18. Wahlperiode

Drucksache **18/2027**

HESSISCHER LANDTAG

09. 03. 2010

Achtunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2009
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 9. März 2010 · Ausgegeben am 15. März 2010
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 38. Tätigkeitsbericht

Register der Rechtsvorschriften zum 38. Tätigkeitsbericht

Kernpunkte

Abkürzungsverzeichnis zum 38. Tätigkeitsbericht

a.a.O.	am angegebenen Ort
a.F.	alte Fassung
AbfG	Abfallgesetz
ABl.	Amtsblatt des Hessischen Kultusministeriums
Abs.	Absatz
AES	Advanced Electronic Signature (fortgeschrittene elektronische Signatur)
A-eSig	Aktionsplan für elektronische Signaturen und die elektronische Identifizierung zur Förderung grenzübergreifender öffentlicher Dienste im Binnenmarkt
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Arbeitsgruppe
AK	Arbeitskreis
allg.	allgemein
AO	Abgabenordnung
ARD	Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
ARGE	Arbeitsgemeinschaften
Art.	Artikel
AU	Abgasuntersuchung
AuslG	Ausländergesetz
awk	Skriptsprache benannt nach den Entwicklern Aho, Weinberger, Kernighan
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
Beck RS	Beck-Rechtsprechung
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des BGH in Zivilsachen (amtl. Sammlung)
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern
BRDrucks.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BVerfG	Bundesverfassungsgericht
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Sammlung der Entscheidungen des Bundesverwaltungsgerichts
bzgl.	bezüglich
CA	Certificate Authority (Zertifizierungsinstanz)
CC	Common Criteria (Gemeinsame Kriterien)
CD	Compact Disc (Speichermedium)
CDU	Christlich Demokratische Union
CRIME	Criminal Research Investigation Management (bei der hessischen Polizei eingesetzte Software)
CSV	Comma-Separated Values (Dateiformat)
d.h.	das heißt
d.J.	dieses Jahres
DEKRA	Deutscher Kraftfahrzeug-Überwachungs-Verein
DIN	Deutsche Industrie-Norm(en)
DMP	Disease-Management-Programm
DMZ	demilitarisierte Zone
DÖV	Die Öffentliche Verwaltung
Drucks.	Drucksache
DSG M-V	Datenschutzgesetz Mecklenburg-Vorpommern
DVBl.	Deutsches Verwaltungsblatt
DVD	Digital Versatile Disc
e.V.	eingetragener Verein
ebd.	ebenda
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
ELSTER	Elektronische Steuererklärung
EnWG	Energiewirtschaftsgesetz
EPA	elektronische Patientenakte
ePR	elektronisches Personenstandsregister

EU	Europäische Union
EuGH	Europäischer Gerichtshof
EURODAC	Europäisches Fingerabdrucksystem (Zusammensetzung aus Européen und Dactyloscopie)
EU-SRL	EU-Signaturrichtlinie
EUV	Vertrag über die Europäische Union
EVG	Evaluationsgegenstand
evtl.	eventuell
Fa.	Firma
FAR	False Acceptance Rate
FDP	Freie Demokratische Partei
ff.	fortfolgende/r/s
ForstG	Forstgesetz
FRR	False Rejection Rate
FTE	Failure To Enrol rate
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
ggf.	gegebenenfalls
GK	Gemeinsame Kontrollinstanz
grds.	grundsätzlich
grep	unter Unix verfügbares Editierprogramm Global/Regular-Expression/Print
GVBl.	Gesetz- und Verordnungsblatt für das Land Hessen
HARIS	Hessisches Analyse- und Recherchesystem
HBA	Heilberufeausweis
HBG	Hessisches Beamtengesetz
HBKG	Hessisches Brand- und Katastrophenschutzgesetz
HDSG	Hessisches Datenschutzgesetz
HENatG	Hessisches Gesetz über Naturschutz und Landschaftspflege
HEPIS	Hessisches Personalinformationssystem (Software)
HGöGD	Hessisches Gesetz über den öffentlichen Gesundheitsdienst
HKHG	Hessisches Krankenhausgesetz
HKM	Hessisches Kultusministerium
HKVZ	Hessisches Kindervorsorgezentrum
HLFV	Hessisches Landesamt für Verfassungsschutz
HMAFG	Hessisches Ministerium für Arbeit, Familie und Gesundheit
HMDIS	Hessisches Ministerium des Innern und für Sport
HMDJ	Hessisches Ministerium der Justiz, für Integration und Europa
HMG	Hessisches Meldegesetz
HPVG	Hessisches Personalvertretungsgesetz
HR	Hessischer Rundfunk
Hrsg.	Herausgeber
HSchulG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HU	Hauptuntersuchung
HWG	Hessisches Wassergesetz
HZD	Hessische Zentrale für Datenverarbeitung
i.d.F.	in der Fassung
i.S.d.	im Sinne des/der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
inkl.	inklusive
IP	Internet Protocol
ISO	Internationale Standardisierungsorganisation
IT	Informationstechnik
IuK	Information und Kommunikation
JGG	Jugendgerichtsgesetz
JGH	Jugendgerichtshilfe
JuVZ	Justiz- und Verwaltungszentrum
JZ	JuristenZeitung
KfH	Kuratorium für Dialyse und Nierentransplantation e.V.
Kfz	Kraftfahrzeug
KIS	Krankenhausinformationssystem
KV Hessen	Kassenärztliche Vereinigung Hessen
LÄK	Landesärztekammer
LARGO	Phantasiename für Datenverarbeitungssystem beim Landesamt für Verfassungsschutz
LDSG S-H	Landesdatenschutzgesetz Schleswig-Holstein
LTDrucks.	Landtagsdrucksache
LuftVG	Luftverkehrsgesetz

m.E.	meines Erachtens
MAC	Media Access Control
MDK	Medizinischer Dienst der Krankenversicherung
MeldDÜVO	Meldedatenübermittlungsverordnung
Mio	Million(en)
MVZ	Medizinisches Versorgungszentrum
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NStz-RR	Rechtsprechungs-Report Strafrecht
o.Ä.	oder Ähnliches
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
ÖPNV	Öffentlicher Personennahverkehr
OSCI	Online Services Computer Interface
OVG	Oberverwaltungsgericht
PC	Personalcomputer
PID	Personal Identifier
PKI	Public Key Infrastruktur
PP	Protection Profiles (Schutzprofile)
PSN	Pseudonym
PStG	Personenstandsgesetz
PStV	Verordnung zur Ausführung des Personenstandsgesetzes
QC	qualified certificate (qualifiziertes Zertifikat)
QES	qualifizierte elektronische Signatur
RA	Registration Authority
RGebStV	Rundfunkgebührenstaatsvertrag
RP	Regierungspräsidium
s.	siehe
S.	Seite
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SigV	Signaturverordnung
SIS	Schengener Informationssystem
SoPart	Bezeichnung einer Software für soziale Dienste der Justiz
SP	Sicherheitsprüfung
SPNV	Schienenpersonennahverkehr
SSCD	Secure Signature Creation Device (sichere Signaturerstellungseinheit)
SSL	Secure Socket Layer
StA	Staatsanwalt(schaft)
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrszulassungsordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication (Genossenschaft der Geldinstitute)
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung an Informationstechnischen Systemen
TMF	Telematikplattform für Medizinische Forschungsnetze
TMG	Telemediengesetz
u.a.	unter anderem
UDP	User Datagram Protocol
USB	Universal Serial Bus (Schnittstelle bei Geräten)
USB-Stick	Speichermedium mit USB-Schnittstelle
UWG	Gesetz gegen den unlauteren Wettbewerb
VerfSchG	Verfassungsschutzgesetz
VerwArch	Verwaltungsarchiv
VoIP	Voice over IP (Voice over Internet Protocol)
VPN	virtual private network
VwVfG	Verwaltungsverfahrensgesetz
WDR	Westdeutscher Rundfunk
WORM-Medien	einmal beschriebene Speichermedien
WTS	Windows Terminal Server
z.B.	zum Beispiel
ZDA	Zertifizierungsdiensteanbieter
ZDF	Zweites Deutsches Fernsehen
Ziff.	Ziffer

Register der Rechtsvorschriften zum 38. Tätigkeitsbericht

AbfG	Gesetz zur Förderung der Kreislaufwirtschaft und Sicherung der umweltverträglichen Beseitigung von Abfällen (Kreislaufwirtschafts- und Abfallgesetz) vom 27. Sept. 1994 (BGBl. I S. 2705), zuletzt geändert durch Art. 3 des Gesetzes vom 11. Aug. 2009 (BGBl. I S. 2723)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union i.d.F. des Vertrags von Lissabon vom 13. Dez. 2007 (ABlEG 2007/C 306/1)
AO	Abgabenordnung 1977 i.d.F. vom 1. Okt. 2002 (BGBl. I S. 3866), zuletzt geändert durch Art. 2 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2474)
BBG	Bundesbeamtengesetz i.d.F. vom 5. Feb. 2009 (BGBl. I S. 160)
BDSG	Bundesdatenschutzgesetz i.d.F. der Bekanntmachung vom 14. Jan. 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 29. Juli 2009 (BGBl. I S. 2254), durch Art. 5 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2355, 2384) und durch Gesetz vom 14. Aug. 2009 (BGBl. I S. 2814)
BGB	Bürgerliches Gesetzbuch i.d.F. vom 2. Jan. 2002 (BGBl. I S. 42; 2003 I S. 738), zuletzt geändert durch Gesetz vom 28. Sept. 2009 (BGBl. I S. 3161)
EG-Beschluss 2009/371	Beschluss des Rates der Europäischen Union zur Errichtung des Europäischen Polizeiamts (Europol) vom 6. Apr. 2009 (ABlEG 2009/L 121/37)
EG-Richtlinie 1999/93	Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (EU-Signaturrichtlinie) vom 13. Dez. 1999 (ABlEG 2000/L13/12)
EG-Richtlinie Nr. 2002/58 bzw. Nr. 2006/24	Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2002 (Datenschutz-Richtlinie für elektronische Kommunikation; ABlEG 2002/L 201/27), geändert durch die Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden vom 15. März 2006 (ABlEG 2006/L 105/54)
EG-Richtlinie 2006/123	Richtlinie des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt (EU-Europäische Dienstleistungsrichtlinie) vom 12. Dez. 2006 (ABlEG 2006/L 376/36)
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz) vom 7. Juli 2005 (BGBl. I S. 3621), zuletzt geändert durch Art. 2 des Gesetzes vom 21. Aug. 2009 (BGBl. I S. 2870)
EU-Vertrag	Vertrag über die Europäische Union vom 25. März 1957 (Rom; ABlEG 2002/C 325/33), i.d.F. des Vertrags von Maastricht vom 7. Feb. 1992 (ABlEG 1992/C 191/1) i.d.F. des Vertrags von Amsterdam vom 2. Okt. 1997 (ABlEG 1997/C 340/1) i.d.F. des Vertrags von Nizza vom 26. Feb. 2001

	(ABlEG 2001/C 80/1) i.d.F. des Vertrags von Lissabon vom 13. Dez. 2007 (ABlEG 2007/C 306/1)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. I S. 1), zuletzt geändert durch Art. 1 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2248)
HBG	Hessisches Beamtengesetz i.d.F. vom 11. Jan. 1989 (GVBl. I S. 25), zuletzt geändert durch Art. 1 des Gesetzes vom 5. März 2009 (GVBl. I S. 95)
HBKG	Hessisches Gesetz über den Brandschutz, die Allgemeine Hilfe und den Katastrophenschutz (Hessisches Brand- und Katastrophenschutzgesetz) vom 17. Dez. 1998 (GVBl. I S. 530), zuletzt geändert durch Art. 1 des Gesetzes vom 18.11.2009 (GVBl. I S. 423)
HDSG	Hessisches Datenschutzgesetz i.d.F. vom 7 Jan. 1999 (GVBl. I S. 98)
HENatG	Hessisches Gesetz über Naturschutz und Landschaftspflege (Hessisches Naturschutzgesetz) i.d.F. vom 4. Dez. 2006 (GVBl. I S. 619), zuletzt geändert durch Gesetz vom 12. Dez. 2007 (GVBl. I S. 851)
HGB	Handelsgesetzbuch vom 10. Mai 1879 (RBBl. S. 219 - BGBl. III/FNA 4100-1), zuletzt geändert durch Gesetz vom 25. Mai 2009 (BGBl. IS. 1102)
HGöGD	Hessisches Gesetz über den öffentlichen Gesundheitsdienst (HGöGD) vom 28. Sept. 2007 (GVBl. I S. 659)
HKHG	Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2002) vom 6. Nov. 2002 (GVBl. I S. 662), zuletzt geändert durch Art. 2 des Gesetzes vom 19. Nov. 2008 (GVBl. I S. 986)
HMG	Hessisches Meldegesetz i.d.F. vom 10. März 2006 (GVBl. I S. 66)
HSchulG	Hessisches Schulgesetz i.d.F. 14. Juni 2005 (GVBl. I S. 442), zuletzt geändert durch Gesetz vom 14. Juli 2009 (GVBl. I S. 265)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i.d.F. vom 14. Jan. 2005 (GVBl. I S. 442), zuletzt geändert durch Gesetz vom 14. Dez. 2009 (GVBl. I S. 635)
HWG	Hessisches Wassergesetz i.d.F. vom 6. Mai 2005 (GVBl. I S. 305), zuletzt geändert durch Art. 1 des Gesetzes vom 19. Nov. 2007 (GVBl. I S. 792)
JGG	Jugendgerichtsgesetz i.d.F vom 11. Dez. 1974 (BGBl. I S. 3427), zuletzt geändert durch Art. 7 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2280)
Kindergesundheitsschutzgesetz	Hessisches Gesetz zur Verbesserung des Gesundheitsschutzes für Kinder vom 14. Dez. 2007 (GVBl. I S. 856)

RGebStV	Rundfunkgebührenstaatsvertrag, ratifiziert durch Gesetz zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland vom 13. Dez. 1991 (GVBl. I S. 367), zuletzt geändert durch Art. 6 Zwölfter Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge, ratifiziert durch Gesetz vom 4. März 2009 (GVBl. I S. 58)
SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 19. Juni 1990 - Schengener Durchführungsübereinkommen (GVBl. 1993 II S. 1010), zuletzt geändert durch EG-Verordnung Nr. 1931 des Europäischen Parlaments und des Rates vom 20. Dez. 2006 (ABlEG 2006/L 405/1)
SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dez. 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes vom 28. März 2009 (BGBl. I S. 634)
SGB II	Zweites Buch Sozialgesetzbuch - Grundsicherung für Arbeitssuchende - vom 24. Dez. 2003 (BGBl. I S. 2954), zuletzt geändert durch Art. 14b des Gesetzes vom 17. Juli 2009 (BGBl. I S. 1990)
SGB V	Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung - vom 20. Dez. 1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 3 des Gesetzes vom 17. März 2009 (BGBl. I S. 534)
SGB VII	Siebtes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung - i.d.F. vom 7. Aug. 1996 (BGBl. I S. 1254), zuletzt geändert Art. 15 Abs. 98 des Gesetzes vom 5. Feb. 2009 (BGBl. I S. 160)
SGB VIII	Achtes Buch Sozialgesetzbuch - Kinder und Jugendhilfe - i.d.F. vom 8. Dez. 1998 (BGBl. I S. 3546), zuletzt geändert durch Art. 105 des Gesetzes vom 17. Dez. 2008 (BGBl. I S. 2586)
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - i.d.F. vom 18. Jan. 2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 3. April 2009 (BGBl. I S. 700)
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)
SigV	Verordnung zur elektronischen Signatur (Signaturverordnung) vom 16. Nov. 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 17. Dez. 2009 (BGBl. I S. 3932)
StPO	Strafprozessordnung i.d.F. der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437)
StVG	Straßenverkehrsgesetz i.d.F. vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 3 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2507)

StVZO	Straßenverkehrs-Zulassungs-Ordnung i.d.F. der Bekanntmachung vom 28. Sept. 1988 (BGBl. I S. 1793), zuletzt geändert durch 31. Verordnung zur Änderung der Straßenverkehrs-Zulassungs-Ordnung vom 26. Mai 2008 (BGBl. I S. 916)
UWG	Gesetz gegen den unlauteren Wettbewerb vom 3. Juli 2004 (BGBl. I S. 1414), zuletzt geändert Art. 2 des Gesetzes vom 29. Juli 2009 (GVBl. I S. 2413)
VerfSchG	Gesetz über das Landesamt für Verfassungsschutz vom 19. Dez. 1990, zuletzt geändert durch das Hessische Sicherheitsüberprüfungsgesetz vom 28. Sept. 2007 (GVBl. I S. 623)
VwVfG	Verwaltungsverfahrensgesetz vom 23. Jan. 2003 (BGBl. I S. 102), zuletzt geändert durch Art. 2 des Gesetzes vom 14. Aug. 2009 (BGBl. I S. 2827)

Kernpunkte

1. Entgegen der Rechtsprechung des Bundesverfassungsgerichts, das dem voraussetzungslosen Anspruch der Betroffenen auf Auskunft über ihre personenbezogenen Daten zentrale Bedeutung für den Grundrechtsschutz beimisst, hat das Bundesministerium der Finanzen die Finanzverwaltungen in einem Erlass angewiesen, Auskunftsansprüche Betroffener nur zu erfüllen, wenn diese ein berechtigtes Interesse nachweisen (Ziff. 3.2).

2. Bildaufnahmen werden zu vielfältigen Zwecken verwendet. Ihre Zulässigkeit hängt von den jeweiligen tatsächlichen und rechtlichen Gegebenheiten ab. Der verdeckte Einsatz von Minikameras anlässlich der Räumung des Camps von Flughafenausbaugegnern im Kelsterbacher Wald war danach unzulässig (Ziff. 4.1.1). Beim Einsatz von Videotechnik zu Planungszwecken und zur Verkehrsüberwachung sind besondere Anforderungen zu beachten (Ziff. 4.1.2 und Ziff. 4.1.3).

3. Nachdem das Bundesverfassungsgericht die Regelungen des HSOG zur Kennzeichenerfassung für nichtig erklärt und die Anforderungen an die Rasterfahndung beanstandet hatte, musste das Gesetz novelliert werden. Dabei war auch die Rechtsprechung zum Schutz des Kernbereichs privater Lebensgestaltung umzusetzen. Die im Dezember verabschiedete Novelle trägt den verfassungsrechtlichen Vorgaben nicht allen Punkten Rechnung (Ziff. 4.2.1).

4. Als Folge der Verabschiedung der neuen Verordnung zur Datenverarbeitung in Schulen (Ziff. 4.5.1) habe ich meine Schulbroschüre überarbeitet und den neuen Rechtsgrundlagen angepasst (Ziff. 4.5.3). Sie enthält die wesentlichen Informationen über die Datenverarbeitung in Schulen. Schulen müssen den Datenschutz auch bei Veröffentlichung von Informationen für Schülerinnen und Schüler, Lehrerinnen und Lehrer, sowie Eltern unter Nutzung sog. digitaler schwarzer Bretter oder der Schul-Homepage beachten (Ziff. 4.5.2).

5. Der Aufbau elektronischer Patientenakten in den Krankenhäusern erfordert eine differenzierte Ausgestaltung der Zugriffsmöglichkeiten durch das Personal. Patientinnen und Patienten rechnen nicht damit und müssen auch nicht damit rechnen, dass jede Mitarbeiterin und jeder Mitarbeiter im Krankenhaus ihre Krankendaten zur Kenntnis nehmen kann. Bei der Umsetzung der datenschutzrechtlichen Vorgaben sind in Hessen wie auch bundesweit Defizite bekannt geworden. Sowohl Krankenhäuser als auch Softwarehersteller sind gefordert, den Datenschutz zu verbessern (Ziff. 4.6.2).

6. Für das praktizierte heimliche Einschalten von Dritten zur Erhebung und Bewertung des Führungsverhaltens Beschäftigter ist eine Rechtsgrundlage nicht ersichtlich. Da für die Verarbeitung von Personaldaten jedoch eine Rechtsgrundlage erforderlich ist, liegt ein grober Datenschutzverstoß vor (Ziff. 4.8.1).

7. Der Einsatz von SAP R/3 HR in der Landesverwaltung ist nunmehr umgehend datenschutzgerecht zu gestalten. Dazu gehört die Umsetzung der gesetzlichen Löschfristen ebenso wie die technische Sicherstellung, dass nur im Umfang der erteilen Berechtigungen auf die Personaldaten zugegriffen werden kann und Zugriffe protokolliert werden (Ziff. 4.8.3, 4.8.4).

8. Die Aufgaben der Feuerwehr machen die Verarbeitung vielfältiger personenbezogener Daten erforderlich, die jeweils verschiedenen Akteuren an verschiedenen Orten zur Verfügung stehen müssen. Datenschutzrechtlich dürfen die Eingriffsbefugnisse gleichwohl nicht vermengt werden. Die IT-Unterstützung muss deshalb unterschiedlichste Anforderungen berücksichtigen, wie die exakte Abbildung der Zugriffsberechtigungen getrennt nach Akteuren und Funktionen, die besondere Behandlung der Daten von Feuerwehrvereinen sowie die Bedingungen für die Nutzung am heimischen PC (Ziff. 5.7.1 und 7.2.1.4). Gesundheitsdaten, die während Feuerwehrübungen erhoben werden, dürfen nicht über die Übung hinaus gespeichert werden (Ziff. 5.7.2).

9. Das Projekt HessenVoice verfolgt das Ziel, für die Hessische Landesverwaltung eine zukunftssichere zentrale Telekommunikationsstruktur mit der Technik "Voice over IP" aufzubauen. Dabei sind Datenschutzaspekte zu berücksichtigen, die bei einem künftigen flächendeckenden Einsatz grundsätzlich auch eine Verschlüsselung erfordern (Ziff. 7.1).

10. Bei der Suche nach sicheren und kostengünstigen Lösungen der ortsungebundenen Datenverarbeitung sind vielfältige Szenarien zu betrachten. USB-Sticks können - richtig eingesetzt - dabei helfen, Datenschutzanforderungen umzusetzen (Ziff. 7.2).

11. Die datenschutzgerechte, für die Nutzenden transparente und rechtssichere elektronische Kommunikation erfordert die strikte Trennung der Funktionen der Authentisierung und der elektronischen Signatur. Auch in Normen und Standards (wie z.B. der Common PKI) muss die Trennung der Funktionen und eine zutreffende klare Bezeichnung in den Zertifikaten vorgeschrieben werden (Ziff. 7.3). Ausschließlich die qualifizierte, nicht aber eine hinter der qualifizierten zurückbleibende fortgeschrittene Signatur eignet sich als elektronisches Äquivalent zur Schriftform. Eine Dokumentsignatur muss wie die Unterschrift ab dem Zeitpunkt der Erstellung unbefristet gelten. Die Landesregierung ist aufgefordert sich dafür einzusetzen, diese Grundsätze auch für den im Aktionsplan der EU-Kommission geplanten europäischen Signaturstandard durchzusetzen (Ziff. 7.4).

1. Einführung

1.1 Allgemeines

In den vorangegangenen Tätigkeitsberichten wurde die Konzeption der informationellen Selbstbestimmung erörtert. Diese Konzeption wurde u.a. von Ladeuer (Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion, DÖV 2009, 45 ff.) und wohl auch Bull (Informationelle Selbstbestimmung Vision oder Illusion, Tübingen, 2009) missverstanden. Daher wird anschließend die Konzeption aus der Sicht des Hessischen Datenschutzbeauftragten noch einmal dargestellt:

1.2 Persönlichkeitsrecht

Der grundrechtliche Datenschutz ist Ausprägung des in der Verfassung verankerten Persönlichkeitsrechts, das neben besonders geregelten Garantien (Art. 10 Abs. 1, Art. 13 Abs. 1 GG) Ausdruck fand im Grundrecht auf informationelle Selbstbestimmung sowie im Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

1.2.1 Werteordnung des Grundgesetzes

Das Grundgesetz ist nicht nur ein Katalog zeitbedingter politischer Zielvorgaben, sondern eine Kodifikation und bildet damit ein System, das aus sich selbst heraus ergänzt werden kann (Werteordnung des Grundgesetzes). Auf der Grundlage dieser Werteordnung erfolgt der gebotene Ausgleich zwischen privaten Freiheitspositionen, sonstigen Grundrechten und staatlichen Eingriffsbefugnissen. Der Ausgleich findet seinen Niederschlag in der Konkretisierung des grundrechtlichen Schutzbereichs und der Formulierung von Schranken, die der Gesetzgeber in Bund und Land, unter Kontrolle durch die Verfassungsgerichtsbarkeit vorzunehmen hat. Im System der Grundrechte ist von der grundsätzlichen Freiheit als Regel und den staatlichen Eingriffsmöglichkeiten als Ausnahme auszugehen. Die Freiheitsrechte bestehen auch dort, wo sie nicht ausdrücklich genannt sind. Es gibt benannte und unbenannte, starke und schwache, schwer und leicht beschränkbare Grundrechte. Maßgeblich ist nicht allein der Gegensatz zwischen speziellen benannten Freiheitsrechten und der allgemeinen Handlungsfreiheit als Auffanggrundrecht. Die unbeschränkbare Menschenwürde auf der einen und die mit plausibler Begründung gesetzgeberisch beschränkbare allgemeine Handlungsfreiheit auf der anderen Seite sind vielmehr Eckpunkte auf einer Skala mit ansteigendem Schutzgehalt: Je mehr sich ein Eingriff der Menschenwürde nähert, desto eher stößt er auf den unbeschränkbaren Kernbereich privater Lebensgestaltung. Je mehr die öffentliche Sphäre der Lebensgestaltung betroffen ist, desto leichter werden die Beschränkungsmöglichkeiten. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts, die schon vor dem Volkszählungsurteil einsetzte, ist der Kernbereich privater Lebensgestaltung absolut geschützt (BVerfGE 6, 32, 41; Beschluss vom 16. Juli 1969 - 1 BvL 19/63, BVerfG Urteil vom 16. Januar 1957 - 1 BvR 253/56 –, BVerfGE 6, 32, 41, BVerfGE 27, 1, 6; vom 15. Januar 1970 - 1BvR 13/68, BVerfGE 27, 344, 350; zuletzt Beschluss vom 10. Juni 2009 - 1 BvR 1107/09, NJW 2009, 3357, 3559). Die allgemeine Handlungsfreiheit reicht demgegenüber nur soweit wie ihre Nutzung nicht gegen die verfassungsmäßige Rechtsordnung verstößt, zu der alle formell und materiell verfassungsmäßigen Gesetze zählen (BVerfG Urteil vom 4. Juli 2000, - 1 BvR 2014/95 –, BVerfGE 103, 197, 205).

1.2.2 Informationelle Selbstbestimmung

Im Urteil vom 15. Dezember 1983 kreierte das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung, das die Befugnis des Einzelnen gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (1 BvR 209, 269, 342, 420, 440, 484/83 –, BVerfGE 65,1 43; ferner BVerfG Beschluss vom 9. März 1988 - 1 BvL 49/8, BVerfGE 78, 77, 84; Beschluss vom 11. Juni 1991 - 1 BvR 239/90 –, BVerfGE 84, 192, 194; Beschluss vom 12. April 2005 - 2 BvR 1027/32 -, 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 –, BVerfGE 117, 202; Beschluss vom 13. Juni 2007 - 1 BvR 1550/03, 2357/04, 603/05, BVerfGE 118, 168; Urteil vom 27. Februar 2008 - 1 BvR 370, 595/07 –, BVerfGE 120, 274, 312; Urteil vom 11. März 2008 - 1 BvR 2074/05, 1254/07 –, BVerfGE 120, 378, 397 ff.; BVerwG Urteil vom 30. April 2008 - 3 C 16.07; BGH Urteil vom 1. März 2007 - IX ZR 189/05 –, BGHZ 171, 252 , 256; BGH Urteil vom 23. Juni 2009 - VI ZR 196/08 - NJW 2009, 2888, 2891). Da ein derartiges Grundrecht im Grundgesetz nicht ausdrücklich genannt ist, hätte das Bundesverfassungsgericht allein auf die allgemeine Handlungsfreiheit zurückgreifen können. Es stützte jedoch das Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Schon vorher hatte das Bundesverfassungsgericht ein Grundrecht auf Privatheit anerkannt und zur Begründung die genannten Bestimmungen herangezogen. Das Grundrecht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Der Einzelne muss jedoch nur solche Beschränkungen hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. Die Anforderungen an die Ermächtigungsgrundlage richten sich nach der Art und Intensität des Grundrechtseingriffs (BVerfGE 120, 378, 401).

1.2.3 Vertraulichkeit und Integrität informationstechnischer Systeme

Das allgemeine Persönlichkeitsrecht aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG erfuhr in der Entscheidung des Bundesverfassungsgerichts vom 27. Februar 2008 (BVerfGE 120, 274) eine weitere besondere Ausprägung als Grundrecht auf Gewährleitung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses Grundrecht schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder 13 GG sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist. Auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Der Einzelne muss jedoch nur solche Beschränkungen seines Rechts hinnehmen, die auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen (BVerfGE 120, 274, 315).

1.3 Datenschutz

1.3.1 Datenschutzrecht

Das allgemeine Persönlichkeitsrecht in seinen Ausprägungen als Recht auf informationelle Selbstbebestimmung und als Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist der Einschränkung im überwiegenden Allgemeininteresse zugänglich. Die Einschränkung kann dann aber nur auf einer gesetzlichen Grundlage erfolgen, die dem Gebot der Normenklarheit entspricht und verhältnismäßig ist. Der Datenschutz ist dabei eine Querschnittsmaterie. Seine Rechtsgrundlagen ergeben sich aus dem allgemeinen und bereichsspezifischen Datenschutzrecht. Die Belange des Datenschutzes sind im jeweiligen Sachzusammenhang mit konträren Belangen Einzelner oder der Allgemeinheit abzuwägen (vgl. Ronellenfitsch, Freiheit, Sicherheit und Datenschutz im Rechtsstaat, in: Festschrift für Seok, 2009, S. 95 ff.). Das bedeutet, dass das Abwägungsmaterial ermittelt, bewertet und sodann gewogen werden muss. Bei der Abwägung sind zwingende Abwägungsvorgaben zu beachten, vom Gesetzgeber besonders hervorgehobene Belange zu optimieren und andere Belange jedenfalls zu berücksichtigen. Zur Orientierung hat der Gesetzgeber Datenschutzgrundsätze normiert, die immer zu beachten sind und konkretisiertes Verfassungsrecht darstellen.

1.3.2 Datenschutzgrundsätze

Bei der Abwägung von Datenschutzbelangen ist auszugehen vom repressiven Verbot der Erhebung, Verarbeitung und Übermittlung personenbezogener Daten, das nur durch eine gesetzliche Ermächtigung oder durch die Zustimmung der Betroffenen aufgehoben werden kann (repressives Verbot mit Zulassungsvorbehalt). Regel ist der Schutz der Privatsphäre, Ausnahme der Eingriff. Während der Staat sich zumeist auf gesetzliche Eingriffsermächtigungen berufen kann, ist im privaten Bereich häufig eine Einwilligung des Betroffenen erforderlich. Die Einwilligung muss freiwillig gegeben werden, spezifisch sein (sich auf einen bestimmten Zweck beziehen), den tatsächlichen Willen der Betroffenen ausdrücken und in voller Kenntnis der Sachlage ohne jeden Zweifel gegeben werden. Aus dem Regel-Ausnahmeverhältnis folgt der Zweckbindungsgrundsatz. Der Grundsatz besagt, dass personenbezogene Daten nur für eindeutig festgelegte rechtmäßige Zwecke erhoben und vor allem nur diesem Zweck entsprechend weiterverarbeitet werden dürfen. Der Grundsatz der Zweckbestimmung setzt sich fort im Grundsatz der zweckgebundenen Aufbewahrung. Länger als es für die Realisierung der legitimierenden Zwecke geboten ist, dürfen personenbezogene Daten nicht aufbewahrt oder verarbeitet werden. Aus dem Regel-Ausnahme-Verhältnis folgt weiter der Transparenzgrundsatz. Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden. Für mobile personenbezogene Speicher- und Verarbeitungsmedien, präzisiert § 8 Abs. 2 HDSG den Transparenzgrundsatz. Danach müssen Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, für die Betroffenen eindeutig erkennbar sein. Spezifische Bedeutung als Datenschutzgrundsatz hat der Grundsatz der Erforderlichkeit. Die Erforderlichkeit ist im Datenschutzrecht noch rigider als das allgemeine Übermaßverbot. Die Erhebung, Verarbeitung und Übermittlung personenbezogener Daten ist nur zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der Daten verarbeitenden Stelle für den jeweils damit verbundenen Zweck erforderlich ist. Hinzu kommt, dass bei der automatisierten Verarbeitung personenbezogener Daten das Verfahren auszuwählen oder zu entwickeln ist, das die zur Zweckerreichung nötige Menge personenbezogener Daten so gering wie möglich hält. Unzulässig ist vor allem die (zweckfreie) Vorratsdatenspeicherung. Ein weiterer Datenschutzgrundsatz ist somit der Grundsatz der Datenverminderung und Datensparsamkeit, der letztlich eine Konkretisierung des Erforderlichkeitsgrundsatzes darstellt und für alle Daten verarbeitenden Stellen gilt.

1.3.3 Einfachgesetzliche Ausgestaltung des Datenschutzes

Das Hessische Datenschutzgesetz vom 7. Oktober 1970 (GVBl. I S. 625) war das "Pionierwerk" des deutschen Datenschutzrechts. Es stamme aus einer Zeit, in der wenige Daten aus begrenzten Lebensbereichen formularmäßig erfasst und in Rechenzentren mit Großrechnern in erster Linie für Verwaltungszwecke verarbeitet wurden. Dadurch entstanden Ängste vor dem "großen Bruder". Inzwischen ist mit der Einführung von Personalcomputern und dem Internet eine völlig andere Situation eingetreten. Die Möglichkeiten privater Datenverarbeitung haben nicht nur Informationsansprüche entstehen lassen. Aus dem großen Bruder ist vielmehr zugleich eine Vielzahl bedrohlicher kleiner Brüder und Schwestern geworden. Der öffentliche und private Bereich gehen ineinander über. Der zeitgemäße Datenschutz lässt sich nur noch mehrdimensional begreifen. Eine Modernisierung des Datenschutzrechts aus einem Guss erscheint dringend geboten. Dabei ist den gemeinschafts- und verfassungsrechtlichen Vorgaben hinsichtlich der Ausgestaltung und Funktion der Datenschutzbehörden Rechnung zu tragen. Bereits nach bestehender Rechtslage sind die verschiedenen Komponenten des Datenschutzes auseinanderzuhalten.

1.3.3.1 Abwehrkomponente

Die Abwehrkomponente des Datenschutzes betrifft den Schutz vor staatlichen Eingriffen in das Persönlichkeitsrecht. Der Schutzgehalt ist im 37. Tätigkeitsbericht ausführlich entwickelt. Das allgemeine Persönlichkeitsrecht wird gemäß Art. 2 Abs. 1 GG durch die verfassungsmäßige Ordnung und Rechte anderer beschränkt. Diese, ebenfalls im erwähnten Tätigkeitsbericht erörterten, Schranken legitimieren Eingriffe in die informationelle Selbstbestimmung und leiten über zur Schutzkomponente.

1.3.3.2 Schutzkomponente

Der Schutz der Privatsphäre ist zunächst eine originäre eigene Aufgabe der Betroffenen. Der beste Datenschutz beginnt bei sich selbst. Offenbar fehlt es vielfach bei der privaten Lebensgestaltung am Bewusstsein dafür, dass man seine Privatheit nicht mehr als nötig aufgeben sollte. Daraus erwächst der staatliche Auftrag, der mangelnden Sensibilisierung der Bevölke-

rung für die Bedeutung des Datenschutzes im Hinblick auf die Persönlichkeitsentfaltung der Bürgerinnen und Bürger entgegenzuwirken. Vor allem folgt aber aus der Schutzkomponente des Datenschutzgrundrechts die staatliche Verpflichtung, den Einzelnen Schutz dagegen zu bieten, dass private Dritte ohne ihr Wissen auf ihre personenbezogenen Daten zugreifen. Der Staat ist Wächter und Schiedsrichter zugleich. Die informationelle Selbstbestimmung erfordert nämlich auch einen geschützten Datenaustausch. Sie setzt sich deshalb fort im Datenzugangsschutz.

1.3.3.3 Datenzugangsschutz

Der Datenzugangschutz ist ein Teilaspekt der Informationszugangsfreiheitsrechten. Die Einführung von Informationszugangsrechten ist nur noch bedingt eine autonome Entscheidung der nationalen Gesetzgeber, namentlich des Hessischen Landtages. Durch die Umweltinformationsrichtlinie 2003/4/EG vom 28. Januar 2003 (ABl. EG 2003 Nr. L 41) ist für Umweltinformationen das Amtsgeheimnis aufgehoben. Im Hinblick auf Umweltinformationen sind damit behördliche Umweltdaten eine allgemein zugängliche Quelle geworden. Auch nach dem Verbraucherinformationsgesetz (VIG) vom 5. November 2007 (BGBl. I S. 2558) werden staatliche und teilweise sogar privaten Stellen auskunftspflichtig, ohne dass die Antragsteller ein besonderes Interesse geltend machen müssten. Dies gilt nicht, wenn auf diese Weise Betriebs- und Geschäftsgeheimnisse oder personenbezogene Daten offenbart würden. Die Frage, ob ein Informationsanspruch besteht, ist damit von der Frage zu trennen, ob ein Auskunftsbegehren im behördlichen Interesse beschränkt werden kann. Zudem steht die Art und Weise des Informationszugangs im Ermessen der Auskunftsbehörde (hierzu Sarah Walz, Zur Art und Weise des Informationszugangs, DÖV 2009, 623 ff.) Der Ausschluss des Informationsanspruchs aus Datenschutzgründen unterliegt der Kontrolle des Hessischen Datenschutzbeauftragten. Es erscheint daher sachgerecht, den Hessischen Datenschutzbeauftragten generell in die Entscheidungsfindung einzubinden. Ob das Land Hessen sich gegenüber einer scheibchenweisen Einführung des Konzepts der Informationszugangsfreiheit sperren kann oder sich um einen kontrollierten Informationszugang bemühen sollte - wie etwa der Bund (Informationsfreiheitsgesetz - IFG - vom 5. September 2005, BGBl. I S. 2722) –, ist politisch zu entscheiden.

1.4 Rechtsentwicklung

1.4.1 Überblick

Die Datenschutzskandale im privaten Bereich des Jahres 2008, die sich auch 2009 fortsetzen, wurden flankiert durch eine intensive Rechtsprechungstätigkeit und rege gesetzgeberische Tätigkeit (Überblick bei Gola/Klug, Die Entwicklung des Datenschutzrechts, NJW 2009, 2577 ff.), die den Zuständigkeitsbereich des Hessischen Datenschutzbeauftragten nicht unberührt lässt. So können Geodaten auch im öffentlichen Bereich Relevanz erlangen. Aus diesem Grund verfolgt der Hessische Datenschutzbeauftragte die Entwicklung mit größter Aufmerksamkeit (vgl. Johannes Caspar, Geoinformationen und Datenschutz am Beispiel des Internetdienstes Google Street View, DÖV 2009, 965 ff.).

1.4.2 Rechtsprechung

Aus dem Jahr 2008, wegen der später erfolgten Veröffentlichung im vorangegangenen Tätigkeitsbericht nicht mehr zu berücksichtigen, war das Urteil der Großen Kammer des EuGH vom 16. Dezember 2008 - C 524/56 - DVBl. 2009, 171, wonach das System zur Verarbeitung personenbezogener Daten im Ausländerzentralregister gegen EU-Recht verstößt. Ebenfalls die Große Kammer des EuGH entschied mit Urteil vom 10. Februar 2009 - C-201/06 (Irland/Europäisches Parlament), NJW 2009, 1801, dass die Richtlinie 2006/24/EG in Art. 95 EG (Vorratsdatenspeicherung) eine ausreichende Rechtsgrundlage finde. Dabei stellt die Kammer ausdrücklich klar, dass sich die Entscheidung auf die Wahl der Rechtsgrundlage beschränke und nicht eine Verletzung der Grundrechte als Folge von mit der Richtlinie verbundenen Eingriffen in das Recht auf Privatsphäre zu Gegenstand habe. Die Entscheidung ist ein Beispiel für Kompetenzanmaßungen von EU-Organen und sollte nicht aus Türöffner für beliebige Verstöße gegen den Grundsatz der Datensparsamkeit missverstanden werden (zutreffend Simitis, Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenzregulierung, NJW 2009, 1782 ff.). Die Rechtsprechung zur Eingriffsqualität der Kfz-Kennzeichenüberwachung (BVerfGE 120, 378) setzte das Bundesverfassungsgericht durch Kammerbeschluss vom 17. Februar 2009 - 1 BvR 2492/08 - und vom 11. August 2009 - 2 BvR 941/08 –, DVBl. 2009, 1237 fort. Um eine Präzisierung des Kernbereichs privater Lebensgestaltung bemüht sich der Kammerbschluss vom 10. Juni 2008 - 1 BvR 1107/0 –, NJW 2006, 3357, 3359. Die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers betrachtet das Bundesverfassungsgericht als Eingriff in Art. 10 Abs. 1 GG, der nach § 94 StPO gerechtfertigt werden kann (ebd.). Auf die informationelle Selbstbestimmung musste das Gericht nicht zurückgreifen. Das gilt auch für den BGH, der die Zulässigkeit einer heimlichen Überwachung von Ehegattengesprächen in einem Besuchsraum in der Untersuchungshaft am Rechtsstaatsprinzip maß und auch von daher zu einem Verwertungsverbot gelangte (Urteil vom 29. April 2009 - 1 StR 701/08 -, NJW 2009, 2463). Bei der Nutzung von Betriebsrechnern zum privaten E-Mail-Verkehr stellt der HessVGH zutreffend auf Art. 10 GG ab, nicht jedoch auf die informationelle Selbstbestimmung (Beschluss vom 19. Mai 2009 - 6 A 2672/08 Z. - NJW 2009, 2470). Für die Mitteilung personenbezogener Daten durch die Polizei in den privaten bzw. in den nicht öffentlichen Bereich lässt § 23 HSOG die Erfüllung polizeilicher Aufgaben genügen. Die Entscheidung des OVG Hamburg vom 4. Juni 2009 - 4 Bf 213/07 –, wonach die Öffentlichkeitsfahndung nach offiziellen Terrorverdächtigen eine erhebliche Gefahr erfordert, lässt Zweifel an der Verfassungsmäßigkeit der hessischen Regelung aufkommen.

1.5 Daseinsvorsorge

1.5.1 Gemeinsamer Ausgangspunkt

Die Hessische Landesregierung hat sich mehrfach dahingehend geäußert, dass sie ebenso wie der Hessische Datenschutzbeauftragte der Ansicht sei, dass jedenfalls die hoheitlichen Bereiche der Daseinsvorsorge dem öffentlichen Bereich zuzuordnen seien. Über die Reichweite der Daseinsvorsorge bestehen allerdings nach wie vor unterschiedliche Auffassungen.

1.5.2 Landesregierung

Auf der 27. Plenarsitzung des Hessischen Landtags vom 19. November 2009 wurde der Standpunkt der Landesregierung wie folgt dargestellt:

Der Hessische Datenschutzbeauftragte vertrete hinsichtlich seiner datenschutzrechtlichen Zuständigkeit für privatrechtlich organisierte Unternehmen, die auf dem Gebiet der Daseinsvorsorge tätig sind, eine sehr weitgehende Auslegung des Gesetzes. Er sei der Ansicht, es handele sich bei diesen immer um öffentliche Stellen im Sinne des Hessischen Datenschutzgesetzes, die damit seiner Aufsicht unterliegen würden, weil sich der Staat der Aufgabe der Daseinsvorsorge nicht entledigen könne. Auch wenn diese Aufgabe durch einen Privaten erfüllt werde, ändere dies nichts an der Zuordnung zum öffentlichen Bereich. Dem hielt der Vertreter der Landesregierung entgegen, das geltende Recht verlange in jedem Fall für jedes Unternehmen, dessen Tätigkeit in den Bereich der Daseinsvorsorge fallen könnte, eine mehrstufige Prüfung auf der Grundlage des § 2 BDSG und des § 3 HDSG. Für öffentliche Stellen in Hessen mit Ausnahme derer des Bundes gelte das HDSG. Für nicht öffentliche Stellen gelte grundsätzlich das Bundesdatenschutzgesetz. Die gesetzliche Definition der nicht öffentlichen Stellen befinde sich in § 2 Abs. 4 BDSG. Der Bund habe insoweit von seiner Gesetzgebungskompetenz Gebrauch gemacht. Weder der Landesgesetzgeber noch die Landesregierung könnten eine hiervon abweichende Regelung treffen. Nach der Systematik des Bundesdatenschutzgesetzes sei eine Vereinigung des privaten Rechts nur dann eine öffentliche Stelle, wenn daran mindestens eine öffentliche Stelle beteiligt sei und sie Aufgaben der öffentlichen Verwaltung wahrnehme. Dies ergebe sich aus § 2 Abs. 3 BDSG. Das Bundesdatenschutzgesetz unterscheide also bei der Zuordnung privatrechtlich organisierter Unternehmen zu den öffentlichen Stellen zwischen hoheitlichen Aufgaben und anderen Aufgaben der öffentlichen Verwaltung. Nur wenn hoheitliche Aufgaben wahrgenommen würden, komme es auf eine Beteiligung der öffentlichen Hand nicht an. Nach Auffassung der Landesregierung dürfe die Definition im Bundesrecht nicht durch eine weite Auslegung des Begriffs der "hoheitlichen Aufgaben" in § 3 Abs. 1 HDSG umgangen werden, wie das der Hessische Datenschutzbeauftragte vorschlage. Private Unternehmen würden sonst entgegen der Regelung des Bundesdatenschutzgesetzes dem Landesdatenschutzgesetz unterworfen. Die Landesregierung sehe es als ihre Aufgabe an, für die korrekte Anwendung des Bundesdatenschutzgesetzes auf nicht öffentliche Stellen Sorge zu tragen. Damit solle weder einer Flucht in das Privatrecht Vorschub geleistet werden, noch solle die Aufgabenstellung des Hessischen Datenschutzbeauftragten ausgehöhlt werden. Hier setze das Bundesrecht der Interpretierbarkeit des Landesrechts eine Grenze.

1.5.3 Hessischer Datenschutzbeauftragter

Das BDSG ist nach seinem § 1 Abs. 2 Nr. 1 anwendbar für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen des Bundes. Eine Legaldefinition der öffentlichen Stellen des Bundes enthält § 2 Abs. 1 Satz 1 BDSG. Danach handelt es sich um "die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform". Dem Wortlaut entsprechend ist auf Bundesebene von einem organisationsrechtlichen Begriff der öffentlichen Stelle auszugehen. Die öffentliche Stelle muss demnach öffentlich-rechtlich organisiert sein. Spiegelbildlich sind öffentliche Stellen der Länder nach der Legaldefinition in § 2 Abs. 2 BDSG "die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform". Diese Legaldefinition betrifft jedoch lediglich die Auslegung des BDSG. Dem Bundesgesetzgeber fehlt es an der Kompetenz, für den Landesbereich den Begriff der öffentlichen Stelle des Landes zu definieren. Das HDSG hat auf eine eigene Legeldefinition verzichtet; es gilt jedoch nach seinem § 3 Abs. 1 für Behörden, aber auch für "sonstige Stellen". In Abgrenzung zum organisationsrechtlichen Behördenbegriff sind "sonstige öffentliche Stellen" funktional, d.h. entsprechend ihrer Aufgabenstellung zu verstehen. Eine sonstige Stelle ist - vergleichbar mit der Stelle öffentlicher Verwaltung i.S.v. § 2 Abs. 1 Nr. 1 UIG - eine Stelle, die öffentlich-rechtlich (hoheitlich oder schlicht-hoheitlich) wie auch privatrechtlich (fiskalisch oder verwaltungsprivatrechtlich) handelt (vgl. BVerwG Urteil vom 18. Oktober 2005 - 7 C 5.04 –, DÖV 2006, 435, 436). Erfasst werden alle Stellen, die bei ihrer Aufgabenerfüllung öffentlich-rechtlichen Bindungen unterliegen. Das sind zum einen alle Stellen, die hoheitliche Aufgaben im engeren Sinne wahrnehmen. Handelt es sich um Personen des privaten Rechts, müssen diese ohnehin mit Hoheitsgewalt beliehen werden, so dass sie dann als Behörden nach § 1 Abs. 2 VwVfG handeln. Zum öffentlichen Bereich zählen aber auch Tätigkeiten zur Erfüllung des öffentlichen Daseinsvorsorgeauftrags. Daseinsvorsorge impliziert nämlich unmittelbare Grundrechtsbindungen. Da Adressat des Datenschutzrechts zur Wahrung der Grundrechte in erster Linie der Staat ist, ist es nur folgrichtig, dass die Datenschutzgesetze in ihrem Anwendungsbereich unterscheiden, ob die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch im weitesten Sinne staatliche Stellen oder durch Bürger beziehungsweise gewerblich Tätige, also private Stellen durchgeführt wird. Nur zur Klarstellung sei darauf hingewiesen, dass der öffentliche Bereich nicht notwendig durchgängig öffentlich-rechtlich geregelt sein muss. Es sind durchaus auch Handlungen auf privatrechtlicher Grundlage möglich, die aber öffentlich-rechtlicher Regulierung unterliegen. Die Überwachung der Einhaltung solcher Regulierungsvorgaben ist mit "Aufsicht" gemeint.

1.5.4 Anwendungsbereiche

Im 37. Tätigkeitsbericht wurden die Anwendungsbereiche der Daseinsvorsorge wie folgt umrissen:

Erfasst werden Bereiche

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

Damit sollten nicht die gesamten erwähnten Bereiche vollständig der Daseinsvorsorge zugeschlagen werden. Die Frage der Kontrollzuständigkeit bedarf vielmehr einer Abklärung mit dem Regierungspräsidium Darmstadt im Einzelfall. Bei dieser Abklärung kann auf folgende Kriterien der Rechtsprechung zurückgegriffen werden:

- Im Bereich der Versorgungswirtschaft sind Träger der öffentlichen Wasserversorgung grundsätzlich die Gemeinden, die zu diesem Zweck Eigenbetriebe führen. Sie können sich bei der Erfüllung dieser Aufgabe privater Dritter bedienen. Gleichwohl bleibt die öffentliche Wasserversorgung eine Aufgabe der Daseinsvorsorge (BVerfG Urteil vom 7. Juni 1977 - 1 BvR 108, 424/73 und 226 /4 –, BVerfGE 45, 63, 78; BGH Urteil vom 25. Februar 1975 - III ZR 12/83 –, BGHZ 91, 84, 86; OLG Frankfurt Urteil vom 16. Februar 1994 - 7 U 10/93 –, NJW-RR 1994 S. 1041). Die Wettbewerbsöffnung durch den erzwungenen Zugang zu den vorhandenen Energieversorgungsleitungen (Durchleitung) dient unter Daseinsvorsorgeaspekten in erster Linie der Versorgung der Endverbraucher (BGH, Urteil vom 19. November 2008 - VIII ZR 138/07, BeckRS 2008 25620 Nr. 8 - Gasversorgung –; BVerfG Kammerbeschluss vom 10. September 2008 - 1 BvR 1914/02, - Elektrizitätsversorgung –. Die Daseinsvorsorgeaufgabe ist eindeutig in § 1 EnWG umschrieben, der als Gesetzeszweck eine möglichst sichere, preisgünstige und umweltverträgliche leitungsgebundene Versorgung mit Elektrizität und Gas im Interesse der Allgemeinheit bestimmt. Priorität genießt die Versorgungssicherheit. Diese wiederum wurde vom Bundesverfassungsgericht unter Berufung auf die Daseinsvorsorge als öffentliche Aufgabe von größter Bedeutung qualifiziert, als "Leistung, deren der Bürger zur Sicherung einer menschenwürdigen Existenz unumgänglich bedarf" (BVerfG, Beschluss vom 20. März 1984 - 1 BvL 28/82 –, BVerfGE 66, 248, 258). Die Abwasserbeseitigung obliegt ebenfalls den Gemeinden, in denen das Abwasser anfällt, soweit sie nicht auf andere Körperschaften des öffentlichen Rechts übertragen ist (§ 52 Abs. 1 HWG). Die Beseitigungspflichtigen können sich zur Erfüllung ihrer Aufgaben Dritter bedienen, auch insoweit handelt es sich um eine Aufgabe der Daseinsvorsorge (BGH Urteil vom 27. Januar 1994 - III ZR 158/91 –, BGHZ 125, 19, 22 f). Spätestens seit Inkrafttreten des AbfG vom 7. Juni 1972 (BGBl. I S. 873) gilt die Abfallentsorgung als eine Aufgabe der Daseinsvorsorge (BVerwG Urt. vom 9. März 1990 - 7 C 21.89 –, BVerwGE 85, 44, 47).

- Eine originäre staatliche Aufgabe ist es, die für das Funktionieren der Industriegesellschaft unentbehrliche Verkehrsinfrastruktur zu gewährleisten. Das gilt grundsätzlich für alle Verkehrswege. Auch der Luftverkehr fällt im Zeitalter des Massentourismus unter die Daseinsvorsorge, was bei der Errichtung und dem Betrieb von Verkehrsflughäfen zu berücksichtigen ist (OLG Frankfurt, Urteil vom 30. August 1996 - 1 HEs 196/96 –, NStZ 1997 S. 200; LG Frankfurt, Urteil vom 13. Mai 1996 - 5/12 Qs 14/56 –, NStZ-RR 1996 S. 259; BVerwG vom 7. Juli 1978 - 4 C 79.76 u.a. –, BVerwGE 6, 119). Die Bahnreform hat den Daseinsvorsorgeauftrag der Eisenbahnen des Bundes und der Länder nicht beseitigt. Jedenfalls der Personenfernverkehr der Eisenbahnen (BGH Urt. vom 21. November 1996 - V ZB 19/96 –, NJW 1997, 744), der SPNV und ÖPNV sind für die Verwirklichung der Mobilitätsbedürfnisse unverzichtbar. Das rechtfertigt es, bestimmte dieser Verkehrsektoren dem Bereich der Daseinsvorsorge zuzuordnen.

- Im Rundfunk bedeutet Daseinsvorsorge Grundversorgung (so bereits Herrmann, Fernsehen und Hörfunk in der Verfassung der Bundesrepublik Deutschland, 1975, S. 322, 332 f, 346, 378). Wie bei der Daseinsvorsorge ist die Beschränkung auf existenznotwendige Leistungen im Lauf der Zeit entfallen. Aus der Grundversorgung im Sinne einer Minimalgarantie wurde der Funktionsauftrag des Rundfunks, dem sowohl der Anstaltsrundfunk wie auch in geringerem Ausmaß die privaten Rundfunkveranstalter unterworfen sind.

- Das Post- und Fernmeldewesen galt schon immer als eine Aufgabe der Daseinsvorsorge. Es ist damit eine öffentliche Aufgabe des Staates. Daran hat sich durch die jüngeren Entwicklungen auf dem Telekommunikationssektor nichts geändert. Die Ermöglichung der Telekommunikation entspricht nicht nur einem Grundbedürfnis des modernen Menschen, sondern ist Voraussetzung für den Gebrauch der Kommunikationsgrundrechte ("Universaldienste"). Das schließt eine Privatisierung der Telekommunikationsdienstleistungen nicht aus. Nach Art. 87 f GG werden Dienstleistungen im Bereich des Postwesens und der Telekommunikation als privatwirtschaftliche Tätigkeiten geführt, wobei jedoch den Bund eine Gewährleistungspflicht für eine angemessene und ausreichende flächendeckende Versorgung trifft. Wann die Versorgung flächendeckend angemessen und ausreichend ist, lässt sich nur unter Zugrundelegung eines Rechtsbegriffs der Daseinsvorsorge ermitteln, der bereichsspezifisch durch das TKG konkretisiert wird.

- Der öffentlich-rechtliche Bankensektor wird ebenfalls durch Daseinsvorsorgeaufgaben legitimiert (BVerfG Urteil vom 14. April 1987 - 1 BvR 775/84 –, BVerfGE 75, 192 ,199 f; Kammerbeschluss vom 23. September 1994 - 2 BvR 1547/85 –, NVwZ 1995 S. 370; BGH Urteil vom 11. Dezember1990 - XI ZR 54/90 –, NJW 1991 S. 78). Die originären staatlichen Daseinsvorsorgeaufgaben reichen vorerst für eine Existenzgarantie der Öffentlichen Banken aus, solange sich die Sparkassen nicht verstärkt aus der Fläche zurückziehen.

- Weitere Anwendungsfelder der Daseinsvorsorge im EU-Kontext ("Services d`intérêt général") können sich bei Bildungs-, Sozial-, Gesundheits-, Kultur- und Freizeiteinrichtungen ergeben. Sie entziehen sich einer generellen Bewertung und erfordern eine Zuständigkeitsabgrenzung im jeweiligen Sachgebiet.

2. Europa

2.1 Vertrag von Lissabon

Der im Dezember 2009 in Kraft getretene Vertrag von Lissabon wirkt sich auch auf das deutsche Datenschutzrecht aus.

Am 1. Dezember 2009 trat der Vertrag von Lissabon in Kraft. Er ist ein weiterer Schritt zur europäischen Integration und bekräftigt die eminente Bedeutung des europäischen Rechts für den deutschen Datenschutz. Er ist freilich kein Surrogat für eine Europäische Verfassung. Maßgeblich sind nach wie vor die europäischen Verträge (Primärrecht). Deren Geltung steht, wie das Bundesverfassungsgericht betont hat, unter dem Vorbehalt von Art. 23 Abs. 2 Satz 3 i.V.m. Art. 79 Abs. 2 GG (Urteil vom 30.06.2009 - 2 BvE 2/08 u.a.-, DVBl. 2009, 1032 = NJW 2009, 2267; hierzu Ruffert, DVBl. 2009, 1197 f.; Gärditz/Hillgruber JZ 2009,872 ff.; Claasen JZ 2009, 881 ff.; Frenz, VerwArch 2009, 475 ff.; Halberstam/Möller German Law Journal 2009, 1241 ff.; Schönberger German Law Journal 2009, 1201 ff.; Nettesheim, NJW 2009, 2867; v. Bogdandy, NJW 2010, 1 ff.). Das bedeutet, dass auch auf europarechtlicher Grundlage in den durch Art. 1 Abs. 1 GG geschützten Kernbereich privater Lebensgestaltung nicht eingedrungen werden darf. Insofern kann man von einem "Vorrang des Rechts auf informationelle Selbstbestimmung vor der AEUV" sprechen (Ronellenfitsch, in: Der Hessische Datenschutzbeauftragte, [Hrsg.], Datenschutz in Deutschland nach dem Vertrag von Lissabon, 2009, S. 75 ff.). Ansonsten bleibt es beim Anwendungsvorrang des EU-Rechts, dem damit auf dem Gebiet des Datenschutzes weiterhin zentrale Bedeutung zukommt.

2.2 Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrnehmung der Interessen der Landesdatenschutzbeauftragten in der europäischen Kontrollinstanz für das Schengener Informationssystem übertragen. Der Beitrag stellt die Arbeitsschwerpunkte der Sitzungen der Kontrollinstanz im Berichtszeitraum dar.

2.2.1 Schengener Informationssystem der zweiten Generation (SIS II)

Im letzten Tätigkeitsbericht (Ziff. 2.1.1) hatte ich Anfang 2009 als voraussichtlichen Termin für den Start von SIS II genannt. Daraus ist nichts geworden. Vielmehr stand die Realisierung von SIS II im Frühjahr d.J. grundsätzlich in Frage, da die entsprechenden Tests in den Mitgliedsländern sehr unbefriedigend ausfielen. Es stand deshalb zur Disposition entweder das bestehende SIS I Plus mit den neuen in den Rechtsgrundlagen für SIS II enthaltenen Funktionalitäten zu einem SIS I Plus Re (Renewal) auszubauen oder doch weiter auf den Ausbau des SIS II zu setzen. Der Rat für Justiz und Inneres entschied dann Anfang Juni d.J., dass das SIS II in zwei weiteren Phasen getestet werden soll, die bis in den Sommer 2010 hinein geplant sind. Wichtig war die Aussage, dass für den Fall, dass die Tests scheitern, das laufende SIS-II-Programm eingestellt und die Entwicklung auf der Grundlage der technischen Lösung SIS I Plus Re fortgesetzt werden soll.

Weiterhin scheint festzustehen, dass die neuen Rechtsgrundlagen für SIS II auf jeden Fall Anwendung finden sollen, sei es für die SIS-I-Plus-Re-Version oder für die bisher vorgesehene SIS-II-Technik.
Die neuen Rechtsgrundlagen für SIS II sehen als Kontrollinstrument nicht mehr die Gemeinsame Kontrollinstanz (GK) vor. Vielmehr soll die Kontrolle durch den Europäischen Datenschutzbeauftragten hinsichtlich des zentralen Teils SIS und der damit zusammenhängenden Fragen vorgenommen werden. Hinzu kommen die nationalen Kontrollinstanzen in den einzelnen Schengen-Staaten, deren Zusammenarbeit durch die in den Rechtsakten vorgesehenen gemeinsamen Sitzungen formalisiert wird.

2.2.2 Gemeinsame Überprüfung der Ausschreibungen zur vorläufigen In Gewahrsamnahme

Die GK hat eine gemeinsame Überprüfung von Ausschreibungen nach Art. 97 Schengener Durchführungsübereinkommen (SDÜ) vorgenommen. Dabei geht es zum einen u.a. um Vermisste und andere Personen sowie Minderjährige.

Art. 97 SDÜ

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

Anlass für die Überprüfung war die sehr unterschiedliche Zahl der Ausschreibungen, die nicht alleine mit der unterschiedlichen Einwohnerzahl des jeweiligen Schengen-Landes erklärt werden konnte.

In dem verabschiedeten Bericht über die gemeinsame Kontrolle stellt die GK u.a. fest, dass nicht in allen Schengen-Staaten Verfahrensvorschriften für die Ausschreibung vorgesehen sind und empfiehlt diese zu erlassen. Sie weist weiterhin darauf hin, dass bei der Ausschreibung von Minderjährigen durch automatische Verfahren sichergestellt werden muss, dass die Ausschreibungen bei Erreichen der Volljährigkeit gelöscht werden. Eine weitere wichtige Forderung betrifft den Zugang der unterschiedlichsten Behörden auf die Ausschreibungen nach Art. 97 SDÜ. Hier ist sicherzustellen, dass nur die in den Vorschriften vorgesehenen Behörden einen derartigen Zugriff haben dürfen.

2.2.3 Gemeinsame Überprüfung der Ausschreibungen zur Wohnsitz- und Aufenthaltsermittlung

Eine weitere konzertiere Überprüfung betrifft die Ausschreibungen nach Art. 98 SDÜ im Schengener Informationssystem. Dabei geht es vor allem um Zeugen und andere Personen, die vor Gericht erscheinen müssen.

Art. 98 Abs. 1 SDÜ

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

Auch bei Art. 98 SDÜ gibt es große Unterschiede in der Anzahl der Ausschreibungen zwischen den einzelnen Schengen-Ländern. Die GK stellt u.a. fest, dass in einigen Fällen das Löschungs- und Prüfverfahren für die Ausschreibungen nicht mit Art. 112 SDÜ in Einklang steht.

Art. 112 Abs. 1 SDÜ

Die zur Personenfahndung in dem Schengener Informationssystem aufgenommenen personenbezogenen Daten werden nicht länger als für den verfolgten Zweck erforderlich gespeichert. Spätestens drei Jahre nach ihrer Einspeicherung ist die Erforderlichkeit der weiteren Speicherung von der ausschreibenden Vertragspartei zu prüfen. …

Zweck der Ausschreibung nach Art. 98 SDÜ ist es, den Aufenthaltsort der gesuchten Person der ausschreibenden Behörde mitzuteilen. Sobald dieser Zweck erfüllt ist, ist die Ausschreibung zu löschen.

Die GK fordert weiterhin, dass nur die in den Vorschriften vorgesehenen Behörden Zugriff auf die Ausschreibungen haben.

2.2.4 Leitfaden zum Auskunftsrecht in allen Schengen-Staaten

Eine Besonderheit des Schengener Durchführungsübereinkommens besteht darin, dass jede Person in jedem Schengen-Staat, Auskunft bzw. Berichtigung oder Löschung über die zu ihrer Person im SIS gespeicherten Daten verlangen kann, unabhängig davon, welcher Staat die Ausschreibung vorgenommen hat.

Art. 109 Abs. 1 SDÜ

Das Recht jeder Person, über die zu ihrer Person im Schengener Informationssystem gespeicherten Daten Auskunft zu erhalten, richtet sich nach dem nationalen Recht der Vertragspartei, in deren Hoheitsgebiet das Auskunftsrecht beansprucht wird. Soweit das nationale Recht dies vorsieht, entscheidet die in Art. 114 Abs. 1 vorgesehene nationale Kontrollinstanz, ob und in welcher Weise Auskunft erteilt wird.

Art. 110 SDÜ

Jeder hat das Recht, auf seine Person bezogene unrichtige Daten berichtigen oder unrechtmäßig gespeicherte Daten löschen zu lassen.

Die Bürger können sich also an eine Vielzahl von Stellen in Europa wenden, die jeweils nach nationalem Recht über die Berichtigungs- und Löschungsbegehren entscheiden.
Die GK hat deshalb die wichtigsten Verfahrensschritte zur Geltendmachung der Rechte in den jeweiligen Schengen-Staaten und die entsprechenden Adressen der Behörden in einem Leitfaden zusammengestellt. Beigefügt sind verschiedene Formbriefe für die Bitte um Auskunft, Löschung oder Berichtigung der über die Betroffenen gespeicherten Daten.

2.3 Gemeinsame Kontrollinstanz für EUROPOL

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

2.3.1 Neue Rechtsgrundlagen für EUROPOL

In meinen letzten Tätigkeitsberichten (36. Tätigkeitsbericht, Ziff. 3.2.1, 37. Tätigkeitsbericht, Ziff. 2.1.2.1) hatte ich darauf hingewiesen, dass das EUROPOL-Abkommen durch einen Ratsbