern erhalten. Identifiziert werden können die Eltern mit etwas Zusatzwissen, das auch zielgerichtet beschafft werden kann, je nach Größe des Wohnorts auch mit Namen und Postleitzahl oder mit Vornamen und Anfangsbuchstaben des Nachnamens. Von einer Veröffentlichung des Anfangsbuchstabens des Nachnamens oder des kompletten Nachnamens der Eltern und/oder (Teilen der) Adresse sollte daher abgesehen werden. Sogar seltene Vornamen der Eltern können unter Umständen bereits zur Identifizierung mit Hilfe von Zusatzwissen ausreichen. Es ist zwar grundsätzlich rechtlich möglich, auch für die Veröffentlichung umfangreicherer Daten die Einwilligung der Eltern einzuholen. Das Krankenhaus hat jedoch zu bedenken, dass den Eltern mit dem Angebot ein guter Service angeboten werden soll. Es liegt im Interesse des Krankenhauses, dass die Veröffentlichung den Eltern nicht später Probleme verursacht, die sie nicht bedacht haben und mit denen sie nicht gerechnet haben. Der Zweck der Veröffentlichung wird regelmäßig erreicht werden können, ohne dass diese zusätzlichen Daten mit dem Bild zusammen veröffentlicht werden. Zumindest sollten die Eltern über das Risiko der Identifizierung informiert werden.

5.9 Sozialwesen

5.9.1 Feststellung der Pflegebedürftigkeit bei Anträgen auf Sozialhilfe

Aufgrund von Anfragen und Beschwerden bezüglich der Einsichtnahme in Pflegedokumentationen habe ich mich 2007 mit dem Verfahren der Feststellung der Pflegebedürftigkeit bei der Stadt Frankfurt befasst. Über die Verfahrensweise wurde Übereinstimmung zwischen der Stadt Frankfurt und mir erzielt. Das bisher von der Stadt Frankfurt verwendete Einwilligungsformular muss überarbeitet werden.

5.9.1.1 Einleitung

Zur Zulässigkeit der Einsichtnahme in Pflegedokumentationen erhalte ich immer wieder Anfragen und Beschwerden. Dies ist auch nicht verwunderlich, da die Pflegedokumentationen oft sehr detaillierte, persönliche und sensitive Daten enthalten. Pflegedokumentationen sind daher auch besonders schutzbedürftig. Sie werden für die Durchführung der Pflege erstellt und dürfen grundsätzlich nur für diesen Zweck verwendet werden. Bei den Anfragen und Diskussionen wird allerdings häufig nicht klar unterschieden zwischen der Frage der Verwendung von Pflegedokumentationen
- bei Anträgen auf Pflegeleistungen nach SGB IX (Soziale Pflegeversicherung) und nach SGB XII (Sozialhilfe),
- bei der Abrechnungsprüfung und
- bei der Qualitätsprüfung,

obwohl die rechtlichen Rahmenbedingungen jeweils unterschiedlich sind.

In diesem Jahr habe ich mich u.a. detailliert mit dem Verfahren der Feststellung der Pflegebedürftigkeit im Rahmen von Anträgen nach SGB XII (Sozialhilfe) beim Jugend- und Sozialamt der Stadt Frankfurt befasst, insbesondere auch mit der Verwendung von Pflegedokumentationen im Rahmen der Antragsprüfung. Das Jugend- und Sozialamt der Stadt Frankfurt am Main ist u.a. zuständig für Leistungen, die sich aus dem SGB XII - Sozialhilfe - ergeben. In § 61 bis § 66 SGB XII ist die Hilfe zur Pflege normiert. Diese wird Pflegebedürftigen gewährt, die selbst nicht pflegeversichert im Sinne des SGB XI (Soziale Pflegeversicherung) sind. Das Gleiche gilt für Pflegebedürftige, bei denen die Leistungen der Pflegekassen (SGB XI) nicht ausreichen. Hier wird die Hilfe zur Pflege dann ergänzend geleistet, wenn die Betroffenen bzw. ihre Angehörigen den Pflegeaufwand aus eigener wirtschaftlicher Kraft nicht schaffen.

5.9.1.2 Datenschutzrechtliche Vorgaben

Bei der Prüfung der Verfahrensweise bin ich von folgenden datenschutzrechtlichen Vorgaben ausgegangen:

- Der Antragsteller muss alle leistungserheblichen, für den Pflegebedarf relevanten Informationen angeben (§ 60 Abs. 1 SGB I).

§ 60 Abs. 1 SGB I

Wer Sozialleistungen beantragt oder erhält, hat

1. alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen,
…

Im Rahmen der Antragsprüfung dürfen aber nur die für die Bearbeitung des Antrags tatsächlich erforderlichen Daten erhoben werden. Konkret bedeutet dies insbesondere, dass nicht routinemäßig Einsicht in evtl. bereits vorhandene Pflegedokumentation genommen werden darf bzw. nicht routinemäßig Pflegedokumentationen für die Antragsbearbeitung kopiert und verwendet werden dürfen, sondern nur im Einzelfall, in dem die Leistungsberechtigung anders nicht abschließend geklärt werden kann.

- Der Kreis der Mitarbeiterinnen und Mitarbeiter, die Zugriff auf die medizinisch-pflegerischen Unterlagen haben, muss klar und restriktiv festgelegt werden.

- Da eine Pflegedokumentation besonders sensitive Daten enthält und sie grundsätzlich nur für die Durchführung der Pflege erstellt wird, muss für die Einsichtnahme im Rahmen der Antragsprüfung eine Einwilligung der Betroffenen eingeholt werden. In der Einwilligungserklärung sind der Zweck der Einsichtnahme und die weitere Verfahrensweise mit den Daten sowie die rechtlichen Rahmenbedingungen (evtl. Mitwirkungspflicht des Antragstellers im Einzelfall nach §§ 60 Abs. 1, 65 SGB I) für die Betroffenen klar darzulegen.

§ 65 Abs. 1 und 2 SGB I

(1) Die Mitwirkungspflichten nach 60 bis 64 bestehen nicht, soweit
1. ihre Erfüllung nicht in einem angemessenen Verhältnis zu der in Anspruch genommenen Sozialleistung oder ihrer Erstattung steht oder
2. ihre Erfüllung dem Betroffenen aus einem wichtigen Grund nicht zugemutet werden kann oder
3. der Leistungsträger sich durch einen geringeren Aufwand als der Antragsteller oder Leistungsberechtigte die erforderlichen Kenntnisse selbst beschaffen kann.

(2) Behandlungen und Untersuchungen,
1. bei denen im Einzelfall ein Schaden für Leben oder Gesundheit nicht mit hoher Wahrscheinlichkeit ausgeschlossen werden kann,
2. die mit erheblichen Schmerzen verbunden sind oder
3. die einen erheblichen Eingriff in die körperliche Unversehrtheit bedeuten, können abgelehnt werden.

5.9.1.3 Verfahrensweise bei der Stadt Frankfurt am Main

In mehreren Besprechungen des Jugend- und Sozialamts, des internen Datenschutzbeauftragten der Stadt Frankfurt und meiner Dienststelle wurde eine Klärung und ein Konsens erzielt über die Verfahrensweise bei der Antragsprüfung. Die künftige Verfahrensweise wurde von der Stadt Frankfurt wie folgt festgelegt:

Betroffene bzw. deren Angehörige stellen beim regional zuständigen Sozialrathaus des Jugend- und Sozialamts der Stadt Frankfurt am Main einen Antrag auf Hilfe zur Pflege. Die örtlich zuständigen Sozialdienste müssen neben der Hilfe zur Pflege auch sonstige Klärungen bzw. Vermittlung weitergehender psychosozialer Hilfe- und Unterstützungsangebote in Einzelfällen herbeiführen. Sie sind zudem die unmittelbaren Ansprechpartner der Klienten bzw. deren Angehöriger und für die Steuerung und Planung der notwendigen Hilfen verantwortlich. Nach Bekanntwerden des Hilfebedarfs (z.B. durch Anruf oder persönliche Vorsprache) erfolgt zunächst eine Beratung durch den Dienst für Alten- und Behindertenhilfe des örtlich zuständigen Sozialrathauses. Dabei werden Art und Umfang des Hilfebedarfs und Möglichkeiten der Hilfen erörtert. Durch die dezentralen Sozialdienste werden häufig auch andere Hilfen aus dem Sozialrecht in den Beratungen erörtert. Dieses erfolgt überwiegend in der häuslichen Umgebung der Antragsteller.

Der Sozialdienst stellt zunächst den akuten Bedarf an ambulanter Hilfe zur Pflege fest. Soweit ärztliche bzw. medizinische Befunde nicht bereits bei Antragstellung dem fallverantwortlichen Sozialdienst vorliegen (dies ist der Regelfall), wird noch ergänzend um die Vorlage entsprechender ärztlicher Stellungnahmen mit den pflegerelevanten Diagnosen gebeten. Dies sind z.B. Festlegungen durch den Medizinischen Dienst der Pflegekassen oder die ärztliche Stellungnahme des Haus- oder Facharztes.

Seitens der dezentralen Sozialdienste und der dezentralen Leistungsabteilung (wirtschaftliche Sozialhilfe) wird gemeinsam mit dem Betroffenen eine Akuthilfe verabredet und eine vorläufige Kostenzusage gegeben. Dies ist insbesondere bei Neuanträgen erforderlich. Hier muss die Sozialbehörde zeitnah reagieren. Der regional zuständige Sozialdienst übersendet die zur abschließenden Antragsbearbeitung eingereichten Unterlagen an den zentralen Fachdienst für ambulante Hilfen zur Pflege mit der Bitte um Begutachtung. Der Fachdienst für ambulante Pflege prüft ausschließlich die pflegerelevanten Sachverhalte, insbesondere mit der Zielsetzung einer fördernden bzw. aktivierenden Pflege für die zu Pflegenden. Seitens des regional zuständigen Sozialdienstes werden keine Kopien aus Pflegedokumentationen gefertigt. Vergleichbar sind die Abläufe in Fällen, bei denen eine Erhöhung des Pflegebedarfs (oder auch eine Reduzierung) beantragt wird.

Der zentrale Fachdienst für ambulante Hilfen entscheidet im Einzelfall, ob bereits alle leistungserheblichen, für den Pflegebedarf relevanten Informationen schlüssig vorliegen und nach Aktenlage über den Antrag entschieden werden kann oder ein Hausbesuch für erforderlich gehalten wird. Die Mitarbeiterinnen und Mitarbeiter des Fachdienstes haben eine pflegefachliche Ausbildung mit (entsprechender) Zusatzqualifikation und langjährige Pflegepraxis. Im Falle eines Hausbesuches wird von der Pflegefachkraft des zentralen Fachdienstes geprüft, ob, soweit überhaupt schon vorhanden, eine Einsicht in die Pflegedokumentation im Einzelfall geboten ist, und ggf., ob eine Kopie von (Teilen) der Pflegedokumentation für die weitere Antragsbearbeitung erforderlich ist.

Vor der Einsichtnahme bzw. der Erstellung einer Kopie der Pflegedokumentation wird von der Pflegefachkraft des zentralen Fachdienstes die Einwilligung des Betroffenen bzw. der Betreuer eingeholt. In den Fällen, in denen Betroffene bzw. ihre Betreuer ihre Einwilligung nicht erteilen, erfolgt keine Einsichtnahme bzw. Kopienerstellung. Über die weitere Verfahrensweise wird nach den Umständen des Einzelfalls entschieden.

Nach der o.a. Überprüfung der Situation wird mit den Betroffenen, deren Angehörigen oder Betreuern und ggf. mit dem bereits tätigen Pflegedienst eine Optimierung der Hilfe erörtert. Dies ist insbesondere in den Fällen notwendig, bei denen

aus Sicht des Fachdienstes seither tatsächlich falsche bzw. nicht geeignete Pflegemaßnahmen durchgeführt wurden oder der tatsächliche Bedarf des Betroffenen nicht gedeckt wird. Abschließend erstellt der Fachdienst sein Gutachten zum Bedarf an Hilfe zur Pflege und übermittelt dieses an das zuständige Sozialrathaus. Von dort werden die entsprechenden Leistungsbescheide erteilt.

Die von dem zentralen Fachdienst für ambulante Hilfe zur Pflege festgestellten Prüfungsergebnisse sind von den regional zuständigen Organisationseinheiten des Jugend- und Sozialamtes (Sozialrathäuser) verbindlich umzusetzen und münden in einen Leistungsbescheid, der durch den Bereich wirtschaftliche Hilfe in den zuständigen Sozialrathäusern verwaltungsrechtlich und technisch abgewickelt wird.

Organisatorisch wurde festgelegt, dass die medizinischen bzw. pflegerelevanten Dokumentationen wie z.B. die Fotokopien beim Prüfdienst verbleiben und nicht an den Sozialdienst bzw. an die wirtschaftliche Sozialhilfe (Leistungsabteilung) weitergegeben werden. Der Zeitraum der Aufbewahrung betrug bisher sieben Jahre. Es wird derzeit noch diskutiert, in welchem Umfang diese Frist verkürzt werden kann.

5.9.1.4 Abschließende Bewertung

Die unter Ziff. 5.9.1.2 dargelegten datenschutzrechtlichen Vorgaben werden von der Stadt Frankfurt bei der Antragsprüfung berücksichtigt:

- Im Zeitraum von Januar bis Juni 2007 hat der zentrale Fachdienst für ambulante Hilfen bei 155 von 208 Anträgen nach Aktenlage ohne Hausbesuch über den Antrag entschieden. Nur in einer geringen Anzahl der Fälle (36 Fälle von 208 im o.a. Zeitraum), die während des Hausbesuches nicht hinreichend geklärt werden konnten, wurde im Einzelfall eine Kopie aus der Pflegedokumentation gezogen, um den Antrag weiter bearbeiten zu können. Die Notwendigkeit einer Einsichtnahme in die Pflegedokumentation kann sich nach Darstellung der Stadt Frankfurt z.B. ergeben, wenn offensichtlich zwischen den Antragsunterlagen und dem Eindruck beim Hausbesuch Diskrepanzen über Art und Umfang der Pflege erkennbar sind. Die Notwendigkeit einer Kopie der Pflegedokumentation kann sich z.B. ergeben, wenn wegen zuvor festgestellter Unklarheiten fachliche Erörterungen z.B. mit dem bereits tätigen ambulanten Pflegedienst oder eine noch zu vertiefende Nachprüfung über den tatsächlichen Pflegebedarf geboten ist. Dies ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

- Der Kreis der Mitarbeiterinnen und Mitarbeiter, die Zugriff auf die medizinisch-pflegerischen Unterlagen haben, wurde klar und entsprechend der jeweiligen Aufgabenstellung festgelegt, insbesondere verbleiben die medizinischen bzw. pflegerelevanten Informationen ausschließlich beim zentralen Fachdienst.

- In den - zahlenmäßig begrenzten - Fällen einer Einsichtnahme in die Pflegedokumentation bzw. einer Kopie der Pflegedokumentation wird eine Einwilligung der Betroffenen eingeholt.

Die Verfahrensweise und die rechtlichen Rahmenbedingungen der Verwendung von Pflegedokumentationen sind allerdings in dem bisher von der Stadt Frankfurt verwendeten Einwilligungsformular nicht korrekt wiedergegeben. Es wurde mir daher zugesagt, dass das Einwilligungsformular überarbeitet wird. Eine Neufassung liegt mir noch nicht vor.

5.9.2 Hartz IV - Datenerhebung bei Dritten

Die Sozialverwaltung ist nur in Ausnahmefällen befugt, Daten über den Leistungsempfänger bei Dritten (z.B. dem Vermieter) zu erheben.

Ein Empfänger von Arbeitslosengeld II hat bei mir angefragt, ob die Verwaltungsbehörde berechtigt sei, bei seinem Vermieter Erkundigungen einzuholen, um einen von der Behörde vermuteten Sozialleistungsbetrug aufzudecken.

Von Sozialbehörden wird regelmäßig der Hinweis gegeben, man habe, um Sozialleistungsmissbrauch zu verhindern, wegen des Untersuchungsgrundsatzes das Recht und auch die Pflicht, den Sachverhalt hinreichend aufzuklären. Dies reicht als Begründung nicht aus.

Zwar ist die Geltung des Untersuchungsgrundsatzes im Verwaltungsverfahren gesetzlich normiert (§ 20 SGB X), aber zugleich ist festgelegt, dass der Sozialdatenschutz im Verhältnis zum Untersuchungsgrundsatz vorrangig ist (§ 37 Satz 3 SGB I).

Diese Vorrangigkeit des Sozialdatenschutzes hat zur Konsequenz, dass die Behörde grundsätzlich nicht berechtigt ist, den Sachverhalt in der Weise aufzuklären, dass sie Auskünfte etwa beim Vermieter eines Sozialleistungsempfängers einholt. Denn im Sozialdatenschutzrecht gilt, nicht anders als im allgemeinen Datenschutzrecht auch, dass Daten grundsätzlich beim Betroffenen zu erheben sind.

Allerdings gilt der Grundsatz der Datenerhebung beim Betroffenen nicht uneingeschränkt. In Ausnahmefällen ist es nämlich nach § 67a SGB X zulässig, Erkundigungen auch bei anderen Personen einzuholen.

§ 67a SGB X

(1) Das Erheben von Sozialdaten…ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle …erforderlich ist…

(2) Sozialdaten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden …
2. bei anderen Personen oder Stellen, wenn …
b) aa) die Aufgaben nach diesem Gesetzbuch ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen …

Eine Aufgabe kann ihrer Art nach eine Erhebung bei anderen Personen erforderlich machen, wenn bspw. infolge falscher oder wenig glaubhafter Angaben des Betroffenen der relevante Sachverhalt schwierig oder nicht zu klären und deshalb eine zusätzliche Befragung Dritter notwendig ist (vergleiche auch Rombach in Hauck-Noftz, SGB X, § 67a, Rdnr. 98, Müller-Thele, Hartz IV-Kontrollmaßnahmen gegen Leistungsmissbrauch, RDV 2005, 257 [258]). Allerdings müssen die Erkundigungen seitens der Behörde so gestaltet werden, dass der Dritte über den Betroffenen nur diejenigen Informationen erhält, die zur Sachverhaltsermittlung notwendig sind. Von einer Befragung Dritter seitens der Behörde muss sogar gänzlich abgesehen werden, falls Anhaltspunkte dafür bestehen, dass dadurch überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden können (§ 67a Abs. 2 SGB X a. E.).

Den anfragenden Bürger habe ich über die eben beschriebene Rechtslage informiert.

5.9.3 Übermittlung von Sozialdaten durch das Jugendamt an das Familiengericht

Soweit ein Informant des Jugendamtes ein berechtigtes Interesse an der Geheimhaltung seiner Daten hat, darf das Jugendamt diese Daten anderen Personen oder Stellen grundsätzlich nicht bekannt geben. Werden diese Daten an das Familiengericht übermittelt, sollte das Jugendamt das Gericht auf die zugesicherte Vertraulichkeit hinweisen.

5.9.3.1 Der Fall

Der behördliche Datenschutzbeauftragte einer Kreisverwaltung trat mit der Frage an mich heran, ob personenbezogene Daten eines Informanten des Jugendamtes an das Familiengericht oder andere Dritte übermittelt werden dürfen.

Konkret ging es um einen Vater, der gegenüber der Behörde angezeigt hatte, dass die von ihm getrennt lebende (alkoholkranke) Ehefrau die beiden aus der Ehe hervorgegangenen Kinder, insbesondere die vier Monate alte Tochter, nicht ordnungsgemäß versorgen könne. Dem vorausgegangen war ein Hilferuf des 16-jährigen Sohnes des getrennt lebenden Paares. Der Vater bat in dem Telefonat mit dem Jugendamt ausdrücklich darum, die Informationen vertraulich zu behandeln, da ihm sonst möglicherweise Repressalien durch den drogenabhängigen Freund der Mutter drohten. Der Allgemeine Soziale Dienst des Landkreises fand die Mutter tatsächlich hilflos vor und übergab die Kinder der Pflege. Ein Vermerk des zuständigen Bearbeiters mit einem Hinweis auf den "Informanten" (also den Vater) sowie Gesprächsprotokolle mit dem 16-jährigen Sohn wurden Bestandteil der Akte. Der Vorgang wurde im weiteren Verlauf samt der Akte an das Familiengericht weitergegeben. Dort wurde die Akte kopiert und der verfahrensbeteiligten Mutter zur Verfügung gestellt, wodurch die Akte auch dem drogenabhängigen Freund der Mutter zur Kenntnis gelangte. Damit wurde bekannt, wer das Verfahren in Gang gebracht und welche Aussagen der Sohn gemacht hatte.

5.9.3.2 Zulässigkeit der Datenübermittlung

5.9.3.2.1 Übermittlung an Dritte

Eine Übermittlung von Daten an andere Personen oder Stellen im Wege z.B. der Akteneinsicht oder der Übergabe von Kopien aus der Akte, z.B. an die Mutter, wäre unzulässig, trägt man den Kernsätzen des Urteil des BVerwG vom 4. September 2003 (BVerwG 5 C 48.02) Rechnung. Danach ist eine Behörde zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge wegen der berechtigten Interessen der Beteiligten oder dritter Personen geheim gehalten werden müssen; jedenfalls bei entgegenstehenden berechtigten Geheimhaltungsinteressen dritter Personen ist sie nicht berechtigt, Akteneinsicht zu gewähren. Bei dem Namen eines Behördeninformanten handelt es sich gemäß § 35 Abs. 1 SGB I i.V.m. § 67 Abs. 1 SGB X um ein geschütztes Sozialdatum, dessen Offenbarung nur nach Maßgabe der gesetzlichen Bestimmungen des § 67d i.V.m. §§ 68 bis 77 SGB X oder einer anderen Rechtsvorschrift im SGB zulässig ist.

Auch eine Auskunftserteilung i.S.d. § 83 Abs. 1 S. 1 SGB X kommt nicht in Betracht, da dem die Regelung des § 83 Abs. 4 Nr. 3 SGB X entgegensteht. Eine Güterabwägung zwischen den in § 25 Abs. 3 bzw. § 83 Abs. 1 Nr. 1 SGB X genannten Auskunftsansprüchen der Mutter und den schutzwürdigen Belangen des Vaters muss dazu führen, die Schutzwürdigkeit höher einzustufen als den Auskunftsanspruch. Das Geheimhaltungsinteresse überwiegt insbesondere dann, wenn keine Anhaltspunkte dafür vorliegen, dass der Informant wider besseres Wissen oder leichtfertig falsche Behauptungen aufgestellt hat.

§ 25 Abs. 3 SGB X

Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge wegen der berechtigten Interessen der Beteiligten oder dritter Personen geheim gehalten werden müssen.

§ 83 Abs. 1 Satz 1 SGB X

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

§ 83 Abs. 4 SGB X

Die Auskunftserteilung unterbleibt, soweit
1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen,

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

Der Vater hatte die von ihm beanspruchte Vertraulichkeit mit möglichen Attacken gegen seine Person begründet, würde der Sachverhalt der Mutter und ihrem Freund zugänglich. In diesem Zusammenhang stellt sich auch die Frage, ob es zwingend war, in den Aktenvermerken den Namen des Informanten zu nennen. Der Umstand, dass ein Informant Vertraulichkeit einfordert, muss nicht zwangsläufig dazu führen, die Akte zu "anonymisieren". Vor allem dann nicht, wenn dies Ausgangspunkt einer umfangreichen Aktion verschiedener Behörden (Jugendamt, Polizei, Familiengericht) ist. Im Gegenteil: Bestandteil einer ordnungsgemäßen Dokumentation ist auch der Initiator solcher Aktionen, vor allem wenn dies massive Eingriffe in die Persönlichkeitsrechte anderer Personen zur Folge hat.

5.9.3.2.2 Datenübermittlung an das Familiengericht

Eine Übermittlung von Sozialdaten ist nach §§ 64 Abs. 2 SGB VIII, 69 Abs. 1 Nr. 2 SGB X zulässig, soweit diese für die Durchführung eines gerichtlichen Verfahrens erforderlich ist.

§ 64 SGB VIII

(1) Sozialdaten dürfen zu dem Zweck übermittelt oder genutzt werden, zu dem sie erhoben worden sind.
(2) Eine Übermittlung für die Erfüllung von Aufgaben nach § 69 des Zehnten Buches ist abweichend von Absatz 1 nur zulässig, soweit dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird.
(2a) Vor einer Übermittlung an eine Fachkraft, die der verantwortlichen Stelle nicht angehört, sind die Sozialdaten zu anonymisieren oder zu pseudonymisieren, soweit die Aufgabenerfüllung dies zulässt.
(3) Sozialdaten dürfen beim Träger der öffentlichen Jugendhilfe zum Zwecke der Planung im Sinne des § 80 gespeichert oder genutzt werden; sie sind unverzüglich zu anonymisieren.

§ 69 Abs. 1 und 2 SGB X

Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist
1. für die Erfüllung der Zwecke, für die sie erhoben worden sind oder für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach diesem Gesetzbuch oder einer solchen Aufgabe des Dritten, an den die Daten übermittelt werden, wenn er eine in § 35 des Ersten Buches genannte Stelle ist,
2. für die Durchführung eines mit der Erfüllung einer Aufgabe nach Nummer 1 zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens oder
3. …

Hält das Jugendamt zur Abwendung einer Gefährdung des Wohls des Kindes oder des Jugendlichen das Tätigwerden des Gerichts für erforderlich, so hat es gemäß § 8a Abs. 3 SGB VIII das Gericht anzurufen.

§ 8a Abs. 3 SGB VIII

Hält das Jugendamt das Tätigwerden des Familiengerichts für erforderlich, so hat es das Gericht anzurufen; dies gilt auch, wenn die Erziehungs- oder Personensorgeberechtigten 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.

Die Übermittlung der im Jugendamt vorhandenen Akte ist demnach zulässig gewesen. Eine "Selektion" der Akte vor deren Abgabe an das Familiengericht durch das Jugendamt war rechtlich nicht geboten. Dem Gericht durften sämtliche Inhalte der Akte bekannt gegeben werden. Die Beurteilung hinsichtlich der Prozessrelevanz bzw. die Entscheidung, ob und wenn ja welche Inhalte den Parteien nicht zur Kenntnis gegeben werden, obliegt ausschließlich dem Gericht bzw. dem Richter. Dabei sollten vom Gericht im Rahmen seines Ermessens schutzwürdige Belange Betroffener berücksichtigt werden.

5.9.3.3 Fazit

Die Übermittlung der Sozialdaten durch Übersendung der Akte des Jugendamts an das Familiengericht war zulässig. Weitere Übermittlungen hat das Jugendamt nicht vorgenommen. Dass das Gericht die gesamte Akte mit dem Namen des Informanten bzw. den Gesprächsaufzeichnungen mit dem Sohn weitergegeben hat, unterlag nicht meiner Bewertung, denn dies war ein Sachverhalt, der in den Bereich der richterlichen Unabhängigkeit fällt. Gerichte unterliegen meiner Kontrolle aber nur, soweit sie nicht in richterlicher Unabhängigkeit tätig werden (§ 24 Abs. 1 Satz 3 HDSG). Dem Datenschutzbeauftragten des Kreises habe ich jedoch den Hinweis gegeben, künftig vor Abgabe derartiger Akten das Gericht auf schutzwürdige Inhalte ausdrücklich aufmerksam zu machen.

5.9.4 Datenschutzbeauftragter bei Trägern der freien Kinder- und Jugendhilfe

Bei Trägern der freien Jugendhilfe ist nach Maßgabe des Bundesdatenschutzgesetzes ein Beauftragter für den Datenschutz zu bestellen.

Ein Träger der freien Jugendhilfe hat mir gegenüber angesprochen, dass mit Blick auf die datenschutzrechtlichen Vorschriften im Kinder- und Jugendhilferecht Unsicherheit besteht, ob ein Datenschutzbeauftragter zu bestellen ist.

Im Gegensatz zu Trägern der öffentlichen Jugendhilfe gehören Träger der freien Jugendhilfe nicht zum staatlichen Bereich (§§ 3, 75 SGB VIII - Kinder- und Jugendhilfe), so dass für sie nicht das HDSG (§ 3 HDSG), sondern grundsätzlich das BDSG maßgebend ist (§ 1 Abs. 2 Nr. 3 BDSG). Insoweit haben Träger der freien Jugendhilfe nach Maßgabe von § 4f BDSG einen Beauftragten für den Datenschutz zu bestellen.

Bei vordergründiger Betrachtung des SGB VIII ist dies allerdings infrage gestellt. Dies liegt daran, dass Träger der öffentlichen mit Trägern der freien Jugendhilfe zusammenarbeiten sollen (§§ 3, 4 SGB VIII) und dass in diesem Fall der öffentlichrechtliche Sozialdatenschutz nicht nur für die Träger der öffentlichen, sondern auch die Träger der freien Jugendhilfe maßgebend ist (§§ 61 Abs. 1 und 3 SGB VIII).

Im Sozialdatenschutzrecht (§§ 67 ff. SGB X) ist auch das Thema Datenschutzbeauftragter bereichsspezifisch geregelt, nichtöffentliche Stellen sind dort allerdings nicht genannt (§ 81 Abs. 4 SGB X).

Daraus nun in einer Art Umkehrschluss abzuleiten, Träger der freien Jugendhilfe seien zur Bestellung eines Datenschutzbeauftragten nicht verpflichtet, wäre allerdings fehlerhaft. Denn dies würde zu dem widersinnigen Ergebnis führen, dass im Bereich der freien Jugendhilfe zwar das im Verhältnis zum allgemeinen Datenschutzrecht (BDSG) strengere Sozialdatenschutzrecht (SGB) maßgebend wäre, diese materiell-rechtliche Verbesserung des Datenschutzes in der freien Jugendhilfe aber durch die Nichtbestellung eines Datenschutzbeauftragten institutionell wieder entwertet würde. Richtigerweise lässt sich die Vorschrift (§ 81 Abs. 4 SGB X) nur so verstehen, dass sie die Bestellung von Datenschutzbeauftragten in der öffentlichen Sozialverwaltung betrifft und dass bei nicht-öffentlichen Stellen insoweit das BDSG anzuwenden ist. Dies hat dann aber gerade zur Konsequenz, dass Träger der freien Jugendhilfe nach Maßgabe von § 4f BDSG einen Datenschutzbeauftragten zu bestellen verpflichtet sind.

Über diese Rechtslage habe ich den anfragenden Träger der freien Jugendhilfe informiert.

5.10 Personalwesen

5.10.1 Personalakteneinsicht durch Innenrevision

Die Innenrevision von Behörden ist berechtigt, Einsicht in Personalakten zu nehmen, soweit dies für die Aufgabenwahrnehmung der Innenrevision erforderlich ist.

Von Behörden bin ich mehrfach auf die Frage angesprochen worden, ob die Innenrevision befugt ist, in Personalakten Einsicht zu nehmen, falls dies zur Abarbeitung des Prüfauftrags notwendig ist.

Die Zulässigkeit, der Innenrevision Personalakten für Prüfzwecke zur Verfügung zu stellen, könnte deshalb bezweifelt werden, weil nach dem Wortlaut des § 107 Abs. 3 HBG, der gemäß § 34 Abs. 1 Satz 2 HDSG auch für Angestellte und Arbeiter gilt, Personalakten für die Innenrevision nicht zugänglich sind.

§ 107 Abs. 3 HBG

Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Allerdings wird die Bedeutung dieser Regelung dadurch relativiert, dass das Personalaktenrecht in erster Linie die Aufgabenwahrnehmung der Personalverwaltung im Blick und im Übrigen keinen abschließenden Charakter hat. Insoweit steht das Personalaktenrecht einer Einsicht durch die Innenrevision nicht von vornherein entgegen. Hinzu kommt, dass die Revisions- und Kontrollaufgabenwahrnehmung datenschutzrechtlich ausdrücklich privilegiert ist. So ist beispielsweise in § 13 HDSG, der das datenschutzrechtliche Gebot der Zweckbindung bei der Weiterverarbeitung personenbezogener Daten normiert, geregelt, dass die Wahrnehmung von Kontrollbefugnissen, zu denen auch Revisionstätigkeiten gehören (vgl. auch Nungesser, HDSG, § 13 Rdnr. 26), mit dem Zweckbindungsgebot vereinbar ist.

§ 13 Abs. 4 HDSG

Personenbezogene Daten, die für andere Zwecke erhoben worden sind, dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen … in dem dafür erforderlichen Umfang verwendet werden.

Aber nicht nur im allgemeinen Datenschutzrecht, sondern auch in bereichsspezifischen Vorschriften wie etwa dem Sozialdatenschutzrecht, das hinsichtlich der Sensibilität der Daten mit dem Personalaktenrecht vergleichbar ist, wird die Vereinbarkeit von Zweckbindung und Revisionstätigkeit ausdrücklich anerkannt (§ 67c Abs. 3 SGB X).

§ 67c Abs. 3 SGB X

Eine Speicherung, Veränderung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle erforderlich ist.

Gesteht man der Innenrevision den Zugang zu Personalakten, soweit dies zur Aufgabenerfüllung erforderlich ist, grundsätzlich zu, so bedeutet dies freilich nicht, dass Personalakteneinsicht schon dann zu gewähren ist, wenn die Innenrevision Informationen aus der Personalakte benötigt. Soweit nämlich eine Auskunft ausreicht, kommt eine Personalaktenvorlage nicht in Betracht (§ 107d Abs. 1 Satz 5 HBG).

§ 107d Abs. 1 Satz 5 HBG

Soweit eine Auskunft ausreicht, ist von einer Vorlage abzusehen.

Ganz in diesem Sinne ist auf Bundesebene vorgesehen, den Zugang der Innenrevision zur Personalakte gesetzlich ausdrücklich klarzustellen, nämlich dass Zugang zur Personalakte die mit Angelegenheiten der Innenrevision beauftragten Beschäftigten haben, soweit sie die zur Durchführung ihrer Aufgaben erforderlichen Erkenntnisse nur auf diesem Weg und nicht durch Auskunft aus der Personalakte gewinnen können (BRDrucks. 615/05, S. 75).

Ich habe mit den anfragenden Dienststellen die Rechtslage wie eben beschrieben erörtert.

5.10.2 Personaldatenverarbeitung von Bewerbern für den pädagogischen Vorbereitungsdienst

Von Bewerbern für den pädagogischen Vorbereitungsdienst dürfen nur die Personaldaten erhoben werden, die für die Einstellungsentscheidung erforderlich sind.

Der Ehemann einer Bewerberin für den pädagogischen Vorbereitungsdienst bat mich um datenschutzrechtliche Prüfung, ob Fragen nach dem Arbeitgeber bzw. der Nichtbeschäftigung des Ehegatten im Zulassungsantrag zum Vorbereitungsdienst für ein Lehramt zulässig sind.

Nach den datenschutzrechtlichen Vorschriften der §§ 107 Abs. 4 HBG, 34 Abs. 1 Satz 2 HDSG dürfen Personaldaten vom Dienstherrn oder Arbeitgeber nur erhoben werden, soweit dies zur Aufgabenwahrnehmung erforderlich ist.

§ 107 Abs. 4 HBG

Der Dienstherr darf personenbezogene Daten über Bewerber, Beamte und ehemalige Beamte nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

Auf meine Nachfrage hin erklärte mir das zuständige Amt für Lehrerbildung, dass die Frage nach der Beschäftigung des Ehepartners bei den gegenwärtig angewandten Kriterien zur Zuerkennung von eventuellen "Härtemerkmalen" keine Bedeutung mehr hat und somit entbehrlich ist.

Nach Abschluss des laufenden Einstellungsverfahrens zum Schuljahresbeginn 2007/08 hat das Amt für Lehrerbildung den Zulassungsantrag zum pädagogischen Vorbereitungsdienst den tatsächlichen Erfordernissen und somit den datenschutzrechtlichen Vorgaben angepasst. Dieser Vorgang zeigt zugleich, dass Datenschutz im dienstlichen Alltag auch zur Verschlankung von Formularen beitragen kann.

Den Eingeber habe ich über diese Entwicklung informiert.

5.10.3 Personaldatenverarbeitung mit SAP R/3 HR

Wiederum war ein Schwerpunkt meiner Tätigkeit die Begleitung der Weiterentwicklung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung. Dabei spielte die Beurteilung von Zugriffsberechtigungen bei der Weiterentwicklung der Auswertungen der Personaldaten und der eingesetzten Verfahren eine zentrale Rolle.

Inzwischen wird die Tendenz deutlich, Zugriffe nicht mehr an Zweckbindung und Erforderlichkeit für die Personaldatenverarbeitung zu binden, sondern die Erforderlichkeit des Zugriffs mit der Ausnutzung der technischen Möglichkeiten zu begründen.

5.10.3.1 Download-Berechtigungen

Schon zu Beginn der SAP-Einführung habe ich gefordert, dass die Vergabe der Download-Berechtigungen restriktiv erfolgen muss.

Mit dieser Berechtigung ist es nämlich möglich, in SAP R/3 HR erstellte Auswertungen mit personenbezogenen Daten auf den jeweiligen Arbeitsplatz-PC herunterzuladen, dort in Excel zu speichern und weiterzuverarbeiten. Es ist auch möglich, mehrere Auswertungen zusammenzuführen und somit außerhalb der sog. "Standardauswertungen" größere Datenbestände

miteinander zu verknüpfen. Eine Kontrolle, ob nur erforderliche und zulässige Auswertungen durchgeführt werden, ist praktisch nicht mehr durchführbar.

Die in SAP R/3 HR hinterlegten Standardauswertungen sind demgegenüber konkret auf die jeweiligen Fragestellungen, die im Rahmen der Sachbearbeitung täglich zu beantworten sind, programmiert.

Jedem Benutzer des Systems werden die auf seine Aufgabenstellungen in der Personalverwaltung passenden Rollen zugeordnet. In diesen Rollen sind auch die Auswertungsmöglichkeiten hinterlegt, die der Nutzer im Rahmen seiner täglichen Arbeit konkret benötigt.
In bestimmten Einzelfällen kann es für Aufgabenstellungen erforderlich sein, Auswertungen zu erstellen, die mit den im Standard zur Verfügung stehenden Auswertungsmöglichkeiten nicht durchgeführt werden können, um ganz spezielle Fragen der jeweiligen Behörde zu beantworten. Dazu benötigen die Verwaltungen im Einzelfall die Download-Berechtigung.

Da dies im Regelfall aber nicht notwendig ist, wurde unter Ziff. 7.4.3 des Zugriffsberechtigungsrahmenkonzepts für das Land Hessen (Version 1.8) ausdrücklich geregelt,

… dass Legitimationsberechtigte und Anwendungsbetreuer (in Verbindung mit der Beantragung der SAP-Rollen) für die USER der betreffenden Behörden die Zuweisung der Download-Berechtigung beantragen müssen.
Um eine unkontrollierte Verarbeitung von vertraulichen Daten des Landes Hessen auf lokalen Arbeitsplatzrechnern einzuschränken, werden diese Rollen restriktiv vergeben.
Vierteljährlich erfolgt eine Überprüfung, ob der einzelne Benutzer die Möglichkeit zum Excel-Download auch tatsächlich nutzt.
Anzumerken ist noch, dass Anwender, die aufgrund anderer Anwendungen neben SAP über eine WTS-up-download-Funktion verfügen, diese auch in SAP nutzen können. Hierüber können aus SAP heraus keine Nachweise oder Statistiken erstellt werden.

Auf eine entsprechende Nachfrage wurde mir mitgeteilt:

Von 5.374 HR-Usern haben 2.718 ein Downloadkonto auf WTS. Von diesen 2.718 sind 1.679 aus SAP R/3 HR heraus berechtigt. Folglich haben 1.039 HR-User ein Downloadkonto auf WTS, sind aber nicht aus SAP R/3 HR heraus berechtigt. Von diesen 1.039 gehören 57 dem HCC/THCC und 445 der HBS an.

Die hohe Anzahl der 445 downloadberechtigten HBS-User entstand aufgrund eines Massentests im Jahr 2006. Derzeit läuft eine Abfrage bei der HBS, wer die Downloadberechtigung noch benötigt.

Es verbleiben 537 HR-User der personalverwaltenden Dienststellen, die ohne aus SAP R/3 HR heraus berechtigt zu sein, ein Downloadkonto auf WTS haben. Somit könnten auch diese User einen Excel-Download von SAP R/3 HR-Berichten durchführen.

Bei dieser hohen Anzahl kann von einer restriktiven Vergabe der Berechtigungen keine Rede mehr sein. Ich habe sofort eine Überprüfung dieser Angelegenheit gefordert.

Zwischenzeitlich wurde mir mitgeteilt, dass 400 Download-Berechtigungen der HBS-User kurzfristig gelöscht wurden.

Die Download-Berechtigungen der übrigen Landesverwaltung werden zurzeit überprüft.

Gerade dieses Beispiel zeigt, dass die einzelnen Verwaltungen alle Möglichkeiten nutzen, die das SAP-System bietet, ohne auf datenschutzrechtliche Belange der Beschäftigten Rücksicht zu nehmen. Es ist davon ausgehen, dass die Personaldaten, die aus dem HR-System heruntergeladen wurden, auf dem Arbeitsplatzrechner dauerhaft gespeichert werden. Damit steigt die Gefahr, dass Subsysteme aufgebaut werden, die nach Beschluss des Kabinetts nicht zulässig sind. Es wurde eindeutig festgelegt, dass das SAP R/3 HR-System das führende Personalverwaltungssystem ist. Die Gefahr, dass die Verwaltungen Personaldaten außerhalb des HR-Systems speichern, mit anderen Daten zusammenführen und im Laufe der Zeit mit veralteten Daten arbeiten, liegt auf der Hand, und dies ist datenschutzrechtlich zu beanstanden.

Ebenso wird deutlich, dass die Festlegungen in den jeweiligen Konzepten, die von mir datenschutzrechtlich begleitet wurden, in der Praxis nicht eingehalten werden.

Ich werde diese Feststellungen zum Anlass nehmen, im nächsten Jahr konkrete Prüfungen auf den Arbeitsplatzrechnern "vor Ort" durchzuführen. Zwischenzeitlich halte ich es für angezeigt, dass die behördlichen Datenschutzbeauftragten, die nach § 5 HDSG von jeder Daten verarbeitenden Dienststelle zu bestellen sind, eine interne Prüfung in dieser Angelegenheit vornehmen.

§ 5 HDSG

(1) Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Bestellt werden dürfen nur Beschäftigte, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt werden. Für die Wahrnehmung seiner Aufgaben nach Abs. 2 muss der behördliche Datenschutzbeauftragte die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Wegen dieser Tätigkeit, bei der er frei von Weisungen ist, darf er nicht benachteiligt werden. Er ist insoweit unmittelbar der Leitung der Daten verarbeitenden Stelle zu unterstellen; in Gemeinden und Gemeindeverbänden kann er auch einem hauptamtlichen Beigeordneten unterstellt werden. Der behördliche

Datenschutzbeauftragte ist im erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen sowie mit den zur Erfüllung seiner Aufgaben notwendigen räumlichen, personellen und sachlichen Mitteln auszustatten. Die Beschäftigten der Daten verarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden.

(2) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen und Hinweise zur Umsetzung zu geben. Zu seinen Aufgaben gehört es insbesondere

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Maßnahmen, die das in § 1 Satz 1 Nr. 1 geschützte Recht betreffen, hinzuwirken,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,

3. die Daten verarbeitende Stelle bei der Umsetzung der nach den §§ 6, 10 und 29 erforderlichen Maßnahmen zu unterstützen,

4. das nach § 6 Abs. 1 zu erstellende Verzeichnis zu führen und für die Einsicht nach § 6 Abs. 2 bereitzuhalten,

5. das Ergebnis der Untersuchung nach § 7 Abs. 6 zu prüfen und im Zweifelsfall den Hessischen Datenschutzbeauftragten zu hören.

Soweit keine gesetzliche Regelung entgegensteht, kann er die zur Erfüllung seiner Aufgaben notwendige Einsicht in Akten und die automatisierte Datenverarbeitung nehmen. Vor einer beabsichtigten Maßnahme nach Satz 2 Nr. 1 ist er rechtzeitig umfassend zu unterrichten und anzuhören. Wird er nicht rechtzeitig an einer Maßnahme beteiligt, ist die Entscheidung über die Maßnahme auszusetzen und die Beteiligung nachzuholen.

(3) Die Daten verarbeitende Stelle kann einen Beschäftigten ihrer Aufsichtsbehörde mit deren Zustimmung zum Beauftragten für den Datenschutz bestellen. Mehrere Daten verarbeitende Stellen können gemeinsam einen ihrer Beschäftigten zum Datenschutzbeauftragten bestellen, wenn dadurch die Erfüllung seiner Aufgabe nicht beeinträchtigt wird. Bestellungen von Personen, die nicht der Daten verarbeitenden Stelle angehören, sind dem Hessischen Datenschutzbeauftragten mitzuteilen.

5.10.3.2 Löschung von Daten im SAP R/3 HR-System

Zum Thema "Löschen von Daten" im SAP-System habe ich mich immer eindeutig geäußert, auf die Vorschriften der §§ 107f HBG, 19 Abs. 3 HDSG und § 34 Abs. 4 HDSG hingewiesen und deren Einhaltung gefordert.

§ 107f HBG

Personalakten sind nach ihrem Abschluss von der personalaktenführenden Behörde fünf Jahre aufzubewahren. Personalakten sind abgeschlossen,
1. wenn der Beamte ohne Versorgungsansprüche aus dem öffentlichen Dienst ausgeschieden ist, mit Ablauf des Jahres der Vollendung des fünfundsechzigsten Lebensjahres, in den Fällen des § 48 dieses Gesetzes und des § 13 des Hessischen Disziplinargesetzes jedoch erst, wenn mögliche Versorgungsempfänger nicht mehr vorhanden sind,
2. wenn der Beamte ohne versorgungsberechtigte Hinterbliebene verstorben ist, mit Ablauf des Todesjahres,
3. Wenn nach dem verstorbenen Beamten versorgungsberechtigte Hinterbliebene vorhanden sind, mit Ablauf des Jahres, in dem die letzte Versorgungsverpflichtung entfallen ist.

(2) Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen sind drei Jahre und über Umzugs- und Reisekosten sechs Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren. Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, sind unverzüglich zurückzugeben oder zu vernichten, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden.

(3) Versorgungsakten sind fünf Jahre nach Ablauf des Jahres, in dem die letzte Versorgungszahlung geleistet worden ist, aufzubewahren; besteht die Möglichkeit eines Wiederauflebens des Anspruchs, sind die Akten dreißig Jahre aufzubewahren.

(4) Die Personalakten werden nach Ablauf der Aufbewahrungsfrist vernichtet, sofern sie nicht vom zuständigen Staatsarchiv übernommen 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 werden dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer auf Grund 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.

§ 34 Abs. 4 HDSG

Im Falle des § 19 Abs. 2 Satz 1 Nr. 2 sind die Daten der Beschäftigten zu löschen. Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Die Löschung von Daten ist im SAP-Standard nicht vorgesehen.

Mir wurde durch die Projektleitung immer wieder versichert, dass die Löschung von Daten bei SAP thematisiert und spätestens drei Jahre nach der erstmaligen Speicherung von Daten (Zeitpunkt, an dem die Aufbewahrungsfrist für die Krankheits- und Urlaubsdaten endet und diese nach § 107f Abs. 2 HBG zu löschen sind) ein entsprechender Löschreport zur Verfügung stehen werde.

Dieser Zeitpunkt ist jetzt erreicht. Seit Einführung des Releases ERP 6.0 am 22. Juni 2007 steht nunmehr ein Standard-Report für die Löschung von Personalnummern und damit für vollständige Löschung von Datensätzen zur Verfügung, dessen Test bisher noch nicht abgeschlossen wurde.

Für das Löschen einzelner Infotypen wurde von SAP ein Beispielreport bereitgestellt, der jedoch die in den Abrechnungsclustern gespeicherten Daten nicht löscht. Somit entstehen im SAP R/3 HR-System Inkonsistenzen, die in Kauf genommen werden müssten. Nach Aussage des HCC ist eine Löschung einzelner Infotypen frühestens nach 36 Monaten möglich, um evtl. erforderliche Rückrechnungen nicht zu gefährden.

Bereits im Jahr 2005 habe ich ein vom Projektbüro des Hessischen Kultusministeriums beim Staatlichen Schulamt in Marburg gefertigtes Konzept für die Löschung von Bewerberdaten in SAP R/3 geprüft und eine Stellungnahme dazu abgegeben. Dieses Konzept sollte umgehend umgesetzt und damit sichergestellt werden, dass Bewerberdaten, die nicht mehr zur Aufgabenerfüllung notwendig sind, gelöscht werden.

Am 30. Oktober d.J. habe ich anlässlich eines Prüfungstermins in Marburg erfahren, dass dies bisher nicht geschehen ist. Mir wurde fest zugesagt, dass die Umsetzung sofort durch das HCC erfolgen soll.

Ich werde die Umsetzung der Löschkonzepte zeitnah und konkret überprüfen. Ein SAP-System, das die Daten, wie gesetzlich vorgeschrieben, nicht rechtzeitig und umfassend löscht, ist datenschutzrechtlich zu beanstanden. Da die Löschung eines der zentralen Datenschutzrechte ist, hätte bereits eine ordnungsgemäß durchgeführte Vorabkontrolle nach § 7 Abs. 6 HDSG das Ergebnis erbringen müssen, dass das Verfahren so nicht eingesetzt werden darf.

5.10.3.3 Konzept "Zentraler Zugriff"

Sowohl in meinem 34. Tätigkeitsbericht als auch im letzten Jahr hatte ich über die Problemstellung des Zugriffs der Ministerien auf die Personaldaten des nachgeordneten Bereichs berichtet.

In § 107 Abs. 3 HBG ist klar geregelt, wer Zugang zu den Personalakten und somit auch zu den im SAP-System gespeicherten Personalaktendaten haben darf.

§ 107 Abs. 3 HBG

Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Ebenso klar regelt der § 107d Abs. 1 HBG, unter welchen Bedingungen der obersten Dienstbehörde die Personalakten vorgelegt werden dürfen, mithin auch ein automatisierter Zugriff auf die im SAP-System gespeicherten personenbezogenen Daten zulässig ist.

Der letzte Satz des Abs. 1 regelt, dass immer dann von einer Vorlage, somit auch von einem vollständigen Zugriff abzusehen ist, wenn eine Auskunft ausreicht.

In Abs. 3 ist geregelt, dass Vorlage und Auskunft auf den jeweils erforderlichen Umfang zu beschränken sind.

§ 107d Abs. 1 und 3 HBG

(1) Ohne Einwilligung des Beamten ist es zulässig, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Das Gleiche gilt für Behörden desselben Geschäftsbereichs, soweit die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist, sowie für Behörden eines anderen Geschäftsbereichs desselben Dienstherrn, soweit diese an einer Personalentscheidung mitzuwirken haben. Ärzten, die im Auftrag der personalverwaltenden Behörde ein medizinisches Gutachten erstellen, darf die Personalakte ebenfalls ohne Einwilligung vorgelegt werden. Für Auskünfte aus der Personalakte gelten Satz 1 bis 3 entsprechend. Soweit eine Auskunft ausreicht, ist von einer Vorlage abzusehen.

(3) Vorlage und Auskunft sind auf den jeweils erforderlichen Umfang zu beschränken.

Meine Rechtsauffassung zu diesem Problem habe ich gegenüber der Landesregierung deutlich dargelegt. Aufgrund meiner Argumentation und durch meine Mitarbeit wurde das sog. "Merkmal Z" ausgeprägt und im SAP R/3 HR-System hinterlegt. Mit diesem Merkmal kann die Berechtigungssteuerung so erfolgen, dass die Ministerien auf die Personaldaten der Beschäftigten des nachgeordneten Bereichs zugreifen können, für die sie nach der Zuständigkeitsverordnung Personal führende Stelle sind.

In ihrer Stellungnahme zu meinem 35. Tätigkeitsbericht hat die Landesregierung zu diesem Thema ausgeführt, dass bei den Dienststellen der Umsetzungsstaffel 06/2006 das "Merkmal Z" bereits im Umsetzungsprozess, d.h., zum frühestmöglichen Zeitpunkt implementiert wurde.

Das Ministerium der Finanzen hat mich über die pilotweise Einführung des "Merkmals Z" bei zwei Finanzämtern informiert. Auf entsprechende Nachfrage wurde mir durch das Ministerium der Finanzen mitgeteilt, dass eine ressortweite Eingabe des "Merkmals Z" nicht erfolgt ist und auch nicht erfolgen soll. Vielmehr wurde mir von Vertretern des Ministeriums der Finanzen ein Diskussionspapier zur Änderung des HBG vorgelegt, zu dem ich eine "erste Einschätzung" abgeben sollte. Geändert werden soll der § 107 HBG. Ziel der Änderung soll sein, dass zukünftig umfassende Zugriffe auf die Personaldaten aller Bediensteten eines Ressorts rechtlich zulässig sein sollen.
Begründet wurde dies mit Argumenten, denen ich nicht folgen kann. In erster Linie wurde vorgetragen, dass man das SAP-System mit allen seinen Möglichkeiten effektiv nutzen wolle. Es wurde wie in fast allen Bereichen, in denen ich Forderungen nach einem möglichst umfassenden Zugriff durch vorgesetzte Dienststellen auf alle Bedienstetendaten des nachgeordneten Bereichs datenschutzrechtlich entgegentreten muss, argumentiert, dass die Ministerverantwortung und eine Verpflichtung zur Qualitätskontrolle dies notwendig machen.

Diese Argumente können mich nicht überzeugen. Der Gesetzgeber hat gerade durch die Regelungen des § 107 ff. HBG und durch die zusätzliche Regelungen des § 34 HDSG die besondere Sensibilität der Personaldaten deutlich gemacht. Nur die Tatsache, dass Personaldaten in einer zentralen Datenbank gespeichert sind und deshalb ein umfassender Zugriff möglich ist, reicht für die Begründung einer Gesetzesänderung nicht aus. Die Gefahr, dass das Recht der Technik angepasst werden soll, wird hier überdeutlich und ist verfassungsrechtlich sehr bedenklich, zumal die Erforderlichkeit für eine so tief in die Persönlichkeitsrechte der Bediensteten eingreifende Änderung des HBG nicht begründet werden kann.

Im Rahmen der Verwaltungsreform ist Verantwortung von oben nach unten übertragen worden. Die Daten der Bediensteten werden auf fast allen Ebenen der hessischen Landesverwaltung permanent qualitätsgeprüft. Die Eingabe der Daten wird natürlich durch den eingebenden Sachbearbeiter vor der Speicherung geprüft. Die zahlungsrelevanten Daten werden durch die Mitarbeiter der HBS geprüft. Es wird bei zahlungsrelevanten Eingaben über eine Schnittstelle eine statistische Kennzahl an das Controlling übermittelt, dort qualitätsgesichert, in das Rechnungswesen eingepflegt und die Personalkosten den jeweiligen Kostenstellen zugeordnet. Die Kostenstellenverantwortlichen prüfen wiederum, ob die verbuchten Kosten des Personals ihre Kostenstelle ordnungsgemäß belasten. Eine weitere Qualitätsprüfung erfolgt mit der Prüfung der Führungsberichte durch die Dienststellenleitungen. Weiterhin werden die den jeweiligen Planstellen zugeordneten Personen noch von den Stellenbewirtschaftern geprüft. Ein weiterer Prüfschritt erfolgt bei der Personalkostenhochrechnung in den Dienststellen, danach auf Buchungskreisebene und, wie zuvor beschrieben, in den Ressorts. Dort kann ich die Notwendigkeit der personenbezogenen Überprüfung der Hochrechnungsdaten allerdings auf keinen Fall erkennen und mittragen.

Die Thematik bezüglich der Notwendigkeit, auf personenbezogene Daten zugreifen zu müssen, um Qualitätssicherung zu betreiben, hat mich z.B. auch bei dem Verfahren zur Pensionsrückstellung beschäftigt.
Auf Grund meiner Argumentation wurde das grundsätzliche Problem der Qualitätssicherung und den damit verbundenen Zugriffen auf personenbezogene Daten durch vorgesetzte Dienststellen in der Gesamtprojektleitung besprochen und dort folgender Beschluss gefasst:

Anlass für das Gespräch war die SAP-Mail des HCC vom 1. November 2007 zur Plausibilitätsprüfung bzgl. der für die Ermittlung der Pensionsückstellungen herangezogenen Daten.

Die Vertreter des Datenschutzbeauftragten räumten ein, dass in einer Übergangs- und qualitätssichernden Phase die bislang in der Verfahrensdokumentation zum 31. Dezember 2006 sowie der anstehenden Dokumentation zum 31. Dezember 2007 vorgesehene Beteiligung der Ressorts mit einer entsprechenden Verprobung erforderlich ist und stattfindet; dies insbesondere vor dem Hintergrund, dass zunächst unterschiedliche Datenquellen (KIDICAP, HR) zu verwenden waren und die Fortentwicklung des Berechnungsprogramms zum 31. Dezember 2007 noch andauert.

Es bestand zugleich Einvernehmen, dass kurzfristig im Rahmen einer sowohl ReWe als auch HR einbeziehenden Bestandsaufnahme der organisatorische Prozess hinsichtlich der Verwendung von personenbezogenen Daten beleuchtet und eindeutige Verantwortlichkeiten zu definieren sind, die eine unnötige Mehrfachprüfung derselben Daten erübrigen.

Die Thematik ist bereits im Rahmen der letzten Rechnungshofprüfungen hinsichtlich der Verprobung der erfolgswirksamen Personalaufwendungen im Rahmen der Bilanzierung der Buchungskreise aufgetreten.

Im Hinblick auf die bereits existente Arbeitsgruppe HR-ReWe-Integration stand die Überlegung im Raum, diese mit entsprechenden Vorarbeiten und hoher Priorität zu beauftragen.

Die Vertreter des Hessischen Datenschutzbeauftragten sind bereits in einer frühen Phase bereit, die entsprechenden Arbeiten zu begleiten sowie soweit erforderlich auch mit Vertretern des Hessischen Rechnungshofs zu erörtern.

Das Ergebnis dieser Untersuchung liegt mir noch nicht vor.

Natürlich muss es möglich sein, dass die Ministerien im Einzelfall im Rahmen der Dienst- und Fachaufsicht auf Daten der Beschäftigten des nachgeordneten Bereichs zugreifen können, wie dies in der Vergangenheit auch der Fall war. Die Frage, ob dies als Begründung für einen allumfassenden und jederzeitigen Vollzugriff ausreicht, wird nach wie vor zwischen den beteiligten Stellen und mir strittig diskutiert.

Ich fordere von der Landesregierung eine klare Aussage, auf welchen Ebenen die Verantwortung für die Qualität der in SAP R/3 HR gespeicherten Personaldaten angesiedelt ist und ab welcher Ebene Auswertungen als ausreichend qualitätsgesichert anzusehen sind. Nur dadurch kann ausgeschlossen werden, dass sich übergeordnete Stellen mit dem Argument, man könne den Daten verarbeiteten Stellen im nachgeordneten Bereich nicht "trauen", entsprechende Zugriffsberechtigung im System eintragen lassen.

5.10.3.4Personalkostenhochrechnung

Schon im letzten Jahr hatte ich über den Zugriff auf Einzelabrechnungsergebnisse im Rahmen der Personalkostenhochrechnung berichtet. Den Personalkostenhochrechnern von vorgesetzten Dienststellen werden nicht nur die "Hochrechnungsdaten" für ihren Zuständigkeitsbereich übermittelt, sondern auch automatisch alle zugrunde liegenden Einzelabrechnungsergebnisse aller Mitarbeiter des nachgeordneten Bereichs zur Verfügung gestellt. Dies hatte ich moniert.

Daraufhin wurde das HCC beauftragt, durch eine Arbeitsgruppe (Team PKPL-Neu) ein neues Fachkonzept für die von SAP neu konzipierte Komponente "Personalkostenplanung (PKPL) im neuen Release ERP 6.0" unter besonderer Berücksichtigung der Datenschutzanforderungen zu erstellen.

Da die Arbeit des "Teams PKPL-Neu" noch nicht beendet ist - zurzeit wird ein Zwischenbericht erstellt -, werde ich mich weiterhin in die dort zu leistende Arbeit einbringen.

Ich war, ebenso wie Vertreter der Ressorts, von Anfang an in die Arbeit der Arbeitsgruppe eingebunden. Die im letzten Tätigkeitsbericht von mir aufgeworfenen Fragen der Erforderlichkeit für den Zugriff auf die Einzelabrechnungsergebnisse des Personals, insbesondere durch die Personalkostenhochrechner der vorgesetzten Dienststellen, wurden auch in diesem Gremium kontrovers diskutiert.

Es gibt in der hessischen Landesverwaltung keine einheitliche Vorgehensweise bei der Personalkostenhochrechnung. So wurde mir von Vertretern einzelner Ressorts ausdrücklich bestätigt, dass sie den Zugriff auf die Einzelabrechnungsergebnisse nicht nutzen und auch nicht benötigen.

Von den Vertretern des Kultusministeriums wurde diese Auffassung ausdrücklich nicht geteilt. Meine im letzten Tätigkeitsbericht aufgeworfenen Fragen zur Erforderlichkeit dieses Zugriffs konnten mir allerdings auch von dort nicht plausibel beantwortet werden. Der Zugriff auf mehr als 50.000 Einzelabrechnungsergebnisse, um - wie behauptet - Fehler bei der Dateneingabe vor Ort herausfiltern zu können, ist nicht nachvollziehbar, weil qualitätssichernde Maßnahmen auf mehreren Ebenen der Verwaltung stattfinden. Die bis zur Erstellung der Personalkostenhochrechnung durchgeführten qualitätssichernden Maßnahmen habe ich unter Ziff. 5.10.3.3 beschrieben.

Auf mein Argument, dass die Verantwortung für die Richtigkeit der Daten bei den jeweils Personal führenden Dienststellen liegt, wurde bisher nicht eingegangen. Immer wieder wurde betont, dass es eine Ministerverantwortung auch für den Einzelfall gäbe und deshalb der Zugriff notwendig sei. Auch meine Hinweise auf die faktische Unmöglichkeit, aus dieser Masse von Einzeldaten Abweichungen bei der Personalkostenhochrechnung analysieren zu können, konnten die Vertreter des Kultusministeriums nicht überzeugen.

Als weitere Begründung für die Zugriffe wurde mir folgender Sachverhalt geschildert:

Dem Land Hessen werden von der Europäischen Union Kosten für eine gewisse Anzahl von Lehrern erstattet, die in EU-Projekten in Hessen eingesetzt werden. Die vom Kultusministerium abzurechnenden Erstattungskosten müssen centgenau berechnet werden und werden direkt im Ministerium aus den über 50.000 Einzelabrechnungsergebnissen ermittelt.

Ich halte dies für nicht zulässig, da für die Berechnung der Bezüge der Bediensteten alleine die Hessische Bezügestelle zuständig ist und diese hierfür die Verantwortung trägt. Auf meine Forderung, die für die Erstattung notwendigen Daten durch die für die Abrechnung zuständige Stelle ermitteln zu lassen, wurde bisher nicht eingegangen.

Um den Anforderungen des Datenschutzes gerecht zu werden, wurden die Ressorts durch das Team PKPL-Neu angeschrieben und um eine entsprechende Stellungnahme gebeten. Der Rücklauf dieser Anfrage wird vom HMDIS zusammen mit den Ressorts und mir ausgewertet. Die Ergebnisse dieser Auswertung sollen gewichtet werden und in das weitere Verfahren einfließen.

Ein genereller Zugriff auf Einzeldaten des nachgeordneten Bereichs ist für den Zweck der Erstellung der Personalkostenhochrechnung nicht erforderlich und somit datenschutzrechtlich nicht zulässig.
Wenn bei der Erstellung der Personalkostenhochrechnung für das gesamte Ressort Klärungsbedarf entsteht, so können diese Fehler - wie in meinem 34. Tätigkeitsbericht beschrieben - nach meiner Überzeugung nur "vor Ort" festgestellt, geklärt und bereinigt werden.

5.10.3.5 Business-Warehouse-HR (HEPISneu)

Die Landesregierung beabsichtigt ein Business-Warehouse-HR zu implementieren, mit dem Führungsberichte und Berichte als Grundlage für strategische Entscheidungen erstellt werden sollen.

Dieses System soll das bisher eingesetzte Verfahren HEPIS ersetzen, mit dem auf der Grundlage des § 120 HBG strategische Berichte erstellt wurden.

§ 120 HBG

Der Minister des Innern kann

1. Grundsätze des Personalwesens entwickeln;

2. Untersuchungen über das Personalwesen anstellen und der Landesregierung und der Landespersonalkommission berichten;

3. Dateien über die Beamten, Angestellten und Arbeiter des Landes sowie die Versorgungsempfänger führen. Die Dateien enthalten persönliche und dienstrechtliche Daten sowie Haushalts- und Organisationsdaten, die für Aufgaben der Nr. 1 und 2 erforderlich sind. Für diese Dateien dürfen die für Besoldungs-, Versorgungs-, Vergütungs- und Lohnzwecke gespeicherten Daten von den zuständigen Stellen an den Minister des Innern übermittelt werden. Die Daten dürfen für Verwaltungs- und Planungszwecke automatisiert verarbeitet werden. Tabellarische Auswertungen dürfen obersten Landesbehörden übermittelt werden, wenn sie zur Erfüllung ihrer Aufgaben erforderlich sind, Namenslisten nur für die Angehörigen ihres Geschäftsbereichs. Die für gesetzlich angeordnete Statistiken erforderlichen Daten dürfen an das Hessische Statistische Landesamt übermittelt werden.

Zurzeit werden in einem Vorprojekt, in dessen Arbeit ich von Anfang an eingebunden war, die Auswertungsanforderungen der Landesverwaltung, die in einem Business-Warehouse-HR erstellt werden sollen, ermittelt und in einem Zwischenbericht zusammengestellt.

Ich habe immer wieder darauf hingewiesen, dass ich es zunächst für notwendig halte, die Aufgaben zu definieren, die mit einem Business-Warehouse-HR erfüllt werden sollen. Ich bin nach wie vor der Auffassung, dass in einem ersten Schritt festgelegt werden muss, welche Arten von Berichten erstellt werden sollen. Nur dann kann definiert werden, ob personenbezogene Daten in einem Business-Warehouse-HR gespeichert, also von SAP R/3 HR über eine Schnittstelle übertragen werden müssen. Nur wenn diese Fakten klar festgelegt sind, können Auswertungsanforderungen durch die Nutzer des Business-Warehouse-HR formuliert werden.

Leider gab es für dieses Vorprojekt keine eindeutigen inhaltlichen Vorgaben. Folglich haben die Ressorts Forderungen formuliert, die Auswertungen verlangen, die personenbezogene Daten bis auf die Ebene der einzelnen Bediensteten beinhalten.

Auch in diesem Fall käme die gleiche Problematik wie beim "Merkmal Z" zum Tragen.

Die besonders zu schützenden Daten der Bediensteten der Polizei, des Landeskriminalamtes und des Landesamtes für Verfassungsschutz wären in einem Business-Warehouse-HR nicht in der gleichen Art und Weise "abgeschottet", wie sie es im SAP R/3 HR-System sind.

Die Ressorts haben an das Vorprojekt ca. 400 Auswertungsanforderungen übermittelt. Diese Anforderungen wurden überarbeitet, teilweise zusammengeführt und mit mir besprochen. Ich habe eine erste Einschätzung abgegeben. Bei einer nicht geringen Anzahl von Auswertungsanforderungen habe ich Bedenken geltend gemacht.

Der zu erstellende Vorbericht wird mit meinen Bedenken der Gesamtprojektleitung zur Entscheidung über das weitere Vorgehen vorgelegt.

Ich werde weiterhin an diesem Projekt beratend mitarbeiten. Dies bedeutet allerdings nicht, dass das Verfahren datenschutzrechtlich unbedenklich entwickelt wird. Eine abschießende Beurteilung ist, wie bei der SAP-Einführung insgesamt, erst zu einem späteren Zeitpunkt möglich.

6. Kommunen

6.1 Ergebnisse der Prüfung von Kommunen

Wie im letzten Jahr habe ich rechtliche und technische Ausprägungen des Einsatzes der Informationstechnik in Kommunen geprüft. Die Erfahrungen haben sich weitgehend bestätigt. Es gab aber auch neue Ergebnisse, die für viele Kommunen von Bedeutung sein können. Die wesentlichen klärungsbedürftigen Sachverhalte sind in einen Katalog, der Fragestellungen und Regelungsbedarf auflistet, und in ein Merkblatt für ehrenamtlich Tätige eingeflossen.

6.1.1 Prüfumfang

Wie im Jahr 2006 habe ich den Status der IT-Sicherheit und den Umfang von Datenverarbeitungen im Auftrag sowie deren vertragliche Regelungen bei hessischen Kommunen geprüft. In diesem Jahr hatte die Mehrzahl der geprüften Kommunen

weniger als 25 Mitarbeiter. Diese Kommunen haben sich für den IT-Betrieb weitgehend auf die Dienstleistung Externer verlassen. Bei den größeren Kommunen gab es in jedem Fall eigenes Personal, für das die Dienstleister eher unterstützend tätig waren.

Auf Basis der Prüfungen habe ich einen Fragenkatalog erarbeitet, der die wesentlichen von mir gefundenen Problemstellungen aufgreift. Da in einem exemplarischen Fall die Einbindung von ehrenamtlich Tätigen nicht korrekt erfolgte, habe ich für diesen Personenkreis ein Merkblatt entworfen, das die zu erfüllenden Anforderungen beschreibt.

6.1.2 Einzelne Feststellungen

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

6.1.2.1 Organisatorische und rechtliche Sachverhalte

6.1.2.1.1 E-Mail und Internet

Ein Dauerbrenner waren Regelungen zur Nutzung von E-Mail und Internet. Hier habe ich bei den meisten Kommunen keine oder unzureichende, d.h. nicht eindeutige, Vorgaben vorgefunden. Gerade die private Nutzung wurde oft ohne schriftliche Regelungen geduldet. Die damit verbundenen Konsequenzen hatte ich bereits dargestellt (vgl. 35. Tätigkeitsbericht, Ziff. 6.1.2.1). Ähnliche Defizite gab es bei allgemeinen Dienstanweisungen zum Umgang mit der IT. Es müssen gerade der Umgang mit Passwörtern, die Nutzung von USB-Geräten - soweit nicht technisch kontrolliert - oder die Installation privater Software geklärt sein.

Insbesondere bei kleineren Kommunen konnte ich feststellen, dass eingehende E-Mails analog normalen Briefen über eine Stelle gehen. Oft ist es das Bürgermeisterbüro. Gegen dieses Konzept habe ich keine Einwände.

In einem Fall musste ich feststellen, dass E-Mails, die sich an ehrenamtlich Tätige richteten, auch an unberechtigte Empfänger resp. E-Mail-Postfächer geschickt wurden. Neben Mitarbeitern der Kommune und ehrenamtlich Tätigen war auch ein Journalist aufgelistet, der nicht zu den berechtigten Empfängern gehörte. Von den E-Mail-Postfächern waren einige nicht den ehrenamtlich Tätigen, den eigentlichen Empfängern, sondern Familienangehörigen zugeordnet. Es gab auch Fälle in denen dienstliche E-Mail-Postfächer aufgelistet waren; beispielsweise bei vertraulichen Unterlagen der Gemeindevertretung zu Grundstücksgeschäften kann aber das E-Mail-Postfach einer Bank auf keinen Fall akzeptiert werden. Ich habe daher gefordert, dass der Versand von Unterlagen per E-Mail an ehrenamtlich Tätige umgehend so zu gestalten ist, dass die rechtlichen Erfordernisse eingehalten werden. Die Anforderungen an die ehrenamtlich Tätigen habe ich in einem Merkblatt zusammengefasst (vgl. Ziff. 6.1.5).

6.1.2.1.2 Umsetzung des HDSG

Selbst klare Anforderungen des HDSG waren nicht immer erfüllt. In einem Fall waren weder ein behördlicher Datenschutzbeauftragter noch ein Vertreter bestellt. Dieser Mangel musste schnell behoben werden.

Die Verträge zur Datenverarbeitung im Auftrag waren auch oft verbesserungswürdig. Sehr häufig fehlte eine Unterwerfungsklausel unter die Kontrolle durch den HDSB, wie sie § 4 HDSG zwingend vorschreibt. In einem Fall fehlte für den Dienstleister, der die gesamte IT betreute, jegliche schriftliche Vereinbarung; es gab folglich keine Übersicht, welche Aufgaben überhaupt vergeben waren.

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

6.1.2.2 Technische Sachverhalte

Immer wieder habe ich viel zu kurze Passwörter vorgefunden. Selbst bei den Administratorkennungen war eine Passwortlänge von fünf Stellen keine Ausnahme. Dies genügt den Anforderungen aus dem Maßnahmenkatalog des BSI nicht.

Bei mehreren Kommunen musste ich feststellen, dass zwar die Benutzerkennungen als Domänenkonten angelegt waren, gleichzeitig waren die Kennungen aber auf ihren Arbeitsstationen als lokale Administratoren eingerichtet. Die Administratorrechte beinhalten umfassende Zugriffsrechte, die dazu führen, dass irrtümlich oder absichtlich
- eine Manipulation/Beschädigung des Betriebssystems möglich wird,
- Dienste und Anwendungen (hier besonders Virenscanner und Firewall) kontrolliert und abgeschaltet werden können,
- Software installiert werden kann.

Dies wurde insbesondere deshalb zum Problem, weil sowohl E-Mail als auch Internet für die Arbeit direkt am Arbeitsplatz eingerichtet waren. Schadcode (E-Mail-Anhänge oder Internetseiten mit Viren, Trojanern u.Ä.) würde daher mit den Administratorrechten des Benutzers ausgeführt. Begründet wurde die Art der Konfiguration damit, dass die Benutzer kaum Hilfestellung durch die Administration benötigen, weil sie fast alle Einstellungen selbst vornehmen können. Das ist zwar einleuchtend, wenn man wenig Rückfragen im täglichen Betrieb erreichen möchte, führt jedoch zu erheblichen Risiken,

wenn beispielsweise mit Trojanern Daten kopiert werden oder die Rechner nicht mehr funktionieren, weil Konfigurationen verändert oder Daten unkontrolliert gelöscht wurden. Ich habe daher empfohlen, die Benutzer nicht als lokale Administratoren einzurichten. Sofern die lokalen Administratorrechte beibehalten werden sollen, sollten zumindest die Anwendungen E-Mail und Internet mit eingeschränkten Rechten ausgeführt werden. Eine der Lösungsmöglichkeiten wäre hierfür das von Microsoft selbst entwickelte "DropMyRights" (http://msdn2.microsoft.com/en-us/library/ms972827.aspx), das die administrativen Rechte des Benutzers für die aufgerufene Anwendung beschränkt.

In einem Fall waren die Server sowie die zentralen Netzwerkkomponenten aufgrund räumlicher Umstände zusammen mit einem Kopierer untergebracht, der allen Mitarbeitern zur Verfügung stand. Alle Mitarbeiter hatten somit Zutritt zu dem Server. Zudem befand sich der Raum direkt neben der Besuchertoilette. Die Zutrittskontrolle nach § 10 Abs. 2 HDSG war nicht erfüllt.

Ein weiterer Schwachpunkt war die Kontrolle der USB-Schnittstellen von Rechnern. Wegen der damit verbundenen Risiken reicht es nicht, mit Dienstanweisungen Nutzungseinschränkungen vorzugeben. Ich halte eine technische Kontrolle für erforderlich (vgl. 32. Tätigkeitsbericht, Ziff. 18.4).

Hinsichtlich der Löschung von Protokolldaten fehlten oft Regelungen. In diesem Zusammenhang habe ich folgende Löschfristen im Grundsatz empfohlen:
- für Protokolle, die der Datensicherheit dienen, sechs Monate
- für Anwendungsprotokolle muss die Löschfrist jeweils fachspezifisch auf die jeweilige Anwendung bezogen festgelegt werden
- Protokolldaten, auf die sich Rechnungen beziehen, sollten gelöscht werden, wenn die Rechnung bezahlt und akzeptiert ist (z.B. bei der Abrechnung nach Plattenzugriffen).

Digitale Kopierer befinden sich mittlerweile bei vielen Kommunen im Einsatz. Da diese Kopierer auf ihrer internen Festplatte die kopierten Dokumente zwischenspeichern, gelten bezüglich der Löschung die gleichen Anforderungen wie an Rechner. Ich habe daher gefordert zu prüfen, ob die Kopien auf der internen Festplatte des Geräts gelöscht bzw. überschrieben werden. Dies kann im Gerät selbst über eine automatisch laufende Softwareroutine geschehen. Ist dies nicht der Fall, müssen die Verträge mit dem Leasingunternehmen sicherstellen, dass die Festplatten des Geräts nach Rücknahme durch das Unternehmen unverzüglich gelöscht werden (vgl. Ziff. 8.2).

6.1.3 Bewertung

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

6.1.4 Katalog zu wichtigen Fragestellungen und Regelungsbedarf

Ausgehend von den bei meinen Prüfungen vorgefundenen Gegebenheiten habe ich die wesentlichen Fragestellungen sowie allgemeine Hinweise zum Regelungsbedarf in dem unten abgedruckten Katalog aufgeführt.

Der Hessische Datenschutzbeauftragte
Regelungen zu Datenschutz und Datensicherung/Datensicherheit
Wichtige Fragestellung und Regelungsbedarf
(Stand 1. Dezember 2007)

Mit diesem Fragenkatalog sollen Themen angesprochen werden, die sich bei Prüfungen und Beratungen immer wieder als klärungsbedürftig gezeigt haben. Nicht alle Fragen müssen zu organisatorischen, technischen oder anderen Maßnahmen und Regelungen führen. Aber ein Verzicht darauf sollte bewusst erfolgen.

1. Konzeptionelle Vorgaben

1.1 Regelungsbedarf

Es gibt eine Reihe von Konzepten, Dienstanweisungen, Regelungen zum IT-Betrieb oder andere Festlegungen wie (Haus-) Standards, die datenschutzrelevant werden können. Die Vorgaben müssen erstellt, verabschiedet und umgesetzt werden.

Wer ist verantwortlich für die Erstellung der konzeptionellen Vorgaben?
Wer ist verantwortlich für die Verabschiedung der konzeptionellen Vorgaben?
Wer ist verantwortlich für die Umsetzung der konzeptionellen Vorgaben?

1.2 Erläuterungen zu IT-Konzepten (Beispiele)

1.2.1 IT-Rahmenkonzept
Das IT-Rahmenkonzept geht auf die Frage ein, "wohin soll die Reise gehen?".
Es geht auch auf Fragen der Finanzierung ein und legt fest, zu welchen Bereichen welche Gremien Entscheidungen vorbereiten, beschließen und umsetzen. Beispiele für Bereiche sind die IT-Architektur, IT-Sicherheit, (Haus-)Standards.

1.2.2 IT-Gesamtkonzept
Das IT-Gesamtkonzept beschreibt den Soll-Zustand der IT aufbauend auf den Ist-Zustand.

1.2.3 Datenschutzkonzepte
Datenschutzkonzepte gibt es insbesondere für die Fachverfahren. Bei der Infrastruktur geht es vorrangig auf die mitarbeiterbezogenen Daten ein, die besonders bei der Protokollierung auftreten; dies gilt speziell für eine Internet-Nutzung. Die Datenschutzkonzepte der Fachverfahren beinhalten meist ein **IT-Sicherheitskonzept** oder werden dadurch ergänzt.

1.2.4 IT-Sicherheitskonzept
Das IT-Sicherheitskonzept sollte die
- Infrastruktur (Netz, Betriebssystem, E-Mail, Internet, …) betreffen und
- Fachverfahren, soweit diese nicht in eigenen Sicherheitskonzepten beschrieben sind, und
- Fachverfahren, die eine übergreifende infrastrukturelle Bedeutung haben (z.B. ein Dokumentenmanagementsystem).

Eine mögliche Vorgehensweise zur Erstellung des Konzepts ist vom BSI beschrieben. In dem Konzept müssen eine Reihe von Festlegungen getroffen werden, die an verschiedenen Stellen greifen. Wichtig ist, dass ein Prozess eingerichtet wird, um die IT-Sicherheit zu gewährleisten. Erfahrungsgemäß gibt es einige Themen, die unbedingt geklärt sein müssen:
- Standardeinstellungen für Passwörter, (Passwortlänge, Komplexität, Historie, Gültigkeitsdauer, …),
- Umgang mit USB-Schnittstellen (blockiert? kontrolliert?),
- Umgang mit anderen drahtlosen Schnittstellen,
- Ist der Einsatz einer Zugriffsschutzsoftware erforderlich?
- Umgang mit Wechseldatenträgern,
- Soll WLAN genutzt werden? Wenn ja, müssen die Standardeinstellungen festgelegt werden?
- Organisatorische Festlegung, wer über den Einsatz welcher Technik/Verfahren entscheidet (ggf. Verweis auf das Rahmenkonzept).

1.2.5 (Haus-)Standards
Die Festlegung von (Haus-)Standards hat zum Ziel, das Zusammenspiel der verschiedenen Komponenten und Programme sicherzustellen. Soweit es Schnittstellen nach außen gibt, beispielsweise die Kommunikation zwischen Meldebehörden, sind bereits oft Standards definiert (XMELD-Datensatz und OSCI als Transportprotokoll) und einzuhalten. Standards für Hardware und Software dienen auch dazu, die Betreuung und Beschaffung zu vereinfachen. Folgende Bereiche bieten sich an, um Festlegungen zu treffen:
- Hardware
- Software
- Datenübermittlung/Kommunikation
- Programmierung
- Dokumentation
- Datensicherung
- Datensicherheit

Im IT-Sicherheitskonzept müssen die wesentlichen Anforderungen festgelegt sein, die dann als "Hausstandard" für die Arbeitsplätze formuliert werden müssen. Wichtige Punkte s.o. 1.2.4.

2. IT-Betrieb

2.1 Festlegung von Zuständigkeiten

Wer ist für welche Teilbereiche des täglichen IT-Betriebs zuständig?
Es wird in aller Regel Personen geben, die bei mehreren der unten aufgeführten Aufgaben eingebunden sind. Meist ergeben sich daraus keine Komplikationen. Bestimmte Interessenskonflikte müssen jedoch in jedem Fall vermieden werden. Dies gilt insbesondere für die Datenschutzkontrolle und damit für den behördlichen Datenschutzbeauftragten.

Falls bei der Festlegung und Durchsetzung von Hausstandards nicht sorgfältig gearbeitet wird, ergeben sich häufig Kompetenzkonflikte. Dürfen beispielsweise Fachabteilungen Software auswählen, ohne vorgegebene Standards zu berücksichtigen, muss anschließend die für den Betrieb zuständige IT-Abteilung Probleme beheben, die sie nicht zu verantworten hat. In den folgenden Punkten geht es überwiegend darum, die konzeptionellen Vorgaben umzusetzen. Teilbereiche des alltäglichen IT-Betriebs sind insbesondere:

2.2 Teilbereiche des IT-Betriebs

2.2.1 Auswahl und Beschaffung von Hardware, Software, Komponenten der Netzinfrastruktur
Bei der Softwareauswahl sind eine Reihe von Anforderungen zu erfüllen. Soweit es den Datenschutz betrifft, muss eine Vorabkontrolle durchgeführt werden (§ 7 Abs. 6 HDSG). Wenn die Entscheidung für ein Verfahren gefallen ist, muss bei der Verarbeitung personenbezogener Daten ein Verfahrensverzeichnis erstellt werden (§ 6 HDSG). Während die fachlichen und rechtlichen Angaben durch das Fachamt beizusteuern sind, beantwortet die IT-Abteilung die technischen Fragestellungen. Der behördliche Datenschutzbeauftragte prüft das Verfahrensverzeichnis und hält es zur Einsicht bereit.

2.2.2 Installationen und Wartung von Hardware, Software, Komponenten der Netzinfrastruktur
Wenn die Aufgabe durch externes Personal durchgeführt wird, handelt es sich eventuell um eine Datenverarbeitung im Auftrag. Dies ist zu prüfen. Wenn ja, so muss ein Vertrag nach § 4 HDSG geschlossen werden.

2.2.3 Betrieb der Informationsverarbeitung und Kommunikationstechnik
In Rechenzentren und großen Verwaltungen mit einer entsprechenden Personalanzahl sollten die Aufgaben Installation und Betrieb personell getrennt sein.

2.2.4 Programmierung
Die meisten Verwaltungen werden keine größeren Anwendungen programmieren. Eine Programmierung wird eher durch einzelne Mitarbeiter auf Basis von Office-Produkten für einzelne Arbeitsplätze erfolgen. Auch diese Anwendungen müssen dokumentiert werden. Werden personenbezogene Daten verarbeitet, ist eine Vorabkontrolle erforderlich.

2.2.5 Test von Software
Eine neue Software ist zu testen. Je nach Umfang der Tests muss eine eigene Projekt-Organisation dafür aufgebaut werden.

2.2.6 Freigabe von Software
Eine Software muss fachlich aber auch technisch freigegeben werden.

2.2.7 Dokumentation von Hardware, Software/Verfahren
In § 6 HDSG werden Verfahrensverzeichnisse gefordert.
Es gibt eventuell noch weitere Vorschriften und Vorgaben, die eine Dokumentation fordern. Für die Hessische Landesverwaltung ist beispielsweise eine interne Dokumentationsrichtlinie für IT-Projekte 2007 erlassen worden.

2.2.8 Datensicherung (Backup)
Je nach Konzept werden Daten zentral oder auch am Arbeitsplatz gesichert. Es muss klar sein, wer für die ordnungsgemäßen Abläufe verantwortlich ist. Wo die Sicherungsmedien gelagert werden bzw. wo sich die Sicherungsgeräte befinden, ist im Sicherheitskonzept zu regeln.

2.2.9 Datensicherheit
Bei der Umsetzung von Datensicherheitsmaßnahmen gibt es oft Konflikte oder Unklarheiten, wer wofür verantwortlich ist.

Dies betrifft beispielsweise die Vergabe von Zugangsrechten zu Räumen, die Vergabe von Benutzerkennungen, die Festlegung von Zugriffsrechten und die Administration der Sicherheitskomponenten insgesamt. Während die Administration zentral erfolgen kann, können Zugriffsrechte in einer Anwendung sinnvollerweise nur von der zuständigen Fachabteilung festgelegt werden; die Zugriffsrechte können dann zentral eingetragen werden.

Es muss klar sein, wer über Zugriffsrechte zu entscheiden hat und wer die Verantwortung dafür trägt, dass die gespeicherten Daten korrekt sind.

2.2.10 Datenschutz
Gerade bei Verträgen mit Dienstleistern, die im Auftrag der Behörde personenbezogene Daten verarbeiten, gibt es oft Defizite weil die Anforderungen von § 4 HDSG nicht oder nur zum Teil erfüllt sind. Wird ein Dritter mit Datenverarbeitungs- oder Wartungsaufgaben betraut, so muss ein Vertrag nach § 4 HDSG abgeschlossen werden. Sofern das HDSG auf den Auftragnehmer keine Anwendung findet, muss sich der Auftragnehmer vertraglich verpflichten, die Bestimmungen des HDSG zu beachten und sich der Kontrolle durch den Hessischen Datenschutzbeauftragten unterwerfen (Musterverträge sind unter www.datenschutz.hessen.de zu finden).

Der behördliche Datenschutzbeauftragte, der die Behördenleitung unterstützt, sollte in die betrieblichen Abläufe eingebunden sein.

2.2.11 Auskunft an Betroffene (§ 18 HDSG)
Die Abläufe bei Auskunftsersuchen sind festzulegen.

3. Elemente einer Dienstanweisung für den Datenschutz

Soweit dem einzelnen Benutzer Vorgaben gemacht werden, sollten sie in Form einer Dienstanweisung zusammengefasst werden. Dabei kann es zweckmäßig sein, zwischen einer Dienstanweisung für Administratoren und einer für "normale" Benutzer zu unterscheiden und auf die jeweils für den Arbeitsbereich typischen Fragen einzugehen.
Mit dem Personalrat abzustimmende Fragestellungen - hier sind die Telearbeit oder die Internetnutzung als Beispiele zu nennen - sind in Dienstvereinbarungen zu regeln.

3.1 Sind die Ziele der Dienstanweisung beschrieben?

3.2 Ist der Geltungsbereich der Dienstanweisung beschrieben?

3.3 Sind die Begriffe, insbesondere die der Datenschutzgesetze, soweit erforderlich, erklärt?

3.4 Sind die allgemeinen Datenschutzmaßnahmen beschrieben?

- Grundlagen
- Verfahrensverzeichnis
- Auskunft
- Benachrichtigung
- Löschung

3.5 Sind die technischen und organisatorischen Datenschutzmaßnahmen beschrieben, die der Benutzer beachten muss?

- Passwortverfahren wie z.B. Passwortlänge ≥ 8 Stellen, komplex, Wechsel alle 30 bis 90 Tage, Historie 13 Generationen, Geheimhaltung, …
- Datensicherung (Wo sind relevante Daten zu speichern? Am Arbeitsplatz mit Sicherung durch den Benutzer oder zentral mit Sicherung durch die IT-Abteilung?)
- Umgang mit Datenträgern wie z.B. Datenträger mit Original-Software, dienstliche USB-Sticks oder Disketten, private Disketten, Kennzeichnung, Aufbewahrung, Weitergabe, Löschung, Verzeichnis, … Es bereitet oft Probleme, die nach dem HDSG geforderte physische Löschung zu gewährleisten. Hierzu sollte es Regelungen oder Lösungen geben (siehe Beitrag 8.2 dieses Tätigkeitsberichtes).
- Maßnahmen zum Schutz vor Viren Einsatz von Virenscannern, Verzicht auf Diskettenlaufwerke, Sperren von USB-Schnittstellen, nur freigegebene Software einsetzen, …
- Behandlung defekter Datenträger
- Verhalten bei Arbeitsunterbrechungen Abschließen der Räume, Abmelden am Rechner, Bildschirmschoner aktivieren, …
- E-Mail bzw. Internetnutzung (s.a. 3.9)

3.6 Was muss bei Änderungen am (PC-)Arbeitsplatz beachtet werden?

Welche Voraussetzungen sind zu beachten?
Wer darf welche Änderungen vornehmen?
- Hardware
- Software
  Bei Eigenprogrammierung muss eine ausreichende Dokumentation gewährleistet sein. Bei Änderungen an der Software muss das Urheberrecht beachtet werden.
- Vernetzung
  Falls Zugänge zu externen Netzen hergestellt werden, z.B. mit Modems, ergeben sich hohe Risiken für die Datensicherheit. Über die Zugänge darf in keinem Fall vom Benutzer eigenständig entschieden werden. Gleiches gilt für den Aufbau von WLANs.

Wer pflegt die Dokumentation (Hardware, Software, Netz), die Verfahrensverzeichnisse und dokumentiert Programmfreigaben?

Ist die Schulung an neuen Geräten/Programmen gewährleistet?

3.7 Dürfen private PCs bzw. private Software zu dienstlichen Zwecken genutzt werden?
(Für Heimarbeitsplätze sind eine eigene Dienstvereinbarung und eine spezielle Dienstanweisung sinnvoll.)

Wenn ja, wie ist zu verfahren?
- Umfang der Nutzung (Lizenzvereinbarungen beachten)
- Antrag
- Genehmigung
- Kontrollbefugnisse
- Rechtsfolgen

3.8 Dürfen dienstliche PCs bzw. dienstliche Software zu privaten Zwecken genutzt werden?

Wenn ja, wie ist zu verfahren?
- Umfang der Nutzung (Lizenzvereinbarungen beachten)
- Antrag
- Genehmigung
- Kontrollbefugnisse
- Rechtsfolgen

3.9 Ist die E-Mail-Nutzung geregelt?

(Die Regelung kann mit der zum Internet zusammengefasst werden; siehe 3.10)
Ist beschrieben, wie mit ein- und ausgehenden E-Mails zu verfahren ist?

Gibt es Festlegungen, unter welchen Bedingungen E-Mail wie zu nutzen ist? (Verschlüsselung, Signatur, Rechtsfolgen, …)

Ist beschrieben, welche Protokolldaten anfallen und unter welchen Bedingungen diese wie ausgewertet werden?

Gibt es funktionsbezogene E-Mail-Adressen und/oder persönliche E-Mail-Adressen?
Zentrale Adressen, je Amt, je Funktion (Personalrat, Datenschutzbeauftragter, …)

Gibt es Vorgaben, wer auf welche Postfächer zugreifen darf?
Hier spielt es eine Rolle, ob funktionsbezogene oder persönliche Postfächer existieren. Auf Grundlage dieser Vorgaben werden Zugriffseinschränkungen vorgenommen.

Wie ist sichergestellt, dass bei (längerer) Abwesenheit auf dienstliche E-Mails zugegriffen werden kann?

Ist eine private Nutzung erlaubt?
Wenn ja, wie ist sichergestellt, dass auf dienstliche E-Mails bei Abwesenheit durch die Dienststelle zugegriffen werden kann? Gibt es eine schriftliche Einwilligung, dass ein Vertreter oder der Administrator bei dienstlichem Erfordernis auch private E-Mails zur Kenntnis nehmen darf?

Wie sind die Abläufe für das Anlegen von Postfächern? Antrag, schriftliche Einwilligung in Einschränkung des Fernmelde-/Briefgeheimnisses, Genehmigung, Kontrollbefugnisse, Rechtsfolgen, …

3.10 Ist die Internet-Nutzung geregelt?

Ist beschrieben, welche Einschränkungen es bei der Internet-Nutzung gibt?
- kein Herunterladen von Software,
- kein Zugriff auf Seiten, die offensichtlich strafrechtsrelevante Inhalte haben,
- Vorgehen, wenn irrtümlich doch ein Zugriff erfolgt ist.

3.11 Sind die Ansprechpartner bei Problemen genannt?

4. Dienstvereinbarung

4.1 Regelungen zur E-Mail- und Internet-Nutzung
Ist beschrieben, für welche Zwecke das Internet zu nutzen ist oder genutzt werden darf?

Ist festgelegt, welche der anfallenden Protokolldaten unter welchen Bedingungen wie ausgewertet werden dürfen?
- Erkennen von Angriffen (Firewall)
- Fehlersuche
- Systemoptimierung
- Gewährleistung der Verfügbarkeit
- Verbot von Leistungs- und Verhaltenskontrollen (§ 13 Abs. 5 und § 34 Abs. 6 HDSG)

Ist festgelegt, wie verfahren wird, wenn der Verdacht besteht, dass ein Mitarbeiter gegen die Dienstanweisung verstoßen hat?
- Information des Personalrats
- Information des behördlichen Datenschutzbeauftragten
- Protokollauswertungen durch die IT-Abteilung unter Hinzuziehung von Personalrat, behördlichem DSB und eventuell anderen Personen (Mehr-Augen-Prinzip)

Ist eine private Nutzung erlaubt?
- Gibt es eine Einwilligungserklärung?
- Ist die Einwilligungserklärung unterzeichnet?

4.2 Einwilligung

Muster einer Kenntnisnahme und Einwilligungserklärung

Durch meine Unterschrift bestätige ich die Kenntnisnahme der beiliegenden Dienstvereinbarung zur E-Mail-, Internet- und Intranet-Nutzung vom …… Die beigefügten, zusätzlichen Richtlinien - (Anmerkung: hier die weiteren relevanten Richtlinien eintragen) - nehme ich zur Kenntnis.

Einwilligung bei privater Nutzung
Wenn Sie (auch weiterhin) den E-Mail-Dienst, das Intranet sowie das Internet in geringfügigem Umfang für private Zwecke nutzen wollen, ist hierfür die Voraussetzung, dass sich die durch diese Dienstvereinbarung festgelegten Zugriffsrechte und Kontrollmechanismen auch auf Daten beziehen, welche infolge privater Benutzung der elektronischen Kommunikationsmittel erzeugt werden. Diese Einwilligung ist freiwillig und kann von Ihnen jederzeit mit Wirkung für die Zukunft widerrufen werden mit der Folge, dass ab dem Widerruf E-Mail, Internet und Intranet nicht mehr privat genutzt werden dürfen. Wenn Sie diese Einwilligung von vornherein nicht abgeben, ist die private Nutzung ebenfalls verboten. Die Einhaltung dieses Verbotes kann kontrolliert werden.

Bitte genau eine Auswahl ankreuzen

☐ Ja, ich möchte E-Mail, Internet und Intranet privat nutzen und willige ein, dass sich die durch diese Dienstvereinbarung festgelegten Zugriffsrechte und Kontrollmechanismen auch auf Daten beziehen, welche infolge meiner privaten Benutzung der elektronischen Kommunikationsmittel erzeugt werden.

☐ Nein, ich erteile die Einwilligung nicht. Ich nehme zur Kenntnis, dass mir ohne diese Einwilligung jegliche private Nutzung untersagt ist.

Vornamen/Nachname
Geburtsdatum
Ort/Datum

Unterschrift

Die unterzeichnete Erklärung ist zu senden an:
(Anmerkung: Hier die *Stelle eintragen, die die Personalakte führt*)
zur Übernahme in die Personalakte

6.1.5 Merkblatt

Auf Grund der Prüfungserfahrungen habe ich für ehrenamtlich Tätige das folgende Merkblatt entwickelt.

Hinweise für ehrenamtlich Tätige in Kommunen

Nach § 24 HGO sind ehrenamtlich Tätige (z.B. ehrenamtliche Magistratsmitglieder, Stadtverordnete oder Mitglieder von Gemeindeversammlungen) zur Verschwiegenheit über Angelegenheiten verpflichtet, die Sie in Ihrer Funktion zur Kenntnis erlangen. Die Verpflichtung gilt nicht nur gegenüber Freunden und Bekannten, sondern natürlich auch gegenüber Familienangehörigen. Der Verstoß gegen die Vorschrift stellt eine Ordnungswidrigkeit gemäß § 24a HGO dar, der mit einer Geldbuße von bis zu eintausend Euro geahndet werden kann. Diese Verpflichtung hat insbesondere Konsequenzen, wenn Sie Unterlagen elektronisch erhalten, sei es mit E-Mail oder durch einen Download aus einem Informationssystem Ihrer Kommune.

1. Auf Ihrem Rechner dürfen keine anderen Personen Zugriffsrechte auf die gespeicherten, mit Ihrer Funktion zusammenhängenden Daten besitzen.

   Ist es Ihr persönlicher Rechner, müssen Sie ihn entsprechend schützen. Der Zutritt muss restriktiv sein, und für die Anmeldung müssen eine Benutzerkennung und ein Passwort verlangt werden. Arbeiten noch andere Personen mit dem Rechner, müssen entsprechende Zugriffsrechte vorhanden sein. Wenn eine andere Person als Administrator den Rechner betreut, darf sie nur in Ihrem Beisein an dem Rechner arbeiten. Für andere Kennungen müssen die Zugriffsrechte so gesetzt sein, dass eine Kenntnisnahme verhindert wird. Weitere Informationen finden Sie unter www.bsi-fuer-buerger.de und auf den Internetseiten von Computerzeitschriften, Datenschutzbeauftragten oder Herstellern.

2. Sie müssen den Rechner mit einem aktuellen Virenscanner und anderen Sicherheitsprogrammen gegen Gefahren aus dem Internet schützen. Weitere Informationen finden Sie beispielsweise unter www.bsi-fuer.buerger.de.

3. Nur Sie dürfen Zugang zu dem Postfach haben, in dem für Sie in Ihrer ehrenamtlichen Funktion die E-Mails ankommen.

   Es darf kein Postfach sein, das andere Personen ebenfalls benutzen, z.B. Familienangehörige. Nur Sie dürfen das Passwort kennen, mit dem auf das Postfach zugegriffen werden kann. Es darf kein Postfach Ihres Arbeitsgebers sein, da der dortige IT-Betreuer oder ein Vertreter von Ihnen im Prinzip Zugriff auf die Daten erhalten könnte.

4. Falls an Sie Daten verschlüsselt übertragen werden, was bei vertraulichen Unterlagen immer der Fall sein muss, dürfen nur Sie das Passwort/den Schlüssel zum Entschlüsseln kennen.

5. Falls Sie die Daten auf einem Wechseldatenträger speichern (USB-Stick, USB-Festplatte, …) dürfen nur Sie Zugriff auf den Datenträger haben. Sie müssen den Datenträger sicher verwahren.

6. Wenn Sie die Daten auf dem Rechner oder einem Datenträger nicht mehr benötigen, löschen Sie sie so, dass sie nicht wiederhergestellt werden können.
   Um eine solche "physische" Datenlöschung zu erreichen, müssen Sie die Daten überschreiben. Hierfür gibt es Hilfsprogramme. Wenn Sie einen Datenträger nicht mehr benötigen, können Sie ihn auch zerstören. Bevor Sie Ihren Rechner verkaufen oder verschenken, löschen Sie unbedingt die Daten; falls Sie Software nicht weitergeben wollen, muss auch diese gelöscht werden.

Sollten Sie noch Fragen haben oder weitere Informationen wünschen, sprechen Sie ihre Kommunalverwaltung direkt an.

6.2 Speicherung von Wahlhelferdaten

Die Gemeinden dürfen die Daten der Mitglieder von Wahlvorständen für künftige Wahlen nur speichern, wenn die Betroffenen der Speicherung nicht widersprochen haben. Auf das Widerspruchsrecht sind die Mitglieder des Wahlvorstandes hinzuweisen. Nicht alle Kommunen kennen und befolgen diese Regel.

In einer Eingabe beschwerte sich ein Bürger darüber, dass er nach der Bundestagswahl jetzt auch für die Landtagswahl zum Mitglied in einen Wahlvorstand berufen worden ist. In keinem Fall habe er sich bei der Gemeinde freiwillig gemeldet. Er wollte deshalb wissen, wie seine Daten in die Wahlhelferdatei gelangt sind und wünschte nähere Auskünfte zu den Berufungsmodalitäten.

Die Nachfrage bei der Stadt ergab Folgendes: Für die Bundestagswahl hatte ihn sein Dienstherr bei der Gemeinde gemeldet. Die Kommune hatte daraufhin seinen Namen in die sog. Wahlhelferdatei aufgenommen. Aus dieser Datei hat sie sich für die Bildung der Wahlvorstände für die kommende Landtagswahl bedient.

Die Benennung durch den Dienstherrn zur Bundestagswahl ist durch § 9 Abs. 5 Bundeswahlgesetz gedeckt.

§ 9 Abs. 5 BWG

Auf Ersuchen der Gemeindebehörden sind zur Sicherstellung der Wahldurchführung die Behörden des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, der Länder, der Gemeinden, der Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts verpflichtet, aus dem Kreis ihrer Bediensteten unter Angabe von Name, Vorname, Geburtsdatum und Anschrift zum Zweck der Berufung als Mitglieder der Wahlvorstände Personen zu benennen, die im Gebiet der ersuchenden Gemeinde wohnen. Die ersuchte Stelle hat den Betroffenen über die übermittelten Daten und den Empfänger zu benachrichtigen.

Ob die erforderliche Benachrichtigung in diesem Fall ordnungsgemäß erfolgt ist, konnte nicht aufgeklärt werden.

Die Gemeinde jedoch hat bei ihrer Aufnahme des Datensatzes in die Wahlhelferdatei für die Landtagswahl im Januar 2008 eine wichtige rechtliche Voraussetzung nicht erfüllt. Zwar sind die Gemeinden sowohl nach dem Landtagswahlgesetz als auch nach dem Kommunalwahlgesetz berechtigt, Daten von Mitgliedern der Wahlvorstände auch für zukünftige Wahlen zu speichern. Dies gilt allerdings nur, wenn die davon betroffenen Personen gegen die weitere Speicherung keinen Widerspruch eingelegt haben. Die Gemeinden sind deshalb verpflichtet, die Mitglieder der Wahlvorstände darauf hinzuweisen, dass sie beabsichtigen, diese Daten für weitere Wahlen zu speichern, wenn der Betroffene dagegen keinen Widerspruch einlegt. Das heißt, sie müssen diesen Personenkreis eindeutig auf dieses bestehende Widerspruchsrecht hinweisen.

§ 15 Abs. 4 LWG

Die Gemeindebehörden sind befugt, personenbezogene Daten von Wahlberechtigten zum Zweck ihrer Berufung zu Mitgliedern von Wahlvorständen zu erheben und zu verarbeiten. Zu diesem Zweck dürfen personenbezogene Daten von Wahlberechtigten, die zur Tätigkeit in Wahlvorständen geeignet sind, auch für künftige Wahlen verarbeitet werden, sofern der Betroffene der Verarbeitung nicht widersprochen hat. Der Betroffene ist über das Widerspruchsrecht zu unterrichten.

An dieser Unterrichtung hat es im vorliegenden Fall gefehlt. Die Überprüfung bei der betroffenen Verwaltung ergab, dass es keinen formularmäßig vorbereiteten Brief an die Wahlhelfer gab, in dem ein Hinweis auf das Widerspruchsrecht enthalten war. Ganz offensichtlich war diese Verpflichtung nicht bekannt. Die Stadt hat zugesichert, das Verfahren umgehend zu ändern.

Eine stichprobenartige Nachfrage bei weiteren hessischen Kommunen ergab, dass die Regelung des § 15 Abs. 4 LWG und § 6 Abs. 4 KWG nur teilweise ordnungsgemäß umgesetzt ist. Aus einigen Kommunen wurde bekannt, dass dort schon seit Jahrzehnten sogenannte Wahlhelferlisten fortgeschrieben werden. Ich habe insoweit die Umsetzung der o.g. Normen gefordert.

6.3 Vereinsförderung durch Kommunen

Die Erforderlichkeit setzt der Erhebung personenbezogener Daten aller Vereinsmitglieder in einer Kommune im Zusammenhang mit Vereinsförderungen Grenzen. Entsprechende Regelungen in den Richtlinien zur Vereinsförderung müssen geändert werden.

Vereine aus verschiedenen Kommunen fragten an, ob es datenschutzrechtlich unbedenklich sei, den Kommunen mit ihren Anträgen auf Vereinsförderung auch eine aktuelle Liste aller Vereinsmitglieder zu übersenden.

Meine Recherchen bei einigen Kommunen ergaben, dass die jeweiligen Richtlinien zur Vereinsförderung vorsehen, dass alle geförderten Vereine jährlich eine Liste mit personenbezogenen Daten aller Vereinsmitglieder zusammen mit dem Förderungsantrag einreichen müssen. Ohne dass ich an der bisherigen ordnungsgemäßen Behandlung der Vereinsmitgliederdaten durch die Kommunen zweifele, gehört es zu meinen Aufgaben als Hessischer Datenschutzbeauftragter, die Speicherung von personenbezogenen Daten auf das erforderliche Maß zu begrenzen. Zur Berechnung der jedem Verein zustehenden Zuschussbeträge ist die generelle Übersendung aktueller Mitgliederlisten nicht erforderlich. Für die Berechnung und Auszahlung von Förderbeträgen genügen Informationen zur Mitgliederzahl, zur Altersstruktur sowie zum Wohnort der Vereinsmitglieder.

Selbstverständlich habe ich keine datenschutzrechtlichen Bedenken, wenn jährlich zur Überprüfung der Richtigkeit der Vereinsangaben einige geförderte Vereine aufgefordert werden, durch Übersendung einer aktuellen Mitgliederliste die Angaben zur Mitgliederstruktur nachzuweisen. Werden die stichprobenartig angeforderten Mitgliederlisten gründlich geprüft und führen fehlerhafte Angaben, z.B. zu einem Ausschluss vom Förderprogramm, kann man sich wirkungsvoll vor falschen Angaben schützen.

Die anfragenden Vereine und die jeweils betroffenen Kommunen habe ich entsprechend informiert.

6.4 Hepatitiswarnung im Einwohnermeldeamt

Die Polizei darf Gesundheitsdaten, die anlässlich einer polizeiärztlichen Untersuchung nach einem Unfall angefallen sind, nicht dem Einwohnermeldeamt übermitteln. Durch klare Anweisungen ist sicherzustellen, dass in ein Freitextfeld des Einwohnermeldedatensatzes nur zulässige Inhalte eingetragen werden.

Ein Einwohner einer hessischen Stadt fragte mich, ob es rechtens sei, dass das Bürgerbüro seiner Stadt über seine Hepatitis-Infektion informiert sei. Zwar habe er vor kurzem der Polizei bei einer polizeiärztlichen Untersuchung gesagt, dass er an Hepatitis-C erkrankt sei, doch habe er nicht damit gerechnet, einige Monate später bei einer Stelle der Stadtverwaltung

dieser Information wieder zu begegnen. Als er einen Reisepass beantragte, habe er auf dem Bildschirm gesehen, dass nach dem Aufrufen des zu seiner Person gespeicherten Einwohnerdatensatzes ein gelb leuchtendes Feld aufblinkte. Darin sei unter Angabe seiner Hepatitis C-Infektion vor ihm gewarnt worden. Er fragte mich, ob er diese Datenspeicherung hinnehmen müsse und ob die vorangegangene Datenübermittlung der Polizei an die Stadtverwaltung rechtmäßig gewesen sei.

Beim Bürgerbüro seiner Stadtverwaltung, welches u.a. die Aufgaben der Einwohnermeldebehörde und der Passstelle wahrnimmt, sah ich den zu seiner Person gespeicherten Einwohnerdatensatz ein. Dort kommt das in Hessen von den Stadt- und Gemeindeverwaltungen oft angewendete DV-Verfahren für das Einwohnerwesen PAMELA (Plattformunabhängiges Melde-, Lohnsteuer- und Ausweiswesen) zur Anwendung. Das Verfahren bietet die Möglichkeit - neben den formatierten und vom Meldegesetz vorgegebenen Datenfeldern - in einem Freitextfeld weitere Informationen zu speichern. Dieses "Sachbearbeiterinfo" genannte Datenfeld wird durch Anklicken eines mit "I" gekennzeichneten Buttons geöffnet. Hat das Datenfeld einen Inhalt, so ist das ansonsten blassblaue "I" leuchtend rot. Im Datensatz der betroffenen Person leuchtete unverkennbar das rote "I". Nach dem Anklicken öffnete sich das leuchtend gelbe Info-Feld. Es enthielt die Angabe: "lt. Auskunft der Polizei, hat Herr XY Hepatitis C! Bitte Vorsicht!".

Der Fall macht in besonderem Maße die Problematik der Verwendung sog. Freitextfelder deutlich. Selbstverständlich hat ein derartiger Hinweis nichts im Einwohnermelde-Datensatz zu suchen. Die Leiterin des Bürgerbüros hat deshalb auch sofort die Löschung dieser Eintragung vorgenommen.

Andere Einwohnermeldeverfahren kommen auch ohne derartige Freitextfelder aus. Datenschutzrechtlich ist die Verwendung solcher Felder stets kritisch, weil - wie der dargestellte Fall zeigt - auch unzulässige Inhalte gespeichert werden können. Wenn man auf die Verwendung von Freitextfeldern nicht verzichten will, ist organisatorisch sicherzustellen, dass sie keine unzulässigen Inhalte enthalten. Aus diesem Grund bedarf es klarer Hinweise an die Mitarbeiter, was in diese Felder eingetragen werden darf. Derartige Hinweise gab es nicht. Ich habe deshalb gefordert, dass ein Leitfaden erstellt wird, aus dem sich für die Mitarbeiter klare Handlungsanweisungen zum Ausfüllen dieser Felder ergeben. Dieser wird derzeit unter Mitarbeit der behördlichen Datenschutzbeauftragten erarbeitet. In einer vorläufigen Anweisung wird darauf hingewiesen, dass die Sachbearbeiter-Info nur für wichtige, dienstliche Belange zu verwenden ist.

Beispiele:
- Örtliche Ermittlung
- Hinweis über einen anderen Wohnsitz oder anderen Familienstand
- Personenstandsurkunde ist nachzureichen
- Fehlende Unterlagen
- Abzuholende oder angeforderte Unterlagen liegen an der Info

Aufgrund dieses Vorfalls habe ich zudem gefordert, dass alle Datensätze mit einer ausgefüllten Sachbearbeiterinfo unter Kontrolle der behördlichen Datenschutzbeauftragten überprüft werden. Bei dieser Auswertung hat sich ergeben, dass noch weitere unzulässige Einträge im Feld Sachbearbeiterinfo vorgenommen wurden. Diese sind inzwischen ebenfalls gelöscht worden.

Danach galt es noch festzustellen, ob die Information auch tatsächlich wie von dem Betroffenen angenommen von der Polizei übermittelt worden war und ob die Datenerhebung bei der Polizei registriert und was genau dort dokumentiert ist.

Die von dem Betroffenen erwähnte polizeiärztliche Untersuchung konnte zeitlich und örtlich genau bestimmt werden. Ich suchte also die zuständige Polizeibehörde auf, bat um Vorlage der Unterlagen zu der in Rede stehenden Unfallaufnahme und sah die in diesem Zusammenhang angefallene Blattsammlung ein. Tatsächlich war die Hepatitis-C-Infektion im ärztlichen Untersuchungsbericht angeführt. Eine Speicherung der Information in den ansonsten zur Person des Betroffenen vorhandenen automatisiert geführten polizeilichen Informationssammlungen lag nicht vor. Auch eine Dokumentation der Übermittlung der Information an die Stadtverwaltung war nicht zu finden. Es blieb mir lediglich festzustellen: Die Information über die Erkrankung ist nach dem Unfallaufnahmebogen an einem späten Freitagabend bei der Polizei registriert und nach dem Protokoll des DV-Verfahrens der Stadtverwaltung am darauffolgenden Montag bei der Meldebehörde eingespeichert worden.

Das zuständige Polizeipräsidium Südosthessen bat ich um eine Stellungnahme zu dem Geschehen. Denn aufgrund des zeitlichen und sachlichen Zusammenhangs bin ich von einer Datenübermittlung der Polizei ausgegangen. Ich fragte, welche Stellen der betreffende Bedienstete noch über die Erkrankung des Betroffenen informiert hat, warum er die Datenübermittlung nicht dokumentiert hat und - falls Fürsorgeüberlegungen sein Handeln bestimmt haben sollten - warum er die Information nicht in den polizeilichen Informationssammlungen hinterlegt hat.

Die Polizei antwortete, der Betroffene habe sich bereits nach seiner Ankunft auf der Polizeistation völlig unangemessen gegenüber den Beamten verhalten. So habe er einen Schreibtisch mit Blut und anderen Körpersekreten benetzt und dabei erwähnt, an Hepatitis C erkrankt zu sein. Die näheren Umstände der Datenübermittlung konnten allerdings nicht geklärt werden. Insbesondere konnte die verantwortliche Person nicht zweifelsfrei ermittelt werden. Die Polizei teilte aber meine Überzeugung, dass sie die Datenübermittlung zu verantworten hat. Als Motiv des unbekannten Polizeibeamten sei anzunehmen, dass er die Mitarbeiter der Stadtverwaltung, die im Rahmen der Überprüfung der Meldedaten mit dem Betroffenen in Kontakt kommen müssten, aufgrund seines Verhaltens auf der Polizeistation zu deren Schutz warnen wollte. Als Rechtsgrundlage hierfür führte die Polizei § 22 Abs. 2 Nr. 2 HSOG an. Danach können Polizeibehörden personenbezogene Daten an Behörden übermitteln, soweit dies zur Abwehr einer Gefahr für die empfangende Stelle erforderlich ist. Zwar sei die Gefahr nicht sonderlich konkret und die Wahrscheinlichkeit des Schadeneintritts eher gering gewesen, doch seien daran umso geringere Anforderungen zu stellen, je größer und folgenschwerer der möglicherweise entstehende Schaden ist. Zwar

sei die für diesen Fall nach § 21 Abs. 1 HSOG gebotene Dokumentation der Datenübermittlung unterblieben. Auch sei der Umgang mit der Information nicht stringent gewesen, weil die polizeiinternen Datenspeicherungen der Polizei nicht um die Warnung angereichert worden ist. Die als Einzelfall bewertete Angelegenheit sei auch intern aufbereitet und entsprechend kommuniziert worden, grundsätzlich könne aber die Datenübermittlung auf § 22 Abs. 2 Nr. 2 HSOG gestützt werden.

Diese Darstellung überzeugt mich im Ergebnis nicht. Weder aus dem Bericht des Arztes noch aus dem des bearbeitenden Polizeibeamten gehen Anhaltspunkte für ein besonderes Vorkommnis oder ein unangemessenes Verhalten hervor. Diesen Unterlagen lässt sich eher das Gegenteil entnehmen. Nachteilig wirkt sich hier die fehlende Dokumentation der Datenübermittlung aus. Der Darstellung, dass es sich um einen Einzelfall gehandelt hat, kann allerdings nicht widersprochen werden. Zu hoffen bleibt, dass mit der internen Aufbereitung und entsprechenden Kommunikation Wiederholungsfällen begegnet ist. Ich habe den Betroffenen darüber informiert, dass die unzulässige Datenspeicherung in der Meldebehörde gelöscht wurde. Ebenso habe ich dargelegt, dass meiner Ansicht nach die Datenübermittlung durch die Polizei unzulässig war.

6.5 Chipkarte als Eintrittskarte und elektronische Geldbörse

Die dauerhafte Speicherung von Konsumationsdaten auf der Zugangskarte zu einem Thermalbad ist datenschutzrechtlich unzulässig. Ich habe deshalb die Neuprogrammierung des Systems gefordert.

Bereits in meinem 33. Tätigkeitsbericht hatte ich über das Zugangssystem zu einem Thermalbad berichtet (Ziff 6.7), bei dem die Dauerkarte als Chiparmband herausgegeben wurde. Dabei hatte ich zum damaligen Zeitpunkt das System nicht beanstandet, da die Speicherung personenbezogener Daten auf dem Chip nur mit Einwilligung der betroffenen Badegäste erfolgte. Es gab auch die Möglichkeit, eine anonyme Dauerkarte in Form eines Chiparmbandes zu erwerben.

Inzwischen gab es erneut Beschwerden über das Zugangssystem. Nicht alle vorgetragenen Vorwürfe erwiesen sich bei der Überprüfung als korrekt. Der anonyme Erwerb einer Dauerkarte war trotz gegenteiliger Behauptung möglich. Allerdings stellte sich bei der Überprüfung heraus, dass die Datenspeicherungen auf der Chipkarte sehr viel umfangreicher waren, als zunächst angenommen. Der besondere Service des Systems ist es, dass Badegäste mit Chipkarte im Schwimmbad kein Bargeld benötigen. Will der Badegast zwischenzeitlich im Schwimmbadrestaurant etwas essen oder trinken oder auch die Sauna besuchen, so kann er diese Leistungen über seinen Chip verbuchen lassen. Diese Informationen werden dann auf dem Server des Betreibers gespeichert. Verlässt der Badegast das Schwimmbad, wird an der Schranke deutlich, ob noch solche Zusatzleistungen abzurechnen sind. Diese Zusatzkonsumationen werden dann an der Kasse des Bades bar oder per EC-Karte beglichen. Das Chipband dient hier nur der Identifikation des Gastes und der Kontrolle der Eintritte.

Man sollte meinen, dass damit für den Badegast der Zahlungsvorgang abgeschlossen ist. Die Überprüfung ergab aber, dass sämtliche Konsumationsvorgänge zu jeder Karte dauerhaft gespeichert werden. Das Schwimmbad konnte auch nach einem Jahr noch genau nachlesen, zu welcher Karte welche Zusatzleistungen abgerechnet wurden. Kein Kunde dürfte davon ausgegangen sein, dass diese Daten nach Verlassen des Schwimmbades weiter gespeichert werden. Die Kundeninformationen erhielten dazu keinerlei Hinweis. Ich halte die Speicherung dieser Daten für datenschutzrechtlich unzulässig, unabhängig davon, ob es sich um eine namensgebundene oder namensungebundene Zugangskarte handelt. Die Abrechnungsdaten für Zusatzkonsumationen sind unmittelbar nach dem Bezahlvorgang durch den Schwimmbadbesucher von den Kartendaten zu trennen. Sicher werden sie noch zu Abrechnungszwecken mit dem Pächter des Lokals benötigt, aber nicht kartenbezogen im System des Thermalbades. Ich habe deshalb gefordert, dass das System umgehend umprogrammiert wird.

Dieser Mangel wiegt noch aus einem weiteren Grund schwer. Die zunächst zur Verfügung stehenden Chipkartenlesegeräte für die Kunden, haben diese Information nicht angezeigt. Der Kunde konnte auch durch das eigene Auslesen die zusätzliche Datenspeicherung gar nicht erkennen. Die Anzeige gab ihm lediglich die Information, wie viele Schwimmbadbesuche noch auf der Karte gespeichert waren.

Wegen technischer Schwierigkeiten liegt das Ergebnis der Umprogrammierung noch nicht vor.

6.6 Zur Nachweispflicht von ledigen Studierenden bei der Begründung eines Nebenwohnsitzes am Studienort

Die Meldebehörde hat für die Richtigkeit des Melderegisters Sorge zu tragen. Sie darf zu diesem Zweck nachprüfen, ob die Zuordnung von Haupt- und Nebenwohnsitz zutreffend ist. Ledige Studierende, die am Studienort einen Nebenwohnsitz begründen und ihren Hauptwohnsitz am entfernten Heimatort beibehalten, sind zur Vorlage von schriftlichen Nachweisen verpflichtet. Diese Nachweispflicht endet jedoch an dem Recht der Meldepflichtigen auf Schutz ihrer Privatsphäre.

Durch zwei Datenschutzbeschwerden wurde ich darauf aufmerksam, dass die Meldebehörde der Universitätsstadt Gießen bei ledigen Studierenden, deren Heimatort mehr als 100 km entfernt ist, überprüft, ob der Status des gemeldeten Nebenwohnsitzes auch tatsächlich zutrifft.

In den Beschwerdefällen forderte die Meldebehörde die Betroffenen auf, detaillierte Angaben zu den Aufenthaltszeiten am Studienort und am Heimatort (zeitliche Gegenüberstellung) zu machen, ihren Studienplan vorzulegen, die Heimfahrten zu belegen und, für den Fall, dass keine eindeutige Aussage getroffen werden kann, bereits vorsorglich eine Angabe zum Lebensmittelpunkt zu machen. Sie kündigte weiterhin an, andernfalls von einer - angeblich durch Rechtsprechung begründeten - Regelvermutung Gebrauch zu machen, nach der bei ledigen Studierenden, deren Heimatort mehr als 100 km vom Studienort entfernt ist, der überwiegende Aufenthalt am Studienort und dieser damit Hauptwohnsitz sei. Das Melderegister sei insoweit von Amts wegen zu berichtigen.

Nach § 16 Abs. 2 HMG ist bei mehreren Wohnungen diejenige die Hauptwohnung, die objektiv häufiger benutzt wird. Bei ledigen Volljährigen ist nach § 16 Abs. 2 Satz 6 im Zweifel der Lebensmittelpunkt maßgeblich.

§ 16 Abs. 2 Satz 1 und 6 HMG

Hauptwohnung ist die überwiegend benutzte Wohnung der Einwohnerin oder des Einwohners. ….

In Zweifelsfällen ist die überwiegend benutzte Wohnung dort, wo der Schwerpunkt der Lebensbeziehungen der Einwohnerin oder des Einwohners liegt. …

Die Meldebehörde darf dies nachprüfen, weil sie für die Richtigkeit des Melderegisters Sorge zu tragen hat und an den Wohnungsstatus unterschiedliche Behördenzuständigkeiten sowie Rechte und Pflichten der Einwohner anknüpfen. Es gibt verschiedene Gerichtsurteile (z.B. BVerwG - 1C 24.90 vom 1. Oktober 1991; HessVGH - 11 UE 4950/88 vom 13. November 1990), die sich mit dem Umfang dieser Nachprüfung beschäftigen. Daraus ergibt sich, dass die Beurteilung in einem Stufenverfahren durchzuführen ist:

- Zunächst ist objektiv der überwiegende zeitliche Aufenthalt an dem Ort festzustellen, an dem sich die Wohnung befindet. Dabei ist eine Einschätzung des künftigen Verhaltens der Betroffenen geboten (Prognoseentscheidung z.B. für das kommende Semesterhalbjahr).

- Bei Studierenden ist eine rein quantitative Berechnung durch Gegenüberstellung der Nutzungszeiten am jeweiligen Ort geboten. Allen Aufenthaltszeiten kommt die gleiche Bedeutung zu. Auf die Qualität der Wohnungen kommt es nicht an.

- Ergeben sich insoweit begründete Zweifel, ist unter Würdigung aller Umstände des konkreten Falles festzustellen, welche der Wohnungen überwiegend benutzt wird. Hierbei ist z.B. auch die Entfernung zwischen beiden Orten zu berücksichtigen, aber auch die Tatsache, dass bei der heutigen allgemeinen Mobilität häufige Heimfahrten auch bei größerer Entfernung durchaus glaubhaft sind.

- Lässt sich dies gleichwohl nicht eindeutig feststellen, liegt ein Zweifelsfall i.S.d. § 16 Abs. 2 Satz 6 HMG vor. Erst dann können die subjektiven Elemente in Betracht gezogen und Betroffene aufgefordert werden, Angaben zum Schwerpunkt ihrer persönlichen Lebensbeziehungen zu machen.

Die Stadt Gießen kann danach zur Klärung der Wohnsitzfrage eine Gegenüberstellung der Nutzungszeiten der beiden Wohnsitze sowie eine Vorlage des Stundenplans verlangen, um die zeitliche Prognose abzugeben. Etwaige persönliche Informationen zum Lebensmittelpunkt, wie z.B. zu Vereinsmitgliedschaften, zu Arztbesuchen, zu gesellschaftlichen, familiären und zwischenmenschlichen Bindungen, dürfen im Einzelfall allerdings erst dann angefordert werden, wenn die objektive Betrachtung unter Einbeziehung aller Umstände zu keiner eindeutigen Entscheidung führt. Eine Aufforderung derartige sensible Daten vorsorglich bekannt zu geben, ist datenschutzrechtlich unzulässig.

Weiterhin gibt es keine gerichtlich begründete Regelvermutung des Inhalts, dass unverheiratete Studierende während ihres Studiums ihre Wohnung vorwiegend am Studienort benutzen. Dieses Argument darf daher auch nicht dazu benutzt werden, um Betroffene zu Auskünften aus ihrer Privatsphäre anzuhalten.

Ich habe die Stadt Gießen darauf hingewiesen, dass die Ermittlungen der Meldebehörden zur Bestimmung der Hauptwohnung ihre Grenzen an dem Recht der Meldepflichtigen auf Schutz ihrer Privatsphäre finden. Die schutzwürdigen Belange von Betroffenen sind gegen das Interesse der Meldebehörde an der Richtigkeit und Fortschreibung des Melderegisters abzuwägen. Die Frage, ob eine Einwohnerin oder ein Einwohner mit Haupt- oder Nebenwohnung in der Gemeinde registriert ist, hat aus Sicht der melderechtlichen Interessenslage der Gemeinde eine untergeordnete Bedeutung. Auswirkungen in andere kommunale Bereiche, bei denen es mittelbar auf die Anzahl der mit Hauptwohnsitz registrierten Einwohner ankommt, wie z.B. beim kommunalen Finanzausgleich oder der Bürgermeisterbesoldung, sind für die Interessensabwägung zulasten der Betroffenen ohne Belang. Die Aufforderung, höchstpersönliche Daten offenzulegen, darf daher nur in der letzten Stufe der Nachforschungen und im Hinblick auf die vorgenannte Interessensabwägung mit Zurückhaltung und Augenmaß erfolgen.

Aus einer weiteren Eingabe habe ich entnommen, dass der Hinweis auf die angebliche Regelvermutung im Anschreiben an die Betroffenen offensichtlich nicht mehr aufgeführt ist. Bezüglich der Aufforderung zur vorsorglichen Bekanntgabe persönlicher Daten zum Lebensmittelpunkt stand eine Reaktion bei Redaktionsschluss noch aus.

7. Sonstige Selbstverwaltungskörperschaften

7.1 Hochschulen

7.1.1 Umfang der Nachweise zu § 6 Abs. 5 Nr. 2 Studienbeitragsgesetz

Eine Befreiung von dem Studienbeitrag hessischer Studierender ist zwar u.a. möglich, wenn er die Pflege eines nahen Angehörigen nachweist. Der Nachweis darf aber nicht dazu führen, dass die Hochschulverwaltung dabei Informationen über Krankheiten und Ähnliches des betroffenen Angehörigen erfährt, es sei denn, dieser hat darin eingewilligt.

Die AOK ließ mir eine Anfrage zukommen, die für alle hessischen Hochschulen Bedeutung hat:
Nach § 6 Abs. 5 Nr. 2 des erstmals im Wintersemester 2007/2008 wirksamen Hessischen Studienbeitragsgesetzes (HStubeiG) muss die Hochschule Studierende, die die Pflege eines nahen Angehörigen nachweisen, auf ihren schriftlichen Antrag von der Beitragspflicht befreien.

§ 6 Abs. 5 Nr. 2 HStubeiG

Die Hochschulen befreien darüber hinaus Studierende von der Beitragspflicht oder ermäßigen die Höhe des Studienbeitrages, wenn die Erhebung des Beitrages aufgrund besonderer Umstände des Einzelfalles eine unbillige Härte darstellen würde. Eine unbillige Härte liegt in der Regel vor bei nachweislicher Pflege eines nach einem Gutachten des Medizinischen Dienstes der Krankenversicherung pflegebedürftigen nahen Angehörigen mit Zuordnung zu einer Pflegestufe nach § 15 Abs. 1 des Elften Buches Sozialgesetzbuch - Soziale Pflegeversicherung - vom 26. Mai 1994 (BGBl. I S. 1014), zuletzt geändert durch Gesetz vom 29. Juni 2006 (BGBl. I S. 1402).

Die AOK legte zur Frage der notwendigen Angaben bezüglich der Pflegesituation ein Antragsformular der Hochschule Darmstadt vor, das als Nachweis eine Bescheinigung des MDK über die Pflegestufe und die Notwendigkeit, Umfang und Häufigkeit der Pflege des Angehörigen verlangte.
Die AOK äußerte dazu aber erhebliche datenschutzrechtliche Bedenken: Damit würden sensible Daten über den betroffenen Angehörigen offenbart, auch könne der MDK nur die Pflegestufe intern bestätigen, die Bescheinigung selbst könne nur die AOK gegenüber dem Antragsteller ausstellen.

Da diese Frage der datenschutzrechtlichen Zulässigkeit des Umfanges des vom Gesetz geforderten Pflege-Nachweises alle hessischen Hochschulen betraf, habe ich zur Klärung und Suche nach praktikablen Lösungen den Arbeitskreis der Datenschutzbeauftragten der hessischen Hochschulen beteiligt.
Rechtlich war dabei der Begriff "nachweisliche Pflege" in § 6 Abs. 5 Nr. 2 Studienbeitragsgesetz zu interpretieren unter Berücksichtigung des allgemeinen Grundsatzes der Erforderlichkeit, wie er - mangels anderweitiger Sondervorschriften - in § 11 Abs. 1 HDSG zum Ausdruck kommt.

§ 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.

Mit der Vorschrift des § 6 Abs. 5 Nr. 2 HStubeiG wollte der Gesetzgeber einen Nachweis vorsehen für die Behauptung des Antragstellers, er pflege einen nahen Angehörigen. Die datenschutzrechtlichen Probleme waren ihm dabei offenbar nicht bewusst. Personenbezogene Gesundheitsdaten gehören nämlich nach § 7 Abs. 4 HDSG zu den sog. sensitiven Daten, deren Verarbeitung nur unter engen Voraussetzungen zugelassen ist.

§ 7 Abs. 4 HDSG

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

Der mir dann übermittelte Vorschlag des erwähnten Arbeitskreises zur Lösung des Problems sah drei Verfahrensarten vor, die ich alle für datenschutzrechtlich konform ansah:

1. Die AOK stellt - nach internem Empfang des MDK-Gutachtens - dem Antragsteller zu dessen Händen eine Bescheinigung aus, die nur den Hinweis auf einen Angehörigen, nicht aber dessen Namen enthält, aber die vom Gesetz verlangte Angabe zur Pflegestufe und den Namen des Antragstellers als der AOK bekannten Pflegeperson. Diese Bescheinigung kann dann der Hochschule zum Verbleib vorgelegt werden, ohne dass genauere Daten über den Angehörigen übermittelt werden.
2. Die AOK bescheinigt dem betroffenen Angehörigen mit dessen Namen, dass er in einer bestimmten Pflegestufe von dem Antragsteller gepflegt wird. Soweit der Angehörige diese Bescheinigung dem Antragsteller zur Vorlage bei der Hochschule übergibt, kann darin seine Einverständniserklärung gesehen werden, die in der Bescheinigung liegenden Informationen zu offenbaren.
3. Der Weg der Einwilligung des Angehörigen in die Offenbarung seiner Daten kann auch beschritten werden, indem er dem Antragsteller das Gutachten des MDK aushändigt und dieser der Hochschule das Gutachten zur direkten Einsicht vorlegt. Die Hochschule darf in diesem Fall lediglich in der Antragakte vermerken, dass die Voraussetzungen des Antrages nachgewiesen wurden. Das Gutachten verbleibt nicht bei der Akte der Hochschule.

Das praktische Problem, dass der Antragsteller eventuell veraltete MDK-Gutachten für diese Antragstellung erneuern oder erstmals veranlassen muss, liegt in seiner Verantwortung.

Den Hochschulen bleibt es überlassen, diese Lösungen in dem entsprechenden Antragsformular zu berücksichtigen.

7.2 Rundfunk

7.2.1 Rechtswidrige Suche nach Schwarzhörern und -sehern

Gebührenbeauftragte des Hessischen Rundfunks dürfen bei der Fahndung nach Schwarzhörern oder -sehern keine Nachbarn befragen.

Im Berichtsjahr musste ich das Verhalten eines Gebührenbeauftragten des HR, der sich unzulässiger Recherchemaßnahmen bedient hatte, förmlich beanstanden.

Eine Bürgerin hatte sich darüber beschwert, dass ein Rundfunkgebührenbeauftragter bei ihren Nachbarn Erkundigungen über sie eingeholt habe. Nach meinen Ermittlungen hatte sich der Beauftragte, nachdem er die Beschwerdeführerin mehrfach nicht in ihrer Wohnung angetroffen hatte, bei Nachbarn nach ihrem Aufenthalt erkundigt und dabei die Auskunft erhalten, dass sie zusätzlich noch eine Wohnung im Nachbarhaus bewohne. Daraufhin warf er in einen Briefkasten, von dem er vermutete, dass er zu der fraglichen Wohnung gehörte, auf dem sich aber kein Namensschild der Betroffenen befand, eine an sie gerichtete Benachrichtigungskarte ein.

Damit hatte der Rundfunkgebührenbeauftragte gleich zweifach gegen das Datenschutzrecht verstoßen: Er hatte rechtswidrig personenbezogene Daten bei privaten Dritten erhoben und rechtswidrig personenbezogene Daten an private Dritte übermittelt.

Der HR bzw. seine Gebührenbeauftragten sind verpflichtet, personenbezogene Daten grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben (§ 12 Abs. 1 Satz 1 HDSG). Der Rundfunkgebührenstaatsvertrag enthält zwar Ausnahmen von diesem Grundsatz. Er gewährt den Landesrundfunkanstalten oder ihren Gebührenbeauftragten jedoch nicht die Befugnis, Informationen über evtl. oder tatsächlich Gebührenpflichtige bei Nachbarn einzuholen. Im Gegenteil: Aus § 4 Abs. 5 Satz 2 RGebStV ergibt sich, dass der Gebührenbeauftragte allenfalls Personen, die in häuslicher Gemeinschaft leben, befragen darf.

§ 12 Abs. 1 Satz 1 HDSG

Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Werden Daten nicht über eine bestimmte Person, sondern über einen bestimmbaren Personenkreis, etwa durch Videoüberwachung, erhoben, dann genügt es, wenn er die seinen schutzwürdigen Belangen angemessene Möglichkeit zur Kenntnisnahme hat.

§ 4 Abs. 5 RGebStV

Die zuständige Landesrundfunkanstalt kann vom Rundfunkteilnehmer oder von Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie ein Rundfunkempfangsgerät zum Empfang bereithalten und dies nicht oder nicht umfassend nach § 3 Abs. 1 und 2 angezeigt haben, Auskunft über diejenigen Tatsachen verlangen, die Grund, Höhe und Zeitraum ihrer Gebührenpflicht betreffen. Die Auskunft kann auch von Personen verlangt werden, die mit den in Satz 1 genannten Personen in häuslicher Gemeinschaft leben. Die Landesrundfunkanstalt kann dabei neben den in § 3 Abs. 2 genannten Daten im Einzelfall weitere Daten erheben, soweit dies nach Satz 1 erforderlich ist; § 3 Abs. 3 Satz 1 gilt entsprechend. Der Anspruch auf Auskunft kann im Verwaltungszwangsverfahren durchgesetzt werden.

Auch das HDSG bietet keine Rechtsgrundlage für eine Befragung der Nachbarn. Es kann dahingestellt bleiben, ob die allgemeinen Erhebungsvorschriften des HDSG neben den Spezialregelungen des RGebStV überhaupt anwendbar sind. Öffentliche Stellen dürfen gemäß § 12 Abs. 3 HDSG bei Dritten außerhalb des öffentlichen Bereichs Daten ohne Kenntnis des Betroffenen nur erheben, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht. Diese Anforderungen können Befragungen von Nachbarn zur Feststellung der Rundfunkgebührenpflicht niemals erfüllen.

§ 12 Abs. 3 HDSG

Beim Betroffenen und bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt.

Wenn der Gebührenbeauftragte tatsächliche Anhaltspunkte hatte, dass die Betroffene ein Rundfunkgerät zum Empfang bereithielt ohne ihre Anzeigepflicht zu erfüllen, wäre eine Melderegisterauskunft nach § 4 Abs. 6 Satz 1 RGebStV in Betracht gekommen. Dann hätte sich herausgestellt, dass die Beschwerdeführerin in der Wohnung im Nachbarhaus nicht gemeldet war. Möglicherweise wäre dadurch der zweite datenschutzrechtliche Verstoß vermieden worden.

§ 4 Abs. 6 Satz 1 RGebStV

Über Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie ein Rundfunkempfangsgerät zum Empfang bereithalten und dies nicht oder nicht umfassend nach § 3 angezeigt haben, dürfen die Landesrundfunkanstalten auch Auskünfte bei den Meldebehörden einholen, soweit dies zur Überwachung der Rundfunkgebührenpflicht erforderlich ist und die Erhebung der Daten beim Betroffenen nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde. Besondere melderechtliche Regelungen des Landesrechts, die eine Übermittlung von Daten an Landesrundfunkanstalten oder die aufgrund des § 8 Abs. 2 Satz 1 von ihnen beauftragte Stelle zulassen, bleiben unberührt.

Der Gebührenbeauftragte hatte nicht nur rechtswidrig personenbezogene Daten erhoben, sondern auch rechtswidrig personenbezogene Daten übermittelt. Er verstieß gegen §§ 11 Abs. 1 und 16 Abs. 1 HDSG.

Durch das Einwerfen einer an die Beschwerdeführerin adressierten Benachrichtigung in einen fremden Briefkasten offenbarte er privaten Dritten, dass die Betroffene keine Rundfunkgeräte angemeldet hatte und der HR deshalb gebührenrechtlich gegen sie ermittelte. Weder auf dem Briefkasten noch auf dem Klingelschild des Nachbarhauses befand sich ihr Name. Sie bestritt, dort zu wohnen und war dort nicht gemeldet. Nach ihren Angaben hatte sie keinen Zugang zu dem Briefkasten. Bei der Benachrichtigung handelte es sich somit um die Übermittlung personenbezogener Daten an Personen außerhalb des öffentlichen Bereichs, nämlich an die Besitzer der Wohnung/des Briefkastens. Diese Datenübermittlung war weder für die Aufgabenerfüllung des Hessischen Rundfunks erforderlich noch hatten die Besitzer des Briefkastens ein berechtigtes Interesse an der Kenntnis des Inhalts der Benachrichtigung. Die Datenübermittlung erfüllte somit weder die Anforderungen des § 11 Abs. 1 noch des § 16 Abs. 1 HDSG für Datenübermittlungen an private Dritte und war daher rechtswidrig.

§ 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 bei einer der beteiligten Stellen vorliegen.

§ 16 Abs. 1 HDSG

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.

Auf meine Beanstandung hin teilte mir der HR mit, dass er den Vorgang zum Anlass genommen habe, die Rundfunkgebührenbeauftragten noch einmal nachdrücklich auf die datenschutzrechtlichen Bestimmungen hinzuweisen. Es sei insbesondere angeordnet worden, Besucherkarten nur so zu verwenden, dass personenbezogene Daten nicht an private Dritte übermittelt werden.

7.3 Handwerksinnung

7.3.1 Handwerksinnung gibt rechtswidrig Einstellungstests von Ausbildungsplatzbewerbern weiter

Handwerksinnungen und Ausbildungsbetriebe dürfen die Ergebnisse von Einstellungstests nur mit schriftlicher Einwilligung des Ausbildungsplatzbewerbers an andere Betriebe weitergeben.

Ein Ausbildungsplatzbewerber beschwerte sich darüber, dass eine Handwerksinnung die Ergebnisse der Einstellungstests von Ausbildungsbetrieben an andere Ausbildungsbetriebe weitergebe. Die daraufhin durchgeführte Überprüfung ergab, dass die Innung regelmäßig die Ergebnisse der Einstellungstests von Ausbildungsbetrieben ohne Einwilligung der Bewerber an andere Ausbildungsbetriebe der Innung übermittelte und damit gegen das Datenschutzrecht verstieß.

7.3.1.1 Verfahren

Die Innung hatte in Kooperation mit Dritten einen Einstellungstest entwickelt, den Mitgliedsbetriebe bei der Geschäftsstelle der Innung anfordern konnten. Der Test blieb ein Jahr lang, d.h. innerhalb einer "Auswahlsaison", die vom 1. Juli bis zum 30. Juni des Folgejahres reichte, inhaltlich unverändert. Der Ausbildungsbetrieb führte den Test durch und schickte im Anschluss daran den ausgefüllten Testbogen an die Innungsgeschäftsstelle. Die Geschäftsstelle veranlasste die Auswertung durch einen beauftragten Lehrer einer Berufsschule. Das Auswertungsergebnis und der überlassene Einstellungstest wurden zusammen mit einer Empfehlung der Innung dem Ausbildungsbetrieb zugeleitet. Eine Kopie des Auswertungsergebnisses verblieb in der Geschäftsstelle der Innung und konnte von anderen Innungsmitgliedern angefordert werden, die das Testergebnis dann in ihrem Auswahlverfahren berücksichtigten und den Ausbildungsplatzbewerber entsprechend informierten.

In ihrer Stellungnahme teilte mir die Handwerksinnung mit, die Ergebnisse der Einstellungstests seien nur weitergeleitet worden, wenn ihr durch Aussage des Ausbildungsbetriebes nachgewiesen worden sei, dass der Ausbildungsplatzbewerber im Bewerbungsgespräch diesem Verfahren zugestimmt habe. Im Beschwerdefall war der Bewerber vom Ausbildungsbetrieb mittels eines Formblattes lediglich gefragt worden, ob er schon einmal an dem Test teilgenommen habe. Die Frage war verbunden mit dem Hinweis, wenn er mit Ja antworte, könne der Ausbildungsbetrieb das Ergebnis bei der Innung anfordern.

7.3.1.2 Verstoß gegen das Datenschutzrecht

Im Laufe des Prüfungsverfahrens ergab sich mit Klärung des Sachverhalts die Notwendigkeit, das RP Darmstadt, das als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich für die Überwachung der Einhaltung der Datenschutzbestimmungen durch die Mitgliedsbetriebe der Innung zuständig ist, einzuschalten. Das RP teilt meine Auffassung, dass das Verfahren rechtswidrig war.

Zu den Aufgaben der Innung gehört zwar die Regelung und Überwachung der Lehrlingsausbildung (§ 54 Abs. 1 Nr. 3 HandwO). Die Durchführung von Einstellungstests der Mitgliedsbetriebe zählt dazu jedoch nicht. Entgegen ihrer Annahme verarbeitete die Innung in diesem Verfahren keine personenbezogenen Daten für sich selbst und war daher keine Daten

verarbeitende Stelle i.S.v. § 2 Abs. 3 HDSG. Sie wurde bei der Auswertung des Einstellungstests datenschutzrechtlich im Auftrag der Ausbildungsbetriebe tätig. Der Lehrer der Berufsschule wertete den Test in einem Unterauftragsverhältnis für die Ausbildungsbetriebe aus. Da die Ausbildungsbetriebe als nicht-öffentliche Stellen nicht dem HDSG unterliegen, galt für das Auftragsdatenverarbeitungsverhältnis zwischen Ausbildungsbetrieb einerseits und Innung sowie Berufsschullehrer andererseits § 11 BDSG. Herr der Daten des Einstellungstests war der Ausbildungsbetrieb, der den Test durchführte. Die Innung und der Lehrer durften die Daten nur im Rahmen der Weisung des Ausbildungsbetriebes verarbeiten.

Ein Ausbildungsbetrieb darf die Ergebnisse von Einstellungstests nur an andere Ausbildungsbetriebe übermitteln, wenn er durch ein Gesetz oder die Einwilligung des Bewerbers dazu ermächtigt ist. Eine besondere Befugnisnorm für die Übermittlung der Testergebnisse ohne Einwilligung der Bewerber existiert nicht. Das BDSG bietet ebenfalls keine Rechtsgrundlage für eine Datenübermittlung ohne Einwilligung der Betroffenen. Die Datenübermittlung erfüllt keinen der Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG. Sie dient weder der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen noch ist sie zur Wahrung berechtigter Interessen des Ausbildungsbetriebes, der den Test durchgeführt hat, erforderlich. Die Voraussetzungen des § 28 Abs. 3 Nr. 1 BDSG sind gleichfalls nicht erfüllt. Die Übermittlung könnte zwar zur Wahrung berechtigter Interessen des anfragenden Ausbildungsbetriebes erforderlich sein, es besteht aber Grund zu der Annahme, dass der Bewerber ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Auch wenn bei der Wiederholung eines Tests Lerneffekte die Verlässlichkeit des zweiten Testergebnisses verfälschen können, ist doch kein Bewerber - sei es ein Ausbildungsplatzbewerber oder ein Arbeitsplatzbewerber - verpflichtet, die Ergebnisse eines gleichen oder ähnlichen Tests aus einer Bewerbung bei einem anderen Arbeitgeber zu offenbaren.

§ 28 Abs. 1 Satz 1 Nr. 1 und 2 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 oder

§ 28 Abs. 3 Nr. 1 BDSG

Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:
1. soweit es zur Wahrung berechtigter Interessen eines Dritten … erforderlich ist … und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, …

Zumindest im Beschwerdefall lag keine ausreichende Einwilligungserklärung für eine Übermittlung der Testergebnisse vor. Eine mutmaßliche Einwilligung, die man hier eventuell hätte annehmen können, kennt das Datenschutzrecht nicht. Die Einwilligung muss ausdrücklich und schriftlich erklärt werden. Der Betroffene muss über den Verarbeitungszweck unterrichtet werden, und die Einwilligung muss auf der freien Entscheidung des Betroffenen beruhen (§ 4a Abs. 1 BDSG). Außerdem muss auf die Freiwilligkeit der Auskunftserteilung hingewiesen werden (§ 4 Abs. 3 Satz 2 BDSG).

Auf ihren Wunsch habe ich die Handwerksinnung bei der Formulierung einer rechtswirksamen Einwilligungserklärung beraten. Zudem habe ich ihr empfohlen, um eine freie Entscheidungssituation zu gewährleisten, die Erklärung nicht, wie vorgesehen, auf dem Testbogen einzuholen. Die Betroffenen sind Jugendliche, die in der Regel im rechtsgeschäftlichen Verkehr unerfahren sein dürften und zudem unter Prüfungsdruck stehen. Eine überlegte und freie Entscheidung kann unter diesen Bedingungen kaum erwartet werden. Ich habe der Innung daher geraten, den Bewerbern den Erklärungsvordruck mit der Einladung zum Einstellungstest zuzusenden. Schließlich habe ich die Innung darauf hingewiesen, dass sie im Auftrag der Ausbildungsbetriebe nur Kopien von Testergebnissen speichern darf, bei denen die Bewerber in die Übermittlung eingewilligt haben.

§ 4a Abs. 1 BDSG

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

§ 4 Abs. 3 Satz 2 BDSG

Werden personenbezogene Daten beim Betroffnen erhoben, so ist er … von der verantwortlichen Stelle … auf die Freiwilligkeit seiner Angaben hinzuweisen.

Angesichts der Kooperationsbereitschaft, welche die Innung zuletzt zeigte, konnte ich in der Sache auf eine datenschutzrechtliche Beanstandung verzichten. Das galt leider nicht für das Prüfungsverfahren. Hier bedurfte es einer förmlichen Beanstandung und der Intervention der Handwerkskammer als Aufsichtsbehörde, um die Innung zu einem datenschutzrechtskonformen Verhalten zu bewegen. Die Handwerksinnung ließ über Monate trotz Mahnung meine Aufforderung zur Stellungnahme unbeantwortet. Ich habe das beispiellose Verhalten der Innung, das einen gravierenden Verstoß gegen die Auskunftspflicht nach § 29 Abs. 1 HDSG darstellte, förmlich beanstandet.

§ 29 Abs. 1 HDSG

Alle Daten verarbeitenden Stellen und ihre Auftragnehmer sind verpflichtet, den HDSB bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere
1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,
2. …

8. Entwicklungen und Empfehlungen im Bereich der Technik

8.1 Einsatz von Signaturen für Verwaltungszwecke

Bei der Prüfung der Gültigkeit von fortgeschrittenen und qualifizierten elektronischen Signaturen gibt es wesentliche Unterschiede. Während die Gültigkeitsprüfung bei qualifizierten Signaturen Auskunft darüber gibt, ob die Signatur zum Zeitpunkt des Signierens des Dokuments gültig war, ist Bezugspunkt der Gültigkeitsprüfung bei fortgeschrittenen Signaturen der Zeitpunkt der Prüfung. Daraus ergeben sich Konsequenzen für den Einsatz von Signaturen in der Verwaltung.
Das zur Erfüllung des RFC-Standards für fortgeschrittene Signaturen erforderliche Key-Back-up der privaten Root- und CA-Schlüssel widerspricht dem Prinzip des Vertrauensankers; eine Änderung der Standards sollte angestrebt werden.

8.1.1 Unterschiede bei der Prüfung elektronischer Signaturen

8.1.1.1 Ablauf der Prüfung einer qualifizierten Signatur

Die Prüfung der qualifizierten Signaturen erfolgt in Deutschland gemäß des Signaturgesetzes (SigG) nach dem Kettenmodell und auf Gültigkeit zum Zeitpunkt der Erstellung (§ 2 Nr. 3a SigG).

§ 2 Nr. 3 SigG

Qualifizierte Signaturen sind elektronische Signaturen nach Nummer 2 (= fortgeschrittene Signaturen), die
a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Jedes Zertifikat trägt die Signatur eines Ausstellenden (§ 7 Abs. 1 SigG).

§ 7 Abs. 1 SigG

Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen: …

Das zur Signatur der ausstellenden Stelle zugehörige Zertifikat (Root-, ZDA-Zertifikat) muss zum Zeitpunkt der Signatur des ausgestellten (in Abb. 1 jeweils darunter dargestellten) Zertifikates gültig sein; nicht aber zu dem Zeitpunkt, in dem letzteres genutzt wird, um weitere Anwender-Zertifikate auszustellen bzw. Dokumente zu signieren. Und schon gar nicht mehr zu dem Zeitpunkt, zu dem eine Signaturprüfung für ein Dokument oder ein Zertifikat erfolgt.

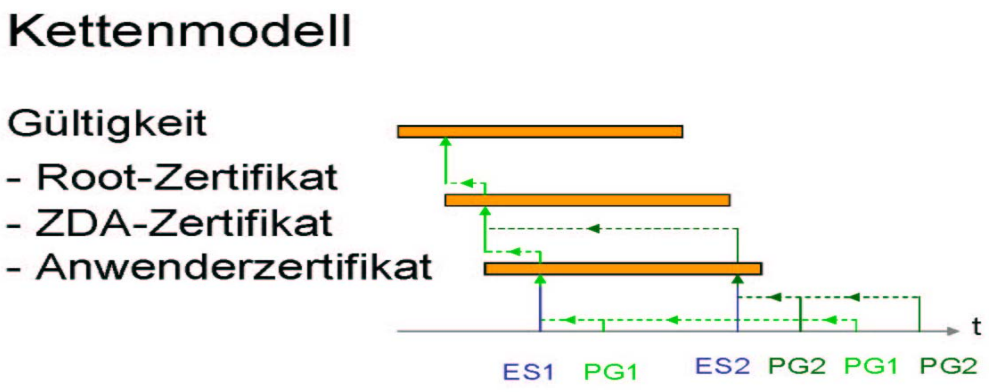

Abb. 1

Der Ablauf der Prüfung nach dem Kettenmodell beginnt von unten (s. Abb. 1):
Die Signatur am Dokument muss auf einem im Zeitpunkt der Erstellung der Signatur gültigen Zertifikat beruhen. In unserem Beispiel ist dies ein Anwender-Zertifikat. Wenn dies der Fall ist, wird die zu diesem Zertifikat gehörige Signatur, also die das Zertifikat ausstellende Signatur des Zertifizierungsdiensteanbieters (ZDA) geprüft. Das zu dieser Signatur gehörige Zertifikat - in der Grafik eine Ebene darüber - muss im Zeitpunkt der Ausstellung des Anwender-Zertifikates gültig gewesen sein.

Wenn dies der Fall ist, wird die zu diesem Zertifikat gehörige, also die das ZDA-Zertifikat ausstellende Signatur geprüft. Das zu dieser Signatur gehörige Root-Zertifikat der Bundesnetzagentur (BNetzA) - in der Grafik eine weitere Ebene darüber - muss im Zeitpunkt der Ausstellung des darunterliegenden ZDA-Zertifikates gültig gewesen sein. Das Zertifikat zu der Signatur, die das Root-Zertifikat ausgestellt hat, wird von der BNetzA veröffentlicht. Damit ist die Prüfung nach dem Kettenmodell beendet. Die "Vertrauenskette", die auf diese Weise technisch überprüft wird, bezieht ihre Vertrauenswürdigkeit aus den Regelungen des SigG für qualifizierte Signaturen, insbesondere den detaillierten Vorschriften für die ZDA.

Der Zeitpunkt des Signierens entspricht - für jegliche Art von Dokumenten und von qualifizierten Zertifikaten - dem des manuellen Unterzeichnens. Eine handschriftliche Unterschrift muss zum Zeitpunkt des Unterzeichnens echt sein, d.h. vom Unterzeichner stammen, und verliert diese Eigenschaft dann nicht mehr. Mit der Prüfung der qualifizierten Signatur nach dem geschilderten Kettenmodell wird dementsprechend die Frage "Ist das Dokument mit einer zum Zeitpunkt des Signierens gültigen Signatur versehen?" zuverlässig beantwortet.

8.1.1.2 Prüfung einer fortgeschrittenen Signatur

Demgegenüber erfolgt die Prüfung fortgeschrittener Signaturen gemäß den RFC-Standards für elektronische Signaturen (RFC = "Request for Comments") nach dem Schalenmodell und auf Gültigkeit zum Zeitpunkt der Prüfung. Die Hessen-PKI, die derzeit unter der Verwaltungs-PKI des Bundes aufgebaut wird, legt diese Standards ebenso wie die Verwaltungs-PKI selbst, in ihren jeweiligen Sicherheitskonzepten (Policies) und bei der Realisierung der Infrastruktur zugrunde. Dies entspricht der Empfehlung in der Anlage IV der EU-Signaturrichtlinie.

Anlage 4 EU-Signaturrichtlinie

Während des Signaturprüfungsvorgangs ist mit hinreichender Sicherheit zu gewährleisten, dass die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats zuverlässig überprüft werden,
… .

8.1.1.2.1 Ablauf der Prüfung nach dem Schalenmodell

Die Prüfung nach dem Schalenmodell bedeutet, dass zum Zeitpunkt der Prüfung die Gültigkeit des Anwenderzertifikates, die Gültigkeit des CA- und Sub-CA-Zertifikates und die Gültigkeit des Root-Zertifikates geprüft wird. Alle an der Ausstellung beteiligten (Root-, CA- und Sub-CA-)Zertifikate müssen zum Zeitpunkt der Prüfung gültig sein (s. Abb. 2a).

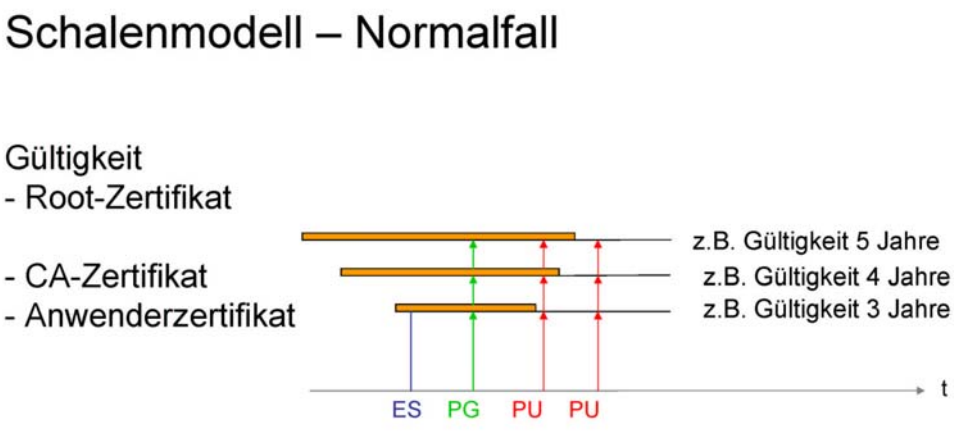

Abb. 2a

Das bedeutet, dass alle Prüfungen zum Ergebnis "ungültig" führen, die in einem Zeitpunkt erfolgen, in dem eines der Zertifikate nicht mehr gültig ist. Das kann - wie in Abb. 2a gezeigt - sein, wenn das Anwenderzertifikat seine Gültigkeit verloren hat oder auch - wie in Abb. 2b gezeigt - eines der darüberliegenden Zertifikate nicht mehr gültig ist. Dabei spielt es keine Rolle, dass jedes Zertifikat im Zeitpunkt des Signierens des jeweils direkt darunterliegenden Zertifikats bzw. Dokumentes gültig war und dass eines der Zertifikate erst später seine Gültigkeit verloren hat.

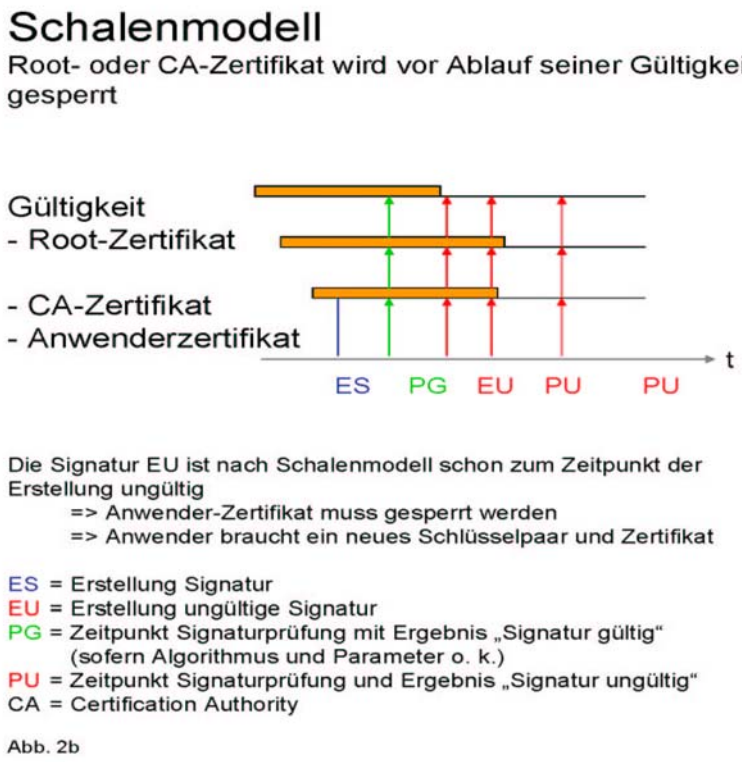

Abb. 2b

Beim Einsatz der fortgeschrittenen Signatur müssen folglich direkt mit dem Zeitpunkt der Ungültigkeit eines Zertifikats konsequenterweise alle darunterliegenden Zertifikate gesperrt und für alle diese Nutzer neue ausgestellt werden - was sehr teuer und aufwändig ist -, um das Erstellen einer von vornherein ungültigen Signatur zu vermeiden. Selbst dies löst aber nicht das Problem, dass ein mit einer seinerzeit gültigen Signatur versehenes Dokument bei der Gültigkeitsprüfung der Signatur fortan das Ergebnis "ungültig" erbringt.

8.1.1.2.2 Ungültigkeit eines Zertifikates und Anforderungen an die Signaturprüfsoftware

Abgelaufene Zertifikate werden nicht gesperrt, weil im RFC-Standard der Ablauf nicht als Sperrgrund aufgeführt ist. Sie sind aber selbstverständlich nicht mehr gültig. Eine Abfrage von Sperrlisten oder eine Abfrage beim OCSP (Online Certificate Status Protocol) bringt aber für abgelaufene Zertifikate als Ergebnis, dass das Zertifikat nicht gesperrt und damit gültig ist. Das bedeutet, dass die Signaturprüfsoftware zuerst selbst prüfen muss, ob - zum Zeitpunkt der Prüfung - eines der beteiligten Zertifikate abgelaufen ist. Damit ist dann die Signatur ungültig und eine Abfrage von Sperrlisten erübrigt sich. Geht die Prüfsoftware nicht diesen Weg, wird sie bei abgelaufenen Zertifikaten fälschlicherweise das Ergebnis "gültig" bringen.

8.1.1.2.3 Folgerungen für den Einsatz fortgeschrittener Signaturen

Der Einsatz einer fortgeschrittenen Signatur für eine reine Transportsicherung bezüglich Authentizität und Integrität bei E-Mails, bei der die Signatur direkt nach dem Kommunikationsvorgang geprüft werden sollte, also in unmittelbarer zeitlicher Folge des Erstellens der Signatur, ist akzeptabel. Weniger problematisch mag dies auch für Transaktionen (z.B. bei Banktransaktionen, die eine Widerspruchsfrist von sechs Wochen haben) sowie für Zutritts- und Zugangskontrollen sein.

Für Dokumente, wie sie auch in der Verwaltung fast ausschließlich zu finden sind, und für E-Mails, soweit es nicht um die reine Transportsicherung geht, ist dagegen der Zeitpunkt der Prüfung unwichtig; es kommt vielmehr ausschließlich auf den Zeitpunkt des Signierens des Dokuments an. Dementsprechend ist die Erwartungshaltung bei der Signaturprüfung von Dokumenten die Antwort auf die Frage: "Ist das Dokument mit einer zum Zeitpunkt des Signierens gültigen Signatur versehen?" Auch bei der handschriftlichen Unterschrift muss diese im Zeitpunkt des Unterzeichnens echt sein, d.h. von dem Unterzeichner stammen. Manuell unterschriebene Dokumente haben kein Verfallsdatum; wenn die Unterschrift echt ist, gilt sie ab dem Augenblick der Unterzeichnung unbefristet.

Aufgrund des für fortgeschrittene Signaturen festgelegten Prüfzeitpunkts und des verwendeten Schalenmodells kann die Signaturprüfung aber keine zuverlässige Antwort auf die Frage der Gültigkeit zum Zeitpunkt des Signierens geben. Das führt in vielen Fällen, nicht nur nach Ablauf der Gültigkeit des Anwender-Zertifikates, sondern ggf. schon vorher bei Ab-

lauf oder Ungültigkeit eines der darüberliegenden Zertifikate - im Hinblick auf die angenommene andere Fragestellung - zu nicht erwarteten bzw. zu sachlich falschen Ergebnissen.

Dies ist den Nutzenden nicht zu vermitteln. Es ist zu befürchten, dass sie dann entweder gar keine Signaturprüfung mehr vornehmen oder das Ergebnis ignorieren.

8.1.1.3 Konsequenzen für den Einsatz von Signaturen in der Verwaltung

Vor der Beschaffung von Signaturkarten und Signaturanwendungskomponenten sind noch eine Reihe von Fragen zu klären:

Es muss überlegt werden, **ob** überhaupt und ggf. wofür **fortgeschrittene Signaturen** in der Verwaltung sinnvoll eingesetzt werden können. Dabei sind rechtliche Fragen des Beweiswertes einer solchen Signatur ebenso wie die obigen Ausführungen zu berücksichtigen. Aus meiner Sicht scheidet jedenfalls die "Unterzeichnung" elektronischer Dokumente als Anwendungsfall aus.

Bei der Beschaffung bzw. beim Einsatz von **Signaturprüfsoftware** für die Prüfung eingehender, mit elektronischer Signatur versehener Dokumente ist darauf zu achten, dass diese Prüfsoftware fortgeschrittene und qualifizierte Signaturen nach dem jeweils zutreffenden Modell prüft. Sie muss zu Beginn der Prüfung klären, um welche Art Signatur es sich handelt, insbesondere, ob nach dem Schalen- oder dem Kettenmodell geprüft werden muss. Andernfalls führt die Prüfung zu einem falschen Ergebnis. An allen Arbeitsplätzen zur Prüfung von Signaturen darf nur Prüfsoftware eingesetzt werden, die sowohl fortgeschrittene als auch qualifizierte Signaturen zutreffend prüft.

Es wird ferner die Frage der Behandlung von signierten Dokumenten und insbesondere die des **Übersignierens** zu klären sein:
Wird mit einem qualifizierten Zeitstempel übersigniert und zu welchem Zeitpunkt ist eine Übersignatur von Dokumenten vorgesehen? Wie erfolgt die Auswahl der mit der Übersignatur zu versehenden Dokumente? Ist sie automatisiert möglich? Ausgehend von dem Ergebnis der Frage nach dem Beweiswert fortgeschrittener Signaturen und dem Ansatz der dortigen Signaturprüfung ist zu überlegen, ob die Übersignatur fortgeschritten signierter Dokumente sinnvoll ist bzw. erfolgen muss. Jedenfalls kann der Beweiswert der ursprünglichen Signatur und deren Rechtswirkung für das Dokument durch eine Übersignatur mit einem qualifizierten Zertifikat nicht erhöht werden.

Insgesamt wird sich auch die Frage stellen, ob - angesichts der unterschiedlichen Anwendungsfelder beider Signaturarten und der Tatsache, dass nur qualifizierte Signaturen das Schriftformerfordernis erfüllen - nicht von vornherein **durchgängig qualifizierte, akkreditierte Signaturen** eingesetzt werden sollten. Diese müssen erst mehr als 33 Jahre nach dem ersten Einsatz, bzw. unbesehen alle beim Schwachwerden des technischen Verfahrens (Algorithmus, Parameter etc.) übersigniert werden.

Das HMDIS sollte mit Unterstützung der Stabsstelle Hessen-PKI die Ressorts vor Aufnahme des Echtbetriebs Hessen-PKI **umfassend informieren** über die Unterschiede nicht nur zwischen den Signaturarten, sondern vor allem über die Unterschiede bezüglich ihrer Gültigkeit, ihrer Prüfung und auch ihrer Rechtswirkung. Nur so können die Ressorts für ihren Bereich die Weichen bezüglich der elektronischen Signatur richtigstellen.

Angesichts des breiteren und für die Verwaltung einschlägigen Einsatzgebietes qualifizierter Signaturen sollte überlegt werden, ob vom Einsatz der fortgeschrittenen Signatur Abstand genommen wird und die eingesparten Kosten nicht besser für die Beschaffung qualifizierter Signaturen eingesetzt werden sollten. Unter dem Gesichtspunkt des breiteren Einsatzfeldes dieser Signaturform sollte auch ein günstigerer Preis für die erforderlichen Signaturerstellungseinheiten bzw. qualifizierten Zertifikate erzielbar sein.

8.1.2 Key-Back-up von privaten Root- und CA-Schlüsseln für fortgeschrittene Signaturen

In den RFC-Standards, die für fortgeschrittene Signaturen genutzt werden, ist festgelegt, dass die Sperrlisten - also die Listen der gesperrten, nicht mehr gültigen Zertifikate - jeweils mit dem Schlüssel signiert sein müssen, mit dem diese Zertifikate ursprünglich ausgestellt wurden. Das ist aber nur möglich, wenn die Schlüssel aufbewahrt werden, um sie für die Sperrung der Zertifikate vorzuhalten. Dieses Key-Back-up der privaten Signaturschlüssel auf der Root-, CA- und Sub-CA-Ebene führt allerdings zu Problemen mit der Erfüllung der Anforderungen des Signaturgesetzes, das - zu Recht - hohe Sicherheitsanforderungen setzt. Nach § 2 Nr. 2c SigG müssen fortgeschrittene Signaturen "mit Mitteln erzeugt werden, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle halten kann". Dem widerspricht die Hinterlegung oder Zweitausfertigung privater Signaturschlüssel. Diese Anforderung muss auch für die Root-, CA- und Sub-CA-Zertifikate gelten, weil sonst die "Verankerung" der Anwenderzertifikate nicht vertrauenswürdig ist. Ohne einen solchen Vertrauensanker ist aber das gesamte System nicht vertrauenswürdig und weist nicht die erforderliche Sicherheit auf.

Deshalb sollte mittelfristig eine Änderung der Policies und ggf. der zugrunde liegenden RFC-Standards angestrebt werden.

Damit werden keineswegs unsignierte Sperrlisten gefordert, sondern eine andere Lösung für die Signatur von Sperrlisten. Die Bundesnetzagentur löst dieses Problem bei den qualifizierten Signaturen mit "indirekten" Sperrlisten. Das bedeutet, die Sperrlisten werden statt mit dem das Zertifikat ausstellenden Schlüssel ("direkte" Sperrliste) mit eigens hierfür erzeugten Sperrlisten-Schlüsseln erstellt, deren Zertifikat und Bestimmungszweck nachgeprüft bzw. abgefragt werden können.

Mein Haus hat das Gesprächsangebot des Bundesamtes für Sicherheit in der Informationstechnik als Betreiber der Verwaltungs-PKI über die Verwaltungs-PKI-Policy angenommen. Wir werden im Rahmen dieser Gespräche auch im Auftrag des

Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gemeinsam mit dem Landesbeauftragten für den Datenschutz in Sachsen-Anhalt versuchen, insbesondere eine Lösung für dieses Problem zu finden.

8.2 Datenschutz beim Umgang mit Speichermedien

Den meisten Nutzern ist beim Umgang mit Speichermedien nicht bewusst, dass Daten nach einfachem Löschen noch lesbar bleiben. Dieser Beitrag zeigt Risiken und Lösungsmöglichkeiten auf.

Mir wurde unter anderem eine Festplatte aus einem Altgerät zur Verfügung gestellt, von der nahezu der gesamte Inhalt - mit teilweise höchst sensiblen Daten - wiederhergestellt werden konnte. Gleiches gilt für einen USB-Stick, den ich im Wege des Datenaustauschs erhielt.

8.2.1 Funktion der Dateiverwaltung

Das Speichern einer Datei erfolgt auf einem Datenträger in Blöcken fester Größe (diese wird beim Formatieren festgelegt) und dem Eintrag eines Verweises auf den ersten Datenblock im Verzeichnis. Als Analogie kann ein Buch dienen, dies hat z.B. 100 Seiten, auf die je 1000 Zeichen (40 Zeilen zu je 25 Zeichen) geschrieben werden können. Das Kapitel beginnt immer an einem Seitenanfang, diese Seitennummer wird im Inhaltsverzeichnis hinterlegt.

Immer noch hält sich die unzutreffende Meinung, eine Datei, die über den Explorer (oder die Kommandozeile mit dem Befehl "del") gelöscht wird (und ggf. aus dem Windows-Papierkorb entfernt wird), sei nicht mehr lesbar. Ebenso wenig genügt das einfache Formatieren eines Datenträgers, um die darauf enthaltenen Daten zu vernichten.

Tatsächlich werden nämlich nur die Verzeichniseinträge im Dateisystem entfernt. Damit ist lediglich der von der Datei verwendete Speicherplatz als frei markiert und kann mit neuen Daten überschrieben werden. Im Buch-Beispiel wird also nur der Eintrag im Inhaltsverzeichnis entfernt, und die bisher verwendeten Seiten können neu beschrieben werden. Damit ist das Kapitel für den Leser nicht mehr vorhanden, da das Auffinden aus seiner Sicht ausschließlich über das Inhaltsverzeichnis erfolgt.

Wichtig ist in diesem Zusammenhang auch, dass das Überschreiben mit neuen Daten gegebenenfalls die alten Daten nicht vollständig entfernt: Wurde ein Datenblock (also die Buchseite) von der alten Datei vollständig belegt, benötigt die neue Datei aber nur einen Teil des Datenblocks, weil sie innerhalb dieses Blocks endet, werden in diesem Datenblock nur die von der neuen Datei benötigten Datenbereiche überschrieben, die übrigen Daten (der alten Datei) bleiben weiterhin lesbar (sog. "cluster tips").

8.2.2 Sicheres Löschen von Dateien

Unter "sicherem Löschen" von Daten sind weitergehende Maßnahmen zu verstehen, die das Wiederherstellen der Daten erschweren oder unmöglich machen. Dies erfolgt im Allgemeinen dadurch, dass der freigegebene Speicherplatz auf dem Datenträger sofort und mehrfach mit Daten überschrieben wird. Die gängigen Verfahren verwenden 3 oder 7, besonders sichere Verfahren bis zu 35 Durchläufe mit festen Daten (z.B. Null-Zeichen) oder Zufallszeichen ("Pseudo-random"). Dies macht auch das Wiederherstellen mit Verfahren, die z.B. auf der Analyse der Magnetschicht einer Festplatte basieren, unmöglich.

Wichtig ist beim Löschen von Dateien auch, dass das Verfahren alle Datenblöcke vollständig überschreibt, also auch die "cluster tips" (s.o.) löscht. Eine Übersicht über Programme, die diesen Erfordernissen genügen, habe ich in Ziffer 8.2.5 aufgeführt.

8.2.3 Umgang mit mobilen Datenträgern

Ein wichtiges Medium zum schnellen und einfachen Datenaustausch ist mittlerweile der USB-Stick geworden. Dies hängt im Wesentlichen damit zusammen, dass solche Sticks von modernen Betriebssystemen schnell und einfach erkannt und eingebunden werden, die Kapazitäten immer weiter steigen und die Geräte mittlerweile sehr günstig zu erwerben sind.

Die meisten Anwender sind sich nicht darüber im Klaren, das das "sorglose" Einstecken ihres USB-Sticks in Rechner einige Risiken beinhaltet.

Dies gilt selbstverständlich auch für andere Medien, die solche Datenträger enthalten (etwa Kameras, MP3-Player mit Speicherkarten) und Disketten (auch wenn deren Nutzung abnimmt).

8.2.3.1 Risiken bei mobilen Datenträgern

8.2.3.1.1 Schadsoftware

Risiken bestehen in der Möglichkeit, den Datenträger mit Viren zu infizieren, falls der Rechner, an den das Gerät angeschlossen wird, nicht aktuell geschützt ist und die infizierten Dateien nicht nur in das eigene, sondern auch in andere Netzwerke zu tragen. Wie einfach dies ist, haben Versuche gezeigt, einen präparierten USB-Stick auf einem öffentlich zugänglichen Platz oder gar einem Firmenparkplatz liegen zu lassen, der dann von einem unbedarften Finder am Arbeitsplatz installiert wird (z.B. "Switchblade").

Zum anderen betrifft dies den Inhalt des Datenträgers, der eventuell nicht oder nicht vollständig für den aktuellen Besucher gedacht ist. Über Werkzeuge wie "USBDumper" oder "Hacksaw", die als Hintergrundprozesse auf einem Rechner aktiv sind, wird der komplette Inhalt eines USB-Sticks auf den Rechner übertragen, ohne das dies einer Interaktion durch den Benutzer bedarf.

8.2.3.1.2 Wiederherstellen von Daten (unbeaufsichtigter Datenaustausch)

Werden mobile Datenträger als Medium für den unbeaufsichtigten Datenaustausch verwendet, bieten sich sogar noch weitergehende Möglichkeiten: Mit Datenrettungswerkzeugen, die das Wiederherstellen gelöschter Dateien ermöglichen, können vermeintlich gelöschte Daten problemlos wiederhergestellt werden, die vielleicht gar nicht für den Besuchten gedacht sind. Auf einem relativ kleinen USB-Stick, der einem meiner Mitarbeiter überlassen wurde, um 4 Dokumente zu kopieren, konnten auf diese Weise über 500 weitere, vorher gelöschte Dateien wiederhergestellt werden, die zum größten Teil auch noch lesbar waren, da der verwendete Speicherplatz noch nicht neu überschrieben wurde.

Datenrettungswerkzeuge orientieren sich nicht am Verzeichnis (im Buch das Inhaltsverzeichnis), sondern arbeiten umgekehrt: sie untersuchen jeden Datenblock auf lesbare Daten und erstellen daraus ein neues Verzeichnis (blättert man das Buch Seite für Seite durch, findet man auch die Kapitel, die nicht im Inhaltsverzeichnis aufgeführt sind).

8.2.3.1.3 Verlust

Sensitive Daten, die auf mobilen Datenträgern transportiert werden, sollten durch geeignete Maßnahmen auch bei Verlust des Datenträgers gesichert sein. Entweder ist dies ein Gerät, das selbst Authentifizierungsmechanismen bereitstellt (z.B. USB-Stick mit Fingerabdrucksensor) oder die Daten auf dem Medium müssen verschlüsselt werden.

Der (unehrliche) Finder kann dann zwar das Medium noch für sich verwenden und neue Daten aufbringen, aber nicht auf die vorhandenen Daten zugreifen. Verschlüsselte Daten können nicht oder nur mit sehr hohem Aufwand entschlüsselt werden, ein durch Fingerabdruck gesicherter USB-Stick kann zwar zurückgesetzt (neu initialisiert werden), dies bedingt aber die Neuformatierung des Geräts inklusive der Löschung aller vorhandenen Daten. Die oben erwähnten Wiederherstellungsmechanismen greifen in diesem Fall nicht, da nicht lesbare (mit dem ursprünglich verwendeten Fingerabdruck verschlüsselte Daten) wiederhergestellt werden.

8.2.3.2 Regeln zur Risikovermeidung beim Umgang mit Daten auf einem mobilen Gerät

1. Löschen Sie nicht mehr benötigte Daten mit einem geeigneten Löschprogramm (das Löschen über den Explorer genügt nicht).
2. Führen Sie in regelmäßigen Abständen eine vollständige Löschung des Datenträgers durch (Löschen aller Dateien und überschreiben des freien Speicherplatzes). Eine Neuformatierung ist nicht ausreichend!
3. Führen Sie nur die für den aktuellen Zweck benötigten Daten auf dem Datenträger mit.
4. Schützen Sie sensitive Daten durch geeignete Maßnahmen vor unbefugtem Zugriff.

8.2.4 Risiken beim Umgang mit sonstigen Datenträgern

Auch eingebaute Speichermedien wie Festplatten in Rechnern und sonstige Geräte mit Datenträgern (insbesondere Digitalkopierer) können bei sorglosem Umgang, etwa im Rahmen der Rück- oder Weitergabe oder bei nicht sachgerechter Entsorgung, sensitive Daten preisgeben.

8.2.4.1 Festplatten in Altgeräten

Es ist durchaus üblich und auch lobenswert, wenn Institutionen nicht mehr verwendete Altgeräte für gemeinnützige Zwecke spenden. Die im Gerät eingebauten Festplatten müssen aber durch geeignete Verfahren sicher gelöscht werden.

Bei besonders sensiblen Bereichen (z.B. Banken oder Kliniken) empfiehlt es sich, die bisherige Festplatte auszubauen und physisch zu vernichten und in das Gerät eine fabrikneue Festplatte einzubauen.

8.2.4.2 Digitalkopierer

Den wenigsten Verantwortlichen ist klar, dass moderne Digitalkopierer Festplatten als Speichermedium verwenden. Geht das Gerät nach Ablauf der Leasingzeit an den Leasinggeber zurück, ist sicherzustellen, dass die vom Gerät gespeicherten Daten sicher gelöscht werden.

Bei Neuverträgen empfiehlt es sich, nur solche Geräte zu verwenden, in denen eine solche Löschroutine dauerhaft aktiv ist und die nicht mehr benötigten Daten auf der Festplatte in festen Zeitabständen selbsttätig überschreibt. Der Umgang mit eventuell bei Rückgabe noch vorhanden Daten durch den Leasingnehmer ist vertraglich zu regeln. Bestehende Verträge sollten dahingehend überprüft werden.

8.2.5 Lösungsmöglichkeiten

Für die beschriebenen Zwecke ist eine Vielzahl von kommerziellen und frei verfügbaren Programmen verfügbar.

Beispiele:

Sicheres Löschen von Festplatten	VS-Clean (Bundesamt für Sicherheit in der Informationstechnik)
Sicheres Löschen von Dateien	Eraser
Verschlüsseln von Dateien	PGP, GnuPG, TrueCrypt
Verschlüsseln von Rechnern (insbesondere Laptops)	SafeGuard Easy
Wiederherstellen von gelöschten Daten	PC Inspector FileRecovery Ontrack EasyRecovery O&O DiskRecovery

8.3 Fehler- und Unfalldatenspeicher

Im letzten Jahr hat sich eine Arbeitsgruppe des Arbeitskreises Technik und des Düsseldorfer Kreises unter meiner Leitung mit dem Thema Fehler- und Unfalldatenspeicher in Pkw beschäftigt. Der Beitrag stellt die Ergebnisse vor, die in ein internes Arbeitspapier eingeflossen sind, auf das ich in Auszügen eingehen möchte.

8.3.1 Auftrag der Arbeitsgruppe

Im April 2006 hat der Düsseldorfer Kreis, die informelle Vereinigung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, das Thema Fehler- und Unfalldatenspeicher behandelt. Um dem Thema von technischer Seite her nachzugehen, wurde der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gebeten, zusammen mit dem Düsseldorfer Kreis ein gemeinsames Arbeitspapier zur Thematik zu erstellen.

Schon vor einiger Zeit war von der Polizei die Frage an mich herangetragen worden, ob es aus datenschutzrechtlicher Sicht Bedenken gibt, wenn sie etwa zur Aufklärung eines Unfalls auf solche Daten zugreift. Entsprechende Geräte kommen auch in Fuhrparks im öffentlichen Personennahverkehr und bei Rettungsdiensten zum Einsatz. Davon kann das Recht auf informationelle Selbstbestimmung betroffen sein. Deshalb habe ich mich intensiv an dieser Arbeitsgruppe beteiligt. Neben dem Verständnis für die technischen Zusammenhänge war mir dabei die rechtliche Einordnung der verarbeiteten Informationen ein Anliegen.

Auftrag der Arbeitsgruppe war eine Beschreibung der technischen Gegebenheiten bei Fehler- und Unfalldatenspeichern. Daneben sollten Kriterien herausgearbeitet werden, um für einzelne Projekte beurteilen zu können, ob dabei personenbezogene Daten verarbeitet werden mit der Konsequenz, dass die Datenschutzgesetze zur Anwendung kommen. "Pay-as-you-drive" (PAYD), Navigations- oder Multimediageräte sollten nicht Gegenstand der Betrachtung sein. Gleiches galt für neue technische Entwicklungen und Szenarien wie vernetzte Pkw und neue Systeme zur Datenübertragung in Fahrzeugen, die zu einem späteren Zeitpunkt angegangen werden sollten.

Die Arbeitsgruppe hat sich in mehreren Sitzungen mit der Thematik befasst. Dabei wurden auch bei Herstellern direkt Informationen eingeholt.

Als Ergebnis wurden die technischen Möglichkeiten beschrieben und Arbeitshilfen erstellt, die Grundlage der datenschutzrechtlichen Bewertung konkreter Projekte sein können.

Die Einschätzungen zur rechtlichen Beurteilung differierten in der Arbeitsgruppe. Meine Einschätzung erläutere ich im Anschluss an die Darstellung der Technik.

8.3.2 Beschreibung der technischen Möglichkeiten

8.3.2.1 Allgemein

Die Beschreibung bezieht sich auf den **heutigen** Stand. Dieser kann sich für neue Fahrzeuge schnell ändern.

Moderne Pkw und Lkw besitzen eine ganze Reihe von Bauteilen, die elektronische Schaltungen umfassen. Die Daten zwischen den Bauteilen werden dabei über verschiedene (Kommunikations-)Bussysteme ausgetauscht, die unterschiedliche Einsatzgebiete haben. Üblich sind derzeit ereignisgesteuerte Bussysteme. Die Entwicklung geht in Richtung von zeitschlitzgesteuerten Systemen. Beispiele für heute verfügbare Bussysteme sind:

LIN (**L**ocal **I**nterconnect **N**etwork, Master-Slave)	geringe Leistungsfähigkeit z.B. bei der Verkabelung in Türen (Fensterheber u.Ä.) eingesetzt
CAN (**C**ontroller **A**rea **N**etwork, CSMA/CA)	normiert (ISO 11898), weitverbreitet, nicht nur in der Automobilindustrie eingesetzt. Nicht echtzeitfähig.
TTCAN (**T**ime **T**riggered **C**ontroller **A**rea **N**etwork)	Weiterentwicklung des CAN mit dem Ziel Mindestantwortzeiten zu garantieren
MOST (**M**edia **O**riented **S**ystem **T**ransport)	Bus für Mediaanwendungen

Für Echtzeitanwendungen sind weitere Bussysteme entwickelt worden, die zukünftig an Bedeutung gewinnen dürften.

Einige Bussysteme sind normiert. Dies betrifft die Datenübertragung. Nicht normiert sind die Daten, die übertragen oder in den Bauteilen gespeichert werden. Hier sind Kfz-herstellerspezifische oder sogar spezifische Eigenarten je Fahrzeugbaureihe zu beachten.

Auf den heute eingesetzten Bussystemen gibt es in der Regel keine absolute Systemzeit. Der Start des Fahrzeugs, also die Zündung, führt ähnlich einem Rechnerstart dazu, dass die Bauteile einen festen Startzustand einnehmen. Zeitmarken werden, soweit vorhanden, relativ zum Startzeitpunkt gesetzt.

8.3.2.2 Fehlerdaten

Fehlerdaten werden insbesondere in Bauteilen mit elektronischen Komponenten gespeichert. Allerdings bieten Hersteller von Kfz-Elektronik auch Controller an, die mehrere Bauteile kontrollieren. Inwieweit damit Fehlerdaten (zusätzlich) im Controller gespeichert werden, konnte noch nicht ermittelt werden. Für Nutzfahrzeuge gibt es Komponenten, über die Informationen zum Zustand des Fahrzeugs sogar während der Fahrt an die Spedition gesendet werden können. Hieraus ergibt sich, dass einer zentralen Speicherung keine technischen, sondern nur konzeptionelle Schranken entgegenstehen.

Welche Daten in Bauteilen gespeichert werden, wird durch die Spezifikation des Fahrzeug-Herstellers bestimmt. Komponentenhersteller setzen diese Vorgaben um. Deshalb ist es in der Regel so, dass ein Komponentenhersteller für verschiedene Kfz-Hersteller verschiedene Bauteile herstellt, die unterschiedliche Daten speichern. Es gibt keine allgemein gültigen Datenkataloge. Welcher Fehler wie gespeichert wird, hängt auch von der Spezifikation ab. So gibt es Fehlerzustände die kumuliert werden und andere, die bei einer fehlerfreien Funktion zurückgesetzt werden. Es gibt in der Praxis bereits ABS-Systeme, die Bremszeiten und Fehler aufzeichnen.

Bei der Diagnose und Wartung eines Bauteils wird der Fehlerspeicher auf Null zurückgesetzt. Mit Diagnosegeräten ist ein Zugriff auf alte Fehlerzustände nicht mehr möglich. Es gibt in der Regel jedoch einen "Shadow-Speicher" bzw. "Permanentspeicher" im Bauteil. Dieser Speicher wird bei einer Wartung nicht auf Null gesetzt. In diesem Speicher werden **alle** Fehlerzustände des Bauteils gespeichert. Ein Zugriff auf diese Daten ist nicht mit Standard-Diagnosegeräten möglich. Zugreifen können nur Hersteller des Bauteils bzw. des Kfz, die mit den Daten vor allem Fälle einer Gewährleistung oder Garantie klären können wollen.

Um Fehlerzustände zuordnen zu können, wird in der Regel der Kilometerstand gespeichert, bei dem der Fehler auftrat. Es handelt sich aber nicht um einen genauen, sondern um einen gerundeten Kilometerstand. Eine Ungenauigkeit von bis zu 16 Kilometer kann, je nach Spezifikation, auftreten. Sollte es in einem Kfz ein Zeitsignal auf dem Bus geben, wäre es auch möglich, eine Zeit zu dem Fehler zu speichern. Dies ist derzeit noch nicht der Fall.

Es gibt keine Authentisierung von Lesegeräten, d.h. wird ein geeignetes Diagnosegerät an das Bussystem angeschlossen, kann es die Fehlerdaten auslesen. Der Zugriffsschutz wird in der Regel dadurch erreicht, dass die Anschlussmöglichkeiten für Diagnosegeräte im Fahrzeuginnern sind und für den Zugriff das Fahrzeug (mit dem Schlüssel) geöffnet werden muss.

8.3.2.3 Unfalldaten

Unfalldaten werden in speziellen Bauteilen, den Unfalldatenspeichern (UDS) für den Zugriff vorgehalten. Im Unterschied zu Fehlerdatenspeichern, die bei neuen (elektronischen) Bauteilen in der Regel immer ab Werk eingebaut sind, werden UDS erst auf Wunsch des Käufers eingebaut.

Der UDS speichert Daten von Bauteilen, die er über die Bussysteme erhält, und Daten, die durch im UDS integrierte Sensoren erfasst werden. Durch integrierte Sensoren werden meist Beschleunigungskräfte erfasst und eine interne Uhr gibt Datum und Uhrzeit vor.

Die Daten werden in einem Ringspeicher gespeichert und nach einer vorgegeben Zeit, in der Regel 45 Sekunden, überschrieben.

Eine dauerhafte Speicherung erfolgt, wenn Sensoren Messwerte liefern, die nach den Parametern als zu speicherndes Ereignis (z.B. Unfall) gewertet werden. Wird ein Ereignis/Unfall erkannt, werden die Daten der letzten ca. 30 Sekunden und der folgenden 15 Sekunden in einem Ereignisspeicher abgelegt. Je nach Bauart des UDS können Daten zu unterschiedlich vielen Ereignissen gespeichert werden. Üblich sind etwa zehn Ereignisse.

In der Regel kann eine Speicherung auch manuell durch den Fahrer ausgelöst werden.
Als Begründung werden Fälle genannt, in denen ein Fahrer nachweisen will, wie sein Fahrverhalten tatsächlich war. Stürzt beispielsweise ein Fahrgast im Bus, könnte der Fahrer mit der Aufzeichnung belegen, dass er nicht ruckartig angefahren ist.

Die Parameter, nach denen ein Ereignis/Unfall erkannt wird und eine Speicherung erfolgt, hängen vom Fahrzeug ab. So müssen z.B. bei einem Lkw andere Beschleunigungswerte als Indiz für einen Unfall gewertet werden, als bei einem Pkw.

Die UDS müssen fest mit der Karosserie verbunden sein, da die internen Sensoren, die Beschleunigungskräfte messen mit denen ein Ereignis erkannt wird, sonst keine verlässlichen Werte liefern.

Folgende Daten werden typischerweise gespeichert:
- Datum
- Uhrzeit
- Längsbeschleunigung bzw. -verzögerung
- Querbeschleunigung bzw. -verzögerung
- Geschwindigkeit
- Zustand von

Zündung, Bremslicht, Blinker, Abblendlicht, Fernlicht, Rückfahrscheinwerfer, ABS, Airbags und bei Einsatzfahrzeugen Blaulicht und Sondersignal.

Aus dem EU-Projekt VERONICA heraus wurden weitere Daten genannt, deren Speicherung für sinnvoll erachtet wird (Geschwindigkeit zu Beginn des Ereignisses, Geschwindigkeitsprofil, Geschwindigkeitsänderung durch Aufprall, Beschleunigungen vor und nach Aufprall, GPS-Position, Sitzhaltung, Fahreraktivitäten, Fahrer-ID, …).

Als Anforderungen an UDS (im Projekt VERONICA wird er als EDR Event Data Recorder/Ereignisdatenspeicher bezeichnet) wurden im Projekt VERONICA genannt:
Es muss sich um fälschungssichere, evaluierte, geprüfte und zertifizierte Technik handeln. Es muss sich um standardisierte Technik handeln, die nur von zugelassenen und zertifizierten Fachleuten ausgewertet werden sollte. Die Daten müssen dem Unfallzeitpunkt zugeordnet sein. Es muss klare Regelungen zur Zweckbindung geben, und ein Zugriff darf nur bei Vorliegen der Vorraussetzungen durch autorisierte Stellen erfolgen (Polizei, Justiz, Versicherungen). Ob diese Anforderungen umgesetzt sind, kann nur im Einzelfall entschieden werden.

8.3.2.4 "Pay-as-you-drive" (PAYD)

Für PAYD-Systeme ist typisch, dass die gespeicherten Daten (Parameter) nicht ereignisbezogen sind, sondern verhaltensbezogen. Dies sind beispielsweise die gefahrenen Kilometer, Reisezeiten, befahrene Straßen(arten), Geschwindigkeit (Durchschnitts- und Höchstgeschwindigkeit), besetzte Sitze, Beschleunigung, Verzögerung usw. PAYD-Systeme werden von der jeweils zuständigen Aufsichtsbehörde geprüft, ob Vertragsinhalt und technische Umsetzung die datenschutzrechtlichen Vorgaben einhalten.

8.3.3 Anmerkungen zu rechtlichen Fragestellungen

Für die Frage, ob die Daten personenbeziehbar sind, ist entscheidend ob - ggf. mit Zusatzwissen - ein Bezug auf eine konkrete Person herstellbar ist und ob dies mit einem vertretbarem Aufwand gelingen kann. Davon zu trennen ist die Frage, ob dieser Rückschluss auf die konkrete Person im Einzelfall gerichtsfest bewiesen wird.

Bei den in den Unfall- und Fehlerdatenspeichern gespeicherten Daten handelt es sich zunächst um technische Informationen. Diese können zu personenbeziehbaren Daten werden, wenn - über eine Verknüpfung mit anderen (externen) Daten - ein Bezug zu einer konkretisierbaren Person möglich ist.
Seitens der Hersteller wurde ausgeführt, dass sie in aller Regel keine Informationen haben, um Daten von Bauteilen einem Halter oder erst recht einem Fahrer zuzuordnen. Die nötigen Daten lägen nur den Werkstätten vor, außer bei der Abwicklung eines Garantiefalls. Allerdings würden die Daten in aller Regel in Verbindung mit der Fahrzeugidentifikationsnummer gespeichert.

Diese kann jedoch immer zumindest auf den aktuellen Halter des Fahrzeugs zurückgeführt werden. Eine mögliche Personalisierung ist somit (auch für den Hersteller) nicht ausgeschlossen. Durch die nur eingeschränkte Zuordnung bestimmter Fehlerzustände zu einem bestimmten Zeitpunkt ist es oft nicht möglich, die Daten einem konkreten Fahrer zuzuordnen. Je nach Konstellation ist der Aufwand, die Daten im Speicher einer bestimmten Person zuzuordnen, daher unterschiedlich hoch. Falls ein Fahrzeug nur von einer Person gefahren wird, ergibt sich eine Zuordnung in jedem Fall. Grundsätzlich ist aber von einer Personenbeziehbarkeit der Informationen auszugehen.

Bei den Unfalldatenspeichern und "pay-as-you-drive" ist der Personenbezug gewollt und insofern unstrittig. Die Situation stellt sich bei Fehlerdatenspeichern anders da. Selbst wenn der Fehlerzustand einem bestimmten Zeitpunkt zugeordnet werden kann, ist damit nicht zwingend eine Aussage über eine (bestimmte) Person verknüpft. Es muss unterschieden werden, zwischen Informationen, die von ihrem Charakter her einem Bauteil eine Eigenschaft zuordnen, etwa der Ausfall einer Blinkleuchte und solchen, die (auch) eine Aussage über das Verhalten des Fahrers treffen können - etwa wenn ein ABS-System speichert, wie oft es anspricht. In diesem Fall würde ein hoher Wert eine Aussage zu der Fahrweise des/der Fahrer beinhalten.

Für die Hersteller bedeutet die grundsätzliche Personenbeziehbarkeit nicht, dass die Verarbeitung dieser Informationen per se ausgeschlossen ist. Allerdings ist im Falle einer Zweckänderung - d.h. wenn die Informationen nicht zur Bearbeitung konkreter Fehlerbehebung verwendet werden sollen - eine Rechtsgrundlage notwendig. Soweit die Daten für Entwicklungs- und Forschungszwecke längerfristig verwendet werden sollen, ist eine anonymisierte Speicherung zu organisieren, d.h. ohne eine Verknüpfung mit der eindeutigen Fahrzeugnummer.

Die faktische Verfügungsgewalt über die im Fahrzeug gespeicherten Daten liegt beim Halter/Fahrer. Dies wird dadurch gewährleistet, dass in der Regel der Zugang zur Schnittstelle nur möglich ist, wenn ein Zugang zum Fahrzeug durch den Inhaber des Schlüssels gewährt wird.

Hersteller des Fahrzeugs und/oder des Informationssystems haben keine Urheberrechte an den mit dem System erzeugten Daten. Die Entwicklung/Auswahl der bzw. die Entscheidung über in den Fahrzeugen eingesetzte Technik berechtigt nicht, über die Nutzung der damit erzeugten Daten zu entscheiden. Dies gilt sowohl für die Frage, von wem als auch welche Daten für welchen Zweck genutzt werden dürfen.

Mit dem Erwerb des Fahrzeugs gehen auch die Verfügungsrechte an den Halter bzw. Fahrer über. Damit dieser seine Rechte wahrnehmen kann, muss er allerdings wissen, dass und in welchem Unfang solche Daten in seinem Fahrzeug erzeugt und gespeichert werden. In jedem Fall sollte die Fahrzeug-Dokumentation daher Aussagen zu Fehlerdaten und deren

Verwendungsmöglichkeiten umfassen. Um die Rechte des Halters an den Daten abzusichern, ist auch an die Möglichkeit zu denken, die Daten verschlüsselt so abzulegen, dass sie nur unter Mitwirkung des Halters auslesbar sind.

8.3.4 Folgerung zur Beurteilung konkreter Projekte mit Unfalldatenspeichern

Bei UDS ist der Personenbezug nicht strittig. Daraus ergeben sich u.a. folgende Datenschutzanforderungen (vgl. auch Projektbericht VERONICA):
- Es darf keine totale Überwachung geben.
- Es dürfen nur Daten gespeichert werden, die unmittelbar vor und nach dem Ereignis (Unfall) anfallen.
- Es muss eine Definition von "Ereignis/Unfall" geben, und die Schwellwerte sind entsprechend zu setzen.
- Es dürfen nur erforderliche Daten gespeichert werden.
- Es muss eine maximale Anzahl von Ereignissen vorgegeben werden, zu denen im UDS Daten gespeichert werden.
- Die Daten sind zu löschen, wenn sie nicht mehr benötigt werden; es muss folglich auch gelöscht werden, wenn die Daten längere Zeit (z.B. sechs Wochen) nicht ausgewertet wurden.
- Es muss möglich sein, Löschprioritäten zu definieren.
- Es muss auch die Speicherdauer für Daten vorgegeben sein, wenn diese aus dem UDS für eine Untersuchung kopiert wurden.
- Die Schnittstellensicherheit und die Datenintegrität müssen ein hohes Niveau haben.
- Ein Zugriff auf die Daten darf nur Personen möglich sein, die die Berechtigung dazu haben.
- Die Datenverarbeitung muss für den Fahrer transparent sein.

Für den verpflichtenden Einsatz von UDS im Kfz muss es eine gesetzliche oder vertragliche Grundlage geben. Die Situation für PAYD-Systeme ist vergleichbar.

8.3.5 Fazit

Wesentliches Ergebnis der Untersuchung für Fehlerdatenspeicher ist, dass die Ausprägung Kfz-hersteller- und sogar baureihenspezifisch ist. Hier ist eine allgemein gültige Beschreibung der Technik nicht möglich.

Die Situation stellt sich für Unfalldatenspeicher etwas anders dar. Die eingesetzte Technik ist wesentlich einheitlicher. Darüber hinaus wurden durch das Projekt der EU "VERONICA" Wünsche und Anforderungen an die Technik für eine künftige wahrscheinliche Entwicklung formuliert.

Allerdings befinden sich die Kriterien, wann die gespeicherten Daten als personenbezogenen anzusehen sind, noch in der Diskussion.

9. Bilanz

9.1 Datenschutz im Verfahren der Verleihung staatlicher Auszeichnungen und Ehrungen (31. Tätigkeitsbericht, Ziff. 3.3)

Bereits in meinem 31. Tätigkeitsbericht hatte ich dargelegt, dass für die Verarbeitung von Daten im Verfahren der Verleihung von staatlichen Auszeichnungen und Ehrungen eine gesetzliche Rechtsgrundlage fehlt. Dies führt zu unzulässigen Datensammlungen. Vor dem Hintergrund, dass die Daten regelmäßig ohne Wissen der Betroffenen erhoben und gespeichert werden, erhält diese Tatsache besonderes Gewicht. Führen negative Erkenntnisse über die Ehrungswürdigkeit dazu, dass die im Verfahren zuständige Stelle eine Auszeichnung ablehnt, können sogar Datensammlungen mit belastenden Daten ohne Wissen der Betroffenen bestehen.

Nach wie vor lehnt die Landesregierung es ab, eine gesetzliche Regelung für die Datenverarbeitung in diesen Verfahren zu schaffen. Allerdings hat sie inzwischen nach Abstimmung mit mir und den beteiligten Ressorts mit Gemeinsamem Erlass vom 25. Oktober 2007 (StAnz. S. 2258 f.) Hinweise zum Datenschutz gegeben. Die dort vorgeschriebene Vorgehensweise im Verfahren der Verleihung von staatlichen Ehrungen entspricht im Wesentlichen den Inhalten der ursprünglich ausgearbeiteten Gesetzesregelung:

- Unter Berücksichtigung des Grundsatzes der Erforderlichkeit und Verhältnismäßigkeit sind möglichst wenige Daten zu erheben.

- Zuerst ist festzustellen, ob die Verdienste ausreichen, um eine Ehrung zu verleihen. Erst danach ist zu prüfen, ob die vorgeschlagene Person auch würdig ist, die Ehrung zu empfangen.

- Daten, die in diesem Verfahren erhoben wurden, dürfen zu keinem anderen Zweck verwendet werden.

- Ist der prüfenden Stelle bekannt, dass die Person keine Ehrung wünscht, darf das Verfahren nicht aufgenommen bzw. es muss eingestellt werden.

- Unabhängig von der Verpflichtung Daten, die nicht mehr erforderlich sind, zu löschen, sind Aufbewahrungs- bzw. Löschfristen festgelegt.

Den Kommunen und anderen mit der Verleihung von staatlichen Ehrungen befassten Stellen ist der Erlass zur Anwendung empfohlen.

9.2 Einsatz zentraler Spamfilter der Landesverwaltung (35. Tätigkeitsbericht, Ziff. 8.2)

Im 35. Tätigkeitsbericht hatte ich mich umfassend mit dem Einsatz von zentralen Spamfiltern beschäftigt.

Die im Jahr 2006 konzipierten und mit mir abgestimmten Anti-Spam-Maßnahmen an den zentralen Internet-Mail-Relay-Gateway des Landes wurden Anfang 2007 umgesetzt. Start des Pilotbetriebs war Mai 2007. Mit der Aktivierung der Maßnahmen - insbesondere durch Aktivierung des Greylistings - konnte das Spam-Aufkommen in Hessen deutlich verringert werden. Der Wirkungsgrad liegt zwischen 75 und 80 %.

Folgende Effekte wurden erzielt:
1. Deutliche Verringerung der insgesamt von den externen Mail-Relay-Servern an die internen Strukturen weitergeleiteten Spam-Mails.
2. Dadurch deutliche Verringerung der Belastung der internen Postfach-Server.
3. Durch die Ablehnung von Spam-Mail werden wesentlich weniger Mails an unbekannte Empfänger in das Landesnetz weitergeleitet.
4. Dadurch müssen von den Postfach-Servern weniger Unzustellbarkeitsnachrichten (NDRs) erzeugt und zurückgeschickt werden.
5. Dadurch kommt es zu einem fast vollständigen Rückgang der so genannten "unsolicited bounces" - also der NDRs an real existierende Empfänger, die aber die ursprüngliche Nachricht nicht geschickt hatten - diese war vom Spammer mit der gefälschten Absende-Adresse verschickt worden.
6. Durch den Rückgang der "unsolicited bounces" konnten die Eintragungen auf den Blacklists (DNSBL oder RBLs) fast auf Null reduziert werden.

Im Pilotzeitraum wurden mehrere Spam-Wellen mit Spitzenlasten bis zu 10.000 Mails pro Minute erfolgreich abgewehrt. Die Anti-Spam-Infrastruktur hat diesen Angriffen - darunter auch BotNet-Angriffe - ohne Leistungsverlust für den produktiven Mailverkehr Stand gehalten. Die internen Strukturen waren von den Angriffen vollständig verschont.

Mit Beginn der Herbstferien konnte - nach einem deutlichen Rückgang der Spam-Belastung nach den Sommerferien - eine erneute Steigerung der Spam-Aktivitäten beobachtet werden. Im Schnitt war nach dem 3. Oktober täglich ein Angriff mit Spitzenlasten von mehr als 8.000 Mails pro Minute zu beobachten. Auch diesen Angriffen hat die Anti-Spam-Struktur Stand gehalten. Der produktive Mail-Verkehr lief ohne Unterbrechung und Leistungsverlust weiter; die internen, geschützten Systeme wurden von den Angriffen nicht erreicht.
Insgesamt kann aus betrieblicher und technischer Sicht eine positive Bilanz gezogen werden.

In den Dienststellen, in denen die private E-Mail-Nutzung zugelassen ist, bedürfen Anti-Spam-Maßnahmen wie SPF und Greylisting der Einwilligung der Beschäftigten. Bislang liegt diese Einwilligung erst im HMDIS und im HMDJ vor. Hier muss noch nachgebessert werden.

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

10.1 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. "Trojaner" heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des "offenen Visiers" zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z.B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betrof-

fen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Softwaredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

10.2 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u.a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z.B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

10.3 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des BVerfG einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des BVerfG ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z.B. ein Jahr) bedroht sind und die auch im Einzelfall schwerwiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Er-

kenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

10.4 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Arbeit erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

10.5 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung - beispielsweise durch den Einsatz von vorbezahlten Karten - ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

10.6 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007 GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.
Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, z.B. durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

10.7 Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. Juni 2007
Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung - ob via Telefon oder Internet - pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von sechs auf zwölf Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen - bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsdatenspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrates eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das BVerfG hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des BVerfG zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

10.8 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007
Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürger berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass

letztlich bei allen vertraglichen Beziehungen - also auch bei Versicherungs- und Arbeitsverträgen - vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

10.9 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007
Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.
Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um "Online-Durchsicht" als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von - auch unverdächtigen - Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit - jedenfalls bei der Verfolgung von Straftaten - die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z.B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durchsuchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des BVerfG in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

10.10 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007
Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z.B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können - auch wenn die Betroffenen über die Umstände informiert wurden - diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen - zusätzlich - zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u.a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

10.11 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2007
Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist u.a., die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.

- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform "Elster" für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuer*fremden* Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Abs. 5 AO zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BAföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z.B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

11. Orientierungshilfe

24. September 2007

Arbeitskreis Medien[1]

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Viele Beschäftigte im öffentlichen Dienst haben heute die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten, ihrer Kommunikationspartner und anderer Betroffener (beispielsweise Dritter, deren Namen in einer E-Mail genannt werden) bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

a) Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber[2] so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung nachträglichen Kontrollen vorzuziehen.

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

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

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

e) Es gibt eine Vielzahl an Möglichkeiten zur Abwehr unerwünschter Nachrichten (Spam), die in verschiedensten Kombinationen und Ausprägungen eingesetzt werden können. Welche Maßnahmen dafür grundsätzlich in Betracht kommen, kann etwa der Anti-Spam-Studie des BSI[3] entnommen werden. Die auf dieser Grundlage denkbaren Lösungen unterscheiden sich sowohl hinsichtlich ihrer Eignung als auch hinsichtlich des Ausmaßes, in dem sie in die Persönlichkeitsrechte der Kommunikationspartner oder Dritter eingreifen. Daher sollte jede Stelle, bevor sie Maßnahmen zur Spam-Abwehr ergreift, eine schriftliche Konzeption hierfür erstellen, der zu entnehmen ist, dass unter den in Betracht kommenden Varianten die datenschutzfreundlichste gewählt wurde.

Die Konzeption sollte dabei folgenden Grundsätzen Rechnung tragen:

- Filter, die Header oder Inhalt elektronischer Post automatisch auf unerwünschte Nachrichten (Spam) prüfen, sollten erst an einem Punkt eingesetzt werden, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.
- Die (zentrale) Markierung spamverdächtiger Nachrichten ist dabei der zentralen Löschung von E-Mails ohne Kenntnis des Empfängers vorzuziehen.
- Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten in größtmöglicher Autonomie über den Umgang mit den an sie gerichteten E-Mails selbst entscheiden können.

II. Dienstliche Nutzung

a) Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (TK-) bzw. Telemedienrechts (vgl. § 11 Abs. 1 Nr. 1 Telemediengesetz, TMG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den jeweils einschlägigen, am Erforderlichkeitsmaßstab orientierten Vorschriften des Beamtenrechts sowie des BDSG bzw. der Landesdatenschutzgesetze.

b) Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall

[1] Die Orientierungshilfe wurde unter Beteiligung des AK Personalwesen erstellt. Sie richtet sich in erster Linie an öffentliche Stellen des Bundes und der Länder. Die hier dargestellten Grundsätze können auch auf den nicht-öffentlichen Bereich übertragen werden.

[2] Zur Vereinfachung bezeichnet "Arbeitgeber" sowohl den Arbeitgeber als auch den öffentlich-rechtlichen Dienstherrn

[3] www.bsi.de/literat/studien/antispam/antispam.pdf

zulässig. Es wird empfohlen, über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

c) Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen, muss eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verkehrsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

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

e) Eine Betriebs- oder Dienstvereinbarung kann nur dann als besondere Rechtsvorschrift angesehen werden, wenn die Datenerhebung, -verarbeitung und -nutzung ausreichend und präzise innerhalb des Erlaubnisumfangs gesetzlicher Bestimmungen geregelt wird und sie das gesetzliche Schutzniveau nicht unterschreitet.

f) Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung der Protokolldaten über die unter a. genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internetnutzung auszuräumen.

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

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

i) Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen kann.

III. Private Nutzung

1. Allgemeines

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

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

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

d) Es gelten die Regelungen der Telekommunikationsgesetzes, des Telemediengesetzes bzw. des Rundfunkstaatsvertrages.

e) Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Beschränkungen nicht akzeptieren wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

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

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

2. Besonderheiten bei E-Mail

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

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

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

d) Eine zentrale Spam-Filterung, bei der automatisch auf den Header oder Inhalte zugegriffen wird, darf nur mit Einwilligung des Empfängers erfolgen, da die Reichweite des Fernmeldegeheimnisses erst endet, wenn die E-Mail in seine vollständige Verfügungsgewalt gelangt ist. Auch dies ist als einschränkende Voraussetzung für die Erlaubnis zur privaten Nutzung (s.o., III.1.e) anzusehen und damit Bestandteil der Einwilligung. Die Einwilligung kann pauschal vorab erfolgen. Die Beschäftigten sind über die Art und Weise der Spam-Filterung, insbesondere über die dabei stattfindende Verarbeitung personenbezogener Daten, zu informieren.

e) Eine darüber hinausgehende inhaltliche Kontrolle ist nicht zulässig.

12. Materialien

30. November 2007

**Arbeitskreis "Technische und organisatorische Datenschutzfragen"
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder**

Technische Aspekte der Online-Durchsuchung

0 Vorbemerkung

Das vorliegende Dokument soll den Ablauf und die technischen Verfahren der geplanten Online-Durchsuchung erläutern und aus technischer Sicht bewerten.

In den Abschnitten 1 bis 4 wird die Online-Durchsuchung beschrieben. Diese Beschreibung basiert auf den Antworten des BMI vom 22. August 2007 zu den Fragenkatalogen des BMJ und der SPD-Bundestagsfraktion. In diesen Abschnitten werden vorwiegend Begriffe verwendet, die aus dem Fragenkatalog stammen, auch wenn sie nicht allgemein anerkannt bzw. akzeptiert sind.

Im Abschnitt 5 werden die Abläufe und Verfahren aus technischer Sicht bewertet. Die Beschreibungen und Schlussfolgerungen hat der AK Technik zusammengestellt. Die Bewertungen gehen von derzeit technisch grundsätzlich möglichen Szenarien aus. In vielen Punkten besteht allerdings noch erheblicher Klärungsbedarf.

1 Begriffe

Informationstechnisches System:
- Gegenstand der Online-Durchsuchung
- System aus Hardware, Software und Daten, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient
- kann bspw. Personalcomputer, Server, vernetzte Verbünde von Computern, Infrastrukturkomponenten (Router, Switsche, DE-CIX-Einrichtungen), externe Speichermedien (z.B. CD-ROMs, DVDs, externe Festplatten, USB-Speicher), Fax-Geräte, Mobilgeräte (z.B. Handys, Smartphones, Blackberrys) betreffen

Online-Durchsuchung:
- Oberbegriff für Online-Durchsicht und Online-Überwachung

Online-Durchsicht:
- einmalige Durchsuchung eines informationstechnischen Systems

Online-Überwachung:
- Überwachung eines informationstechnischen Systems über einen gewissen Zeitraum
  Anm.: Inhalte aktueller Telekommunikationsvorgänge sollen nicht Gegenstand der Online-Überwachung sein

Quellen-TKÜ:
- ausschließliche Erhebung von Telekommunikationsinhalten

Anm.: soll sonstige, auf der Festplatte abgelegte Inhalte nicht betreffen

Remote-Forensic-Software (RFS):
- interne Bezeichnung des BKA für die zu verwendende Software

2 Phasen der Online-Durchsuchung

2.1 Technische Vorabklärung

2.1.1 Art der Informationsgewinnung
- Telekommunikationsüberwachung
- Portscan
- herkömmliche Ermittlungsmaßnahmen
- Einsatz von V-Leuten
- Einsatz von verdeckten Ermittlern

2.1.2 Art der zu beschaffenden Informationen über das Zielsystem
- Betriebssystemtyp und -version
- Internetzugang
- Browsertyp und -version
- installierte Software (Produkte und Versionen)
- Online-Verhalten der Zielperson
- Möglichkeiten der Einbringung der RFS

2.2 Technische Vorbereitung

2.2.1 Einbringungsmöglichkeiten der RFS

2.2.1.1 Aussagen des BMI im Fragenkatalog vom 22. August 2007
Das BMI bleibt bei der Beantwortung der Fragen hinsichtlich der Möglichkeiten der Einbringung sehr unkonkret und beschränkt sich auf Aussagen wie:

"Es gibt eine Vielzahl von Einbringungsmöglichkeiten, die auf Tauglichkeit für den jeweiligen Einsatz überprüft und eventuell angepasst werden müssen."

"Eine generelle Aussage zur genauen Einbringungsmethode ist nicht möglich …"

"Es besteht Einigkeit darüber, dass kein Interesse daran besteht, Hintertüren in Betriebs- und Anwendungssysteme einzubauen …"

"Die Einbringung der RFS im Wege der E-Mail-Kommunikation kann je nach Einzelfall ein geeignetes Mittel darstellen."

2.3 Technische Umsetzung

2.3.1 Zielstellung
Online-Durchsicht: Was hat die Zielperson bezogen auf ihr informationstechnisches System in der Vergangenheit gemacht?

Online-Überwachung: Was macht die Zielperson bezogen auf ihr informationstechnisches System aktuell?

2.3.2 Informationen/Aktivitäten
Folgende Informationen sollen erhoben bzw. Aktivitäten durchgeführt werden:

Online-Durchsicht:
- Informationen über das System selbst
- auf dem Zielsystem gespeicherte Daten
- Suche nach Dateien mit bestimmten Namen
- Suche nach Dateien mit bestimmten Dateiendungen
- Suche nach Eigenschaften/Attributen (z. B. Zugriffsdaten)
- Schlüsselwortsuche
- Suche in bestimmten Verzeichnissen
- Suche nach Dateien eines bestimmten Dateityps

Online-Überwachung:
- alle Funktionen der Durchsicht und zusätzlich

- Erfassung flüchtiger Daten (Passworteingaben; Texte, die nicht übertragen werden; in Bearbeitung befindliche verschlüsselte Dateien)
- Erfassung von Klartexten vor einer Verschlüsselung
- Erfassung von Klartexten nach einer Entschlüsselung
- Einsatz von Key-Loggern zum Abfangen von Tatstatureingaben, beispielsweise von kryptographischen Schlüsseln

An den Computer angeschlossene oder mit diesem kommunizierende Geräte wie Mikrofone, Webcams oder Scanner sollen nicht überwacht werden. Mit diesen Geräten erhobene und auf dem informationstechnischen System gespeicherte Daten können jedoch Gegenstand der Durchsicht/Überwachung sein.

Online-Durchsicht und Online-Überwachung sollen sich ebenfalls nicht auf Telekommunikationsdaten erstrecken. Die technische Vorgehensweise ist vergleichbar, und offensichtlich wird auch der gleiche "technische Baukasten", wenn auch mit unterschiedlichen Bausteinen, genutzt.

Wie eine Vermischung beider Maßnahmen verhindert werden soll, wird nicht beschrieben.

2.3.3 Auswahl/Eingrenzung der zu erhebenden Informationen
Die zu sichernde Datenmenge soll anhand von vorher festgelegten Suchkriterien begrenzt werden. Folgende Möglichkeiten sollen dabei technisch umsetzbar sein:
- Erfassen der Inhalte von Dateien,
- Recherche mittels Suchbegriffen,
- Recherche in gelöschten Texten,
- Überwachung von Befehlen und genutzten Funktionen,
- Recherche nach und Erhebung von Passwörtern, Signaturen und -schlüsseln,

- Einschränkung auf ein tägliches Überwachungszeitfenster (z.B. 20 - 22.00 Uhr),
- Einschränkung auf bestimmte Nutzer.

2.3.4 Umgehungs-/Überwindungsmöglichkeiten von Kryptierungen
Das BMI sieht mehrere Möglichkeiten, Kryptierungen zu umgehen, von denen jedoch nicht alle genutzt werden sollen.

a) Abzweigen von Klar-Informationen vor der Ver- bzw. nach der Entschlüsselung
   - soll genutzt werden

b) Zugriff auf Schlüssel mit Sniffer-Software und/oder Key-Loggern
   - ist eine der vorgesehenen Online-Maßnahmen

c) Verwendung von absichtlich geschwächten Verschlüsselungsprodukten
   - "Der generelle Einbau von staatlichen Hintertüren ist derzeit politisch nicht gewollt."

d) treuhänderische Hinterlegung von kryptographischen Schlüsseln (key escrow)
   - "… in Deutschland politisch nicht durchsetzbar… und technisch wenig erfolgversprechend…"

2.3.5 Ausleitung der Informationen
Die gewonnenen Ergebnisse werden so lange auf dem informationstechnischen System zwischengelagert, bis eine Internetverbindung durch die Zielperson hergestellt wird. Die Daten werden verschlüsselt abgelegt. Nach der Übertragung auf den Rechner der Sicherheitsbehörde werden die Daten auf dem informationstechnischen System gelöscht.

2.4 Dauer und Beendigung der Maßnahme

2.4.1 Dauer der Maßnahme

2.4.1.1 Online-Durchsicht
Die Dauer der Durchsicht und der anschließenden Übermittlung ist abhängig
- von dem Online-Verhalten der Zielperson,
- vom Durchsuchungszweck,
- von der Anzahl und der Größe der zu übertragenden Dateien,
- von der Bandbreite des TK-Anschlusses des Zielsystems,
- vom Betriebszustand des Systems,
- von den Sicherungsmaßnahmen, die die Zielperson getroffen hat.

Die Durchsicht und die anschließende Übertragung kann einen Zeitraum von wenigen Minuten bis zu mehreren Tagen in Anspruch nehmen.

2.4.1.2 Online-Überwachung
Die Überwachungsdauer ist in der Regel wesentlich länger als bei der Online-Durchsicht und soll sich aus dem dann gesetzlich festgelegten Überwachungszeitraum ergeben.

2.4.2 Zeitpunkt und Art der Beendigung

Die Maßnahme soll planmäßig beendet werden, wenn

- die erhobenen Daten als ausreichend angesehen werden,
- der ursprüngliche Verdacht entkräftet wurde,
- die Durchsuchungserlaubnis aufgehoben wurde oder
- der gesetzlich zulässige Überwachungszeitraum erreicht ist.

In diesen Fällen soll sich die RFS auf ein entsprechendes Kommando hin (manuelle Auslösung) selbst deinstallieren.

Darüber hinaus soll die RFS ein Verfallsdatum und Zähler erhalten, die eine Selbst-Deinstallation der Software gewährleisten. Auf diese Weise soll auch eine ungewollte, erneute Aktivierung der RFS etwa nach dem Wiederaufsetzen des Systems mittels Datensicherungen (Back-Up) verhindert werden.

Unter Umständen ist es erforderlich, dass die Maßnahme nicht planmäßig beendet werden muss, bspw.

- bei erfolgloser Kontaktaufnahme mit dem Zielsystem (falls bspw. keine Internetverbindung durch die Zielperson aufgebaut wird) oder bei

- (der eigentlich ausgeschlossenen) Entdeckung der RFS durch Antivirenprogramme, IDS-Systeme oder ähnliche Tools.

Die Deinstallation soll sich ausschließlich auf die RFS auswirken und keine Beeinträchtigungen des Zielsystems nach sich ziehen.

Es ist nicht beabsichtigt, den "Ursprungszustand" des Zielsystems nach der Deinstallation der RFS herzustellen, da sich das Zielsystem während der Laufzeit der RFS ohnehin ständig verändert. Lediglich Änderungen, die die RFS an der Systemkonfiguration vorgenommen hat, sollen bei der Deinstallation der RFS rückgängig gemacht werden.

3 IT-Sicherheitsrisiko für Zielrechner

Mit der selbstentwickelten Software RFS sollen keine Daten auf dem Zielsystem manipuliert werden. Durch Hinterlegung des Quellcodes der RFS, etwa beim genehmigenden Richter, soll die Nachprüfbarkeit dieser Aussage in einem späteren Verfahren garantiert werden können.

Sensible Infrastrukturen in Staat und Wirtschaft sollen nicht gefährdet sein, da keine Online-Durchsuchung von Rechnern in Behörden oder Unternehmen vorgesehen ist.

Die Nutzung der RFS durch Dritte für eigene Zwecke soll nicht möglich sein, da "… die Software keine eigenen Verbreitungsroutinen und auch einen wirksamen Schutz gegen Missbrauch beinhaltet".

Es soll sichergestellt sein, dass die Software RFS "… nicht ohne erheblichen Aufwand …" dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann.

Der generelle Einbau von "staatlichen Hintertüren" in Verschlüsselungsprodukte ist derzeit politisch nicht gewollt. Es besteht Einigkeit darüber, dass kein Interesse daran besteht, "Hintertüren" in Betriebs- und Anwendungssysteme einzubauen. Sie hätten nicht nur für die IT-Sicherheit, sondern auch für die deutsche Wirtschaft fatale Konsequenzen.

4 Beweissicherheit/Computer-Forensik

4.1 "Konventionelle" Beweiserhebung auf Computersystemen

Das BMI beschreibt die konventionelle Durchführung einer Datenträgeruntersuchung (DTU) nur sehr kurz:

- Kopie anfertigen,
- Verifizierung der Kopie,
- Erstellen einer Sicherheitskopie,
- Auswertungen anhand der Kopie, ausführliche Dokumentation.

4.2 Beweiskraft der Online-Durchsuchung

Das BMI hat keine Zweifel an der Beweiskraft der Online-Durchsuchung und verweist auf Folgendes:

- Die Online-Durchsuchung soll lückenlos dokumentiert werden (z. B. die Einbringung der RFS, alle Remote-Zugriffe, alle auf dem Zielrechner durchgeführte Befehle).

- Die Integrität der übertragenen Daten soll durch Hash-, Verschlüsselungs- und Signaturverfahren sichergestellt werden.

Das BMI räumt jedoch ein, dass eine Wiederholung der Überwachungsaktivitäten "… wegen des dynamischen Charakters …" der gesamten Maßnahme nicht möglich ist.

Nach Ansicht des BMI ist die Beweiskraft jedoch nicht immer relevant. Lediglich bei der Nutzung der Online-Durchsuchung im Bereich der Strafverfolgung ist die forensische Beweiserhebung Zweck der Maßnahme. Bei der Nutzung als Maßnahme zur Gefahrenabwehr ist die Erkenntnisgewinnung einziger Zweck.

5 Bewertung und Schlussfolgerungen

5.1 Einbringung der RFS

Der "Erfolg" der Online-Durchsuchung hängt maßgeblich davon ab, ob es technisch und organisatorisch möglich ist, die RFS unbemerkt in das Zielsystem einzubringen. Nachfolgend werden die Erfolgsaussichten bei den bisher diskutierten Einbringungsmethoden diskutiert und generelle Schutzmaßnahmen erläutert.

5.1.1 Einbringungsmöglichkeiten

Da das BMI nicht detailliert auf Einbringungsmöglichkeiten eingeht (vgl. Punkt 2.2.1.1), werden hier einige Möglichkeiten vorgestellt, die - nach dem derzeitigen Stand der Technik - prinzipiell geeignet sind, fremde Rechner unbemerkt mit Software zu infiltrieren.

a) mit "Hilfe" der Zielperson:

- verheißungsvolle E-Mails / Instant Messages mit der RFS als Anhang
- offizielle E-Mails von Behörden mit der RFS als Anhang
- E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint
- manipulierte Web-Seiten, von denen die RFS heruntergeladen wird
- Herumliegenlassen/Zusenden von CDs, USB-Sticks und ähnlichen Datenträgern

b) ohne Hilfe der Zielperson:

- Ausnutzen von Software-Sicherheitslücken mit spezieller, auf die jeweilige Lücke zugeschnittener Software (sog. Exploits)
- Zero-Day-Exploit: erscheint meist am selben Tag, an dem eine Sicherheitslücke allgemein bekannt wird
- Less-Than-Zero-Day-Exploit: wird bereits vor Bekanntwerden einer Sicherheitslücke angeboten
- von Herstellern eingebaute Hintertüren
- Hintertüren in staatlichen E-Government-Anwendungen
- Infektion von Downloads "on the fly"
- physischer Zugriff auf den Zielrechner durch Eindringen in die von der Zielperson benutzten Räume

5.1.2 "Erfolgsaussichten" bei der Einbringung

a) mit "Hilfe" der Zielperson:

- verheißungsvolle E-Mails/Instant Messages mit der RFS als Anhang
  - geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden

- offizielle E-Mails von Behörden mit der RFS als Anhang
  - geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum solche E-Mails öffnen werden

- E-Mails, bei denen der Absender gefälscht wurde, und dem Adressaten vertrauenswürdig erscheint
  - mittlere Erfolgsaussichten, sofern die Zielperson dem Absender ungeprüft vertraut

- manipulierte Web-Seiten, von denen die RFS heruntergeladen wird
  - mittlere Erfolgsaussichten, sofern die Zielperson keine Sandbox einsetzt und konfiguriert

- Herumliegenlassen/Zusenden von CDs, USB-Sticks und ähnlichen Datenträgern
  - geringe Erfolgsaussichten, weil sensibilisierte Zielpersonen kaum ihnen unbekannte Datenträger auf Rechnern mit sensiblen Inhalten nutzen werden

b) ohne Hilfe der Zielperson:

- Ausnutzen von Software-Sicherheitslücken (bekannte Lücken oder Zero-Day-Exploits/Less-Than-Zero-Day-Exploits)
  - mittlere Erfolgsaussichten bei bereits länger bekannten Lücken, sofern keine aktuellen Patches eingespielt wurden
  - hohe Erfolgsaussichten bei Zero-Day-Exploits, weil Schutzmöglichkeiten noch nicht verfügbar sind
  - sehr hohe Erfolgsaussichten bei Less-Than-Zero-Day-Exploits, weil praktisch kein Schutz möglich ist

- von Herstellern eingebaute Hintertüren
  - geringe Erfolgsaussichten, sofern die Zielperson Open-Source-Software einsetzt

- Hintertüren in E-Government-Anwendungen

=> geringe Erfolgsaussichten, weil die Zielpersonen solche Anwendungen kaum nutzen werden

- Infektion von Downloads "on the fly"
  - hohe Erfolgsaussichten, da nur wenige Downloads digital signiert sind
  - hohe Erfolgsaussichten auch bei signierten Downloads, sofern die Hersteller mitwirken

- physischer Zugriff auf die IT-Zielsysteme
  - geringe Erfolgsaussichten bei Einzelsystemen, da ständig unter Kontrolle der Nutzer (z. B. Notebooks)
  - hohe Erfolgsaussichten bei komplexen Systemen und Infrastrukturkomponenten, da Eingriffe nur schwer feststellbar sind

5.1.3 Generelle Gegenmaßnahmen und ihre Schutzwirkung

- Nutzung von zwei PCs (ein Online- und ein Offline-System)
- Daten durchlaufen den Online-PC beim Senden und Empfangen nur verschlüsselt
- Übertragung der Daten zum Bearbeiten (Lesen, Schreiben) bspw. per USB-Stick auf den Offline-PC
  - verhindert das Auslesen mit hoher Wahrscheinlichkeit

- Live-System von CD/DVD
- dauerhafte Änderungen am Betriebssystem mit Hilfe der RFS sind nicht möglich
- nach jedem Neustart von CD/DVD ist der Originalzustand wieder hergestellt
  - verhindert das Auslesen mit hoher Wahrscheinlichkeit

- Nutzung eines virtuellen Zweitsystems
- geschützte Umgebung für das Betriebssystem
- sicherer Kanal in das Gastsystem möglich
  - verhindert das Auslesen aus der geschützten Umgebung mit hoher Wahrscheinlichkeit

- Einsatz von Virenscannern
- einfache Scanner finden nur Schadsoftware mit bekannten Mustern (Signaturen)
  - RFS soll hochspezialisiert sein und von handelsüblichen Scannern angeblich nicht entdeckt werden

- gute Produkte suchen nicht nur nach bekannten Mustern, sondern versuchen, das Verhalten von Software zu analysieren (proaktive Verfahren wie Heuristik oder Sandbox-Technologie)
  - ob hier die RFS unentdeckt bleibt, ist zumindest fraglich

- Einsatz von Intrusion Detection Systemen (IDS)
- erkennen von Angriffsmustern und von Veränderungen der Systemkonfiguration
- schon das Erkennen der Tatsache, dass ein System verändert wurde, könnte auf die RFS hindeuten
  - ob hier die RFS unentdeckt bleibt, ist zumindest fraglich

- Einsatz von Firewalls
- vom Nutzer zugelassene Kommunikation (E-Mails, Downloads) werden nicht unterbunden
- verschlüsselter Datenverkehr ist ebenfalls nicht filterbar
  - Schutz vor RFS kaum realisierbar

- Einsatz des TPM (Trusted Platform Modul)
- erlaubt dem Betriebssystem, Veränderungen zu erkennen
- gewollte Downloads werden möglicherweise nicht als Risiko erkannt
- Hintertüren von Softwareherstellern werden nicht erkannt
  - Schutz vor RFS zurzeit nicht abschließend bewertbar

- Nutzung des Systems ausschließlich nach Anmeldung mit Kennung und Passwort
- bei Nutzerkennungen ohne Admin-Rechten können Installationsmöglichkeiten eingeschränkt werden
- Software-Installation nur mit Admin-Rechten zulassen
  - erschwert das Einbringen der RFS unter bestimmten Umständen

- komplette Festplattenverschlüsselung
- Installationsmöglichkeiten insbesondere bei physikalischem Zugriff kaum gegeben
- erschwert das Einbringen der RFS unter bestimmten Umständen

5.2 Reichweite der Eingriffe

Die Tatsache, dass nicht nur Personalcomputer, sondern beispielsweise auch Server (bspw. Mailserver), vernetzte Verbünde von Computern und komplexe Infrastrukturkomponenten (z. B. Router, Switche, DE-CIX-Einrichtungen) von der Online-Durchsuchung betroffen sein können (vgl. Punkt 1), verdeutlicht die Reichweite und damit die Eingriffstiefe dieser Maßnahme. Werden derartige IT-Komponenten überwacht, muss davon ausgegangen werden, dass nicht nur Einzelpersonen, sondern immer eine kaum einzugrenzende Anzahl von Betroffenen überwacht wird. Das BMI weist zwar darauf hin, dass bei Systemen, die unter der administrativen Betreuung Dritter stehen, anstelle der Online-Überwachung grundsätzlich der direkte Weg zu den jeweiligen Stellen gesucht würde, der aktuelle Gesetzentwurf schließt den Einsatz der RFS jedoch auch hier nicht aus.

Zudem lässt sich die Reichweite schon deshalb kaum einschätzen, weil es einer konkreten Definition des Begriffs "Verbund" mangelt. Es kann sich dabei sowohl um ein kleines lokales Netz handeln als auch um ausgedehnte Firmen-Netze (Intranets). Dass unter diesen Voraussetzungen die Online-Durchsuchung nicht einmal mehr auf Deutschland beschränkt werden kann, bleibt vom BMI völlig unerwähnt.

Im Übrigen ist bereits bei der Online-Durchsuchung von Einzelsystemen wie Personalcomputern oder Laptops davon auszugehen, dass nicht nur Einzelpersonen überwacht werden. Auch in diesen Fällen ist nicht auszuschließen, dass mehrere Personen das System nutzen, und somit von der Maßnahme betroffen sind.

Die Reichweite der Eingriffe kann auch anhand der Art zu erhebender Informationen (vgl. Punkt 2.3.2) verdeutlicht werden. Die Suche nach bestimmten Dateien bedeutet nämlich in der Praxis, dass bspw. gezielt nach E-Mail-Adressbüchern, Kontaktlisten, Logdateien, Schlüsselbünden, Konfigurationsdateien, Cache-Dateien, Browser-Historien oder Sicherheitskopien gesucht werden kann.

5.3 IT-Sicherheitsrisiko für den Zielrechner

Da grundsätzlich zu bezweifeln ist, dass eine komplexe Software wie die RFS vollständig fehlerfrei programmiert wurde, ist äußerst fraglich, ob

- die Software weder durch Antivirenprogramme noch durch IDS-Systeme entdeckt werden kann,
- die Nutzung der RFS durch Dritte für eigene Zwecke wirklich ausgeschlossen werden kann,
- die RFS nicht doch dazu veranlasst werden kann, Daten an einen anderen als den von den Sicherheitsbehörden benutzten Server zu senden und ob
- die Software tatsächlich einen wirksamen Schutz gegen Missbrauch beinhaltet (vgl. Punkt 3).

Im Übrigen schließt das BMI nicht vollständig aus, dass die RFS missbraucht werden kann. Zitat: "Speziell wird sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden und dass die Software weder von außen erkannt noch angesprochen werden kann." Wie hoch der Aufwand tatsächlich ist, wäre zu prüfen.

Jedenfalls ist das BMI in der Pflicht, belastbare Nachweise für die Behauptungen vorzulegen, dass

- tatsächlich keine Daten auf dem Zielsystem manipuliert werden,
- sensible Infrastrukturen in Staat und Wirtschaft nicht gefährdet sind,
- die Nutzung der RFS durch Dritte für eigene Zwecke nicht möglich ist,
- die Software nicht dazu veranlasst werden kann, an einen anderen als den von den Sicherheitsbehörden benutzten Server zurückzumelden,
- die Software weder von außen erkannt noch angesprochen werden kann und
- keine Hintertüren oder absichtlich eingebaute Schwachstellen in Hard- und Software verwendet werden.

5.4 Beweissicherheit

5.4.1 Konventionelle Computer-Forensik

Um elektronisch gespeicherte Daten auf Computersystemen als rechtskräftige Beweise verwenden zu können, sind eine Reihe technisch-organisatorischer Anforderungen umzusetzen. Hansen/Krause erläutern den Ablauf wie folgt:

In der Regel sind vier Schritte erforderlich:

1. Identifizierung
- Klärung, welche Informationen als Beweise erhoben werden sollen
- Festlegen der Vorgehensweise und der Mittel/Werkzeuge

2. Sicherstellung
- Sicherstellung der Zielrechner in Anwesenheit von Zeugen und ggf. Eigner
- ggf. Sicherstellung weiterer Dateninhalte aus flüchtigen Speichern vor der Abschaltung des Systems
- Sicherung der Datenträger gegen nachträgliche Veränderungen (z. B. Schreibschutz, kryptographische Verfahren zur digitalen Signatur)
- Erstellen einer Image-Kopie

3. Analyse
- die Analyse durch sachverständige Kriminaltechniker
- Analyse nie am Originalsystem sondern immer an der Kopie

4. Aufbereitung und Präsentation
- Zusammenfassung der Analyse in einem Bericht

5.4.2 Beweissicherheit der Online-Durchsuchung

Im Gegensatz zur konventionellen Computer-Forensik, die auf die garantierte Unverändertheit des Untersuchungsgegenstandes setzt, ist bei der Online-Durchsuchung die Veränderung des Untersuchungsgegenstandes - bedingt durch das Einbringen der RFS - die Voraussetzung für die Beweiserhebung. Schon diese Tatsache widerspricht allen Vorgaben der klassischen Computer-Forensik. Ob mit dem Start der RFS auf dem Zielsystem tatsächlich (weitere) Änderungen sicher ausge-

schlossen werden können (vgl. Punkt 3), kann kaum zweifelsfrei bewiesen werden. Damit ist auch der Beweiswert der erhobenen Daten äußerst fraglich.

Ob es darüber hinaus möglich ist, die zu untersuchenden Daten bei der Übertragung zum Server der Sicherheitsbehörde verlässlich vor Manipulation und Veränderung zu schützen, ist fraglich. Es dürfte kaum möglich sein, auf einem fremdkontrollierten Zielsystem (nämlich durch die Zielperson) verlässlich kryptographische Verfahren wie etwa die digitale Signatur durchzuführen.

Auch die angeblich lückenlose Protokollierung aller Aktivitäten und die Hinterlegung des Quellcodes der RFS (vgl. Punkt 4.2) kann nicht garantieren, dass Daten auf dem Zielsystem verändert werden - und sei es durch Software-Fehler in der RFS oder im Betriebssystem des Zielsystems.

Der Nutzen der Hinterlegung des Quellcodes ist ohnehin mehr als fragwürdig. Mit dieser Maßnahme will das BMI offenbar sicherstellen, dass der Quellcode im Bedarfsfall vollständig analysiert werden kann. Zieht man jedoch in Betracht, dass eine Quellcodeanalyse einen erheblichen Aufwand an Zeit und hochqualifiziertem Fachpersonal erfordert, wird eine solche Analyse wohl kaum vor dem Einsatz der Software angefordert werden. Vielmehr ist anzunehmen, dass lediglich eine nachträgliche Quellcode-Analyse angefordert wird, um bspw. in einem strafrechtlichen Verfahren die "ordnungsgemäße" Funktion der RFS beweisen zu können.

Doch selbst dieser Beweis muss unvollständig bleiben. Es ist davon auszugehen, dass der Vorgang der Online-Durchsuchung von den Sicherheitsbehörden von außen "gesteuert" wird. So wird beispielsweise die Möglichkeit bestehen, durch "Nachladen" von Softwarekomponenten im Laufe der Online-Durchsuchung die Originalsoftware zu verändern, um sie aktuellen Anforderungen entsprechend anpassen zu können (etwa Nachladen erweiterter Suchkriterien). Dass durch diese Maßnahme der Beweiswert des hinterlegten Quellcodes nichtig ist, versteht sich von selbst.

Der Beweiswert der mit der Online-Durchsuchung erhobenen Daten bleibt daher in jedem Fall äußerst fragwürdig.

5.5 Schutz des Kernbereichs der privaten Lebensgestaltung

Dass eine Online-Durchsuchung solche Bereiche unberücksichtigt lässt, die durch bestimmte Dateinamen oder Dateiendungen adressiert werden, ist kaum anzunehmen. Allein die Tatsache, dass eine Datei mit "Liebesbrief.doc" bezeichnet ist, wird sicher nicht dazu führen, dass Inhalte dieser Datei nicht an den Server der Sicherheitsbehörde übertragen werden.

Auch die Suche nach Eigenschaften/Attributen wird kaum zu Einschränkungen führen, weil eine verlässliche Schlussfolgerung auf Inhalte nicht möglich ist.

Ebenso ist die Suche nach Schlüsselworten, die Suche in bestimmten Verzeichnissen oder die Suche nach Dateien eines bestimmten Dateityps keine geeignete Methode, Daten aus dem Kernbereich der privaten Lebensgestaltung zu schützen.

Selbst wenn Erkennungsalgorithmen entwickelt werden könnten, in deren Ergebnis der Kernbereich definiert werden kann, wäre immer eine Durchsuchung des Gesamtdatenbestandes nötig, um entsprechende Indexierungen zu ermöglichen. Es ist somit kein technisches Verfahren erkennbar, mit dem ein "automatisierter Kernbereichsschutz" realisiert werden kann.

Das BMI räumt folgerichtig ein, dass "… der Schutz des Kernbereichs anderer Nutzer wie auch des Beschuldigten allein mit technischen Mitteln nicht abschließend garantiert werden kann …", und dieser Schutz nur im Rahmen der Auswertung der erhobenen Daten gewährleistet werden kann.

Im Ergebnis ist festzustellen, dass der Kernbereich der privaten Lebensgestaltung bei einer Online-Durchsuchung durch technische Mittel nicht angemessen geschützt werden kann.

Die Erklärungen des BMI und des BKA zur Zahl der zu erwartenden Online-Durchsuchungen (bisher wird von maximal zehn Maßnahmen pro Jahr gesprochen) darf nicht dazu führen, den Eingriff in den Kernbereich der privaten Lebensgestaltung zu verharmlosen und in der Folge die Online-Durchsuchung zu legitimieren. Selbst wenn die Online-Durchsuchung - angesichts geringer Fallzahlen - als angemessenes Mittel zur Terrorismus- bzw. Extremismusbekämpfung angesehen werden würde, darf nicht außer Acht bleiben, dass der technische Fortschritt sehr schnell dazu führen kann, dass die Online-Durchsuchung zu einem Standardwerkzeug der Sicherheitsbehörden werden kann. Dann wäre vor dem Hintergrund der jetzigen technischen Möglichkeiten ein Eingriffsinstrument legitimiert worden, das bei fortschreitender Technikentwicklung völlig unangemessen wäre.

Im Übrigen ist angesichts der künftig abnehmenden Anzahl der Festnetzanschlüsse und der zunehmenden Kommunikation per IP-Telefonie ohnehin zu hinterfragen, welche Fallzahlen künftig zu erwarten sind und ob die bisher vom BMI betonte Trennung der Online-Durchsuchung von der "Quellen-TKÜ" Bestand haben wird. Aus den Aussagen des BMI zum Problem der verschlüsselten Kommunikation wird deutlich, dass die mit der RFS verbundenen technischen Möglichkeiten die Grundlage darstellen sollen, um angesichts der technischen Entwicklungen (Konvergenz der Netze, Verschlüsselung, Vielfalt der Kommunikationsdienste) die Strafverfolgungsbehörden technisch nicht den Anschluss verlieren zu lassen und ihnen die Möglichkeiten zu erhalten, über die sie gegenwärtig bei der TKÜ verfügen.

5.6 Auswirkungen auf das Vertrauen in die IT-Infrastruktur und Folgen für die Akzeptanz von E-Government-Verfahren

IT-Sicherheit und Datenschutz sind die zentralen Akzeptanzkriterien der sich herausbildenden Informationsgesellschaft und der weltweiten Daten- und Kommunikationsnetze. Eine Folge der heimlichen Online-Durchsuchung wird eine tiefgreifende

Vertrauenskrise sein. Bürgerinnen und Bürger und möglicherweise auch Unternehmen werden nicht mehr bereit sein, staatliche E-Government-Angebote zu nutzen, da sie den Missbrauch dieser Verfahren für die Zwecke der Online-Durchsuchung befürchten.

So hat beispielsweise die Finanzverwaltung schon jetzt massive Bedenken geäußert, dass ihre Bemühungen um die breite Nutzung der elektronischen Steuererklärung (ELSTER) durch die Diskussionen um die Online-Durchsuchung konterkariert werden. Schon jetzt - vor dem Einsatz der Online-Durchsuchung - werden sinkende Nutzungszahlen erwartet.

Selbst die elektronische Kommunikation zwischen Bürgerinnen und Bürgern bzw. Unternehmen mit staatlichen Stellen per E-Mail wird künftig gemieden werden, weil das BMI nicht ausschließt, dass die RFS mittels E-Mails verbreitet wird.

Auch die elektronische Kommunikation mit der Wirtschaft wird in Mitleidenschaft gezogen werden. Wenn Kunden sich nicht mehr der Vertraulichkeit der elektronischen Kommunikation sicher sein können, werden sie wieder auf die konventionelle Kommunikationswege zurückgreifen. Sie werden dann möglicherweise auf Anwendungen wie Online-Banking und E-Commerce-Verfahren verzichten.

Zudem ist zu befürchten, dass etwa Personalcomputer nicht mehr auf dem aktuellen Sicherheitsstand gehalten werden. Aus Furcht vor infiltrierten Downloads könnten Nutzer beispielsweise auf die regelmäßigen Sicherheits-Updates verzichten. Dies wird zu einem Anstieg der Computerkriminalität führen, da Sicherheitslücken nicht mehr beseitigt werden.

Das BMI weist zwar darauf hin, dass so genannte Hintertüren nicht eingebaut werden sollen. Es ist jedoch - zumindest aus technischer Sicht - mit ziemlicher Sicherheit davon auszugehen, dass vorhandene Hintertüren und unveröffentlichte Sicherheitslücken genutzt werden. Insbesondere damit konterkariert das BMI jedoch die Beteuerungen der Bundesregierung, den Bürgern und der Wirtschaft eine sichere und vertrauenswürdige IT-Infrastruktur zur Verfügung zu stellen. Es ist nämlich zu befürchten, dass (evtl. zunächst nur) dem BMI bekannte Sicherheitslücken nicht so schnell wie möglich publiziert werden, damit Schutzmaßnahmen ergriffen werden können, sondern dass diese Lücken bewusst über längere Zeit offen gehalten werden, um sie für die Zwecke der Online-Durchsuchung zu nutzen. Damit kann insbesondere der Wirtschaft erheblicher Schaden zugefügt werden (Stichwort Computer-Spionage). Die Wahrscheinlichkeit ist nämlich sehr hoch, dass das BMI gerade nicht exklusive "Nutzungsrechte" an solchen Sicherheitslücken hat.

Fraglich ist in diesem Zusammenhang auch, welche Rolle das Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig spielen soll bzw. noch spielen kann. Das BMI weist zwar ausdrücklich darauf hin, dass das BSI angewiesen wurde, sich nicht aktiv an der Entwicklung der für die Online-Durchsuchung einzusetzenden Software zu beteiligen. Ob das BMI tatsächlich dauerhaft auf den Sachverstand des BSI verzichten wird, darf zumindest bezweifelt werden. Das Vertrauen in das BSI als glaubwürdigem Berater in Fragen der IT-Sicherheit ist schon jetzt sowohl in der Wirtschaft als auch bei Bürgern nachhaltig beeinträchtigt.

Schließlich darf nicht außer Acht gelassen werden, dass auch Kriminelle das Verfahren der Online-Durchsuchung oder zumindest bewusst in Kauf genommene Sicherheitslücken nutzen werden. Die Tatsache, dass Sicherheitsbehörden beharrlich davon ausgehen, dass die Online-Durchsuchung technisch durchführbar ist, wird Kriminelle in zunehmendem Maße veranlassen, sich diese Methode für ihre Zwecke nutzbar zu machen. Selbst wenn die Online-Durchsuchung für Sicherheitsbehörden nicht verwendet werden dürfte - etwa infolge einer Entscheidung des BVerfG - ist selbstverständlich davon auszugehen, dass Kriminelle alle technischen Möglichkeiten künftig nutzen werden.

Schon allein dieser Aspekt verdeutlicht, wie wichtig es künftig sein wird, alle Nutzer von Informations- und Kommunikationstechnik weiter zu sensibilisieren. Es ist auch Aufgabe der Datenschutzbeauftragten des Bundes und der Länder, sowohl die Verantwortlichen in Wirtschaft und Verwaltung als auch Bürgerinnen und Bürger zu informieren und zu beraten, um auch dadurch ein höheres Sicherheitsbewusstsein zu erreichen.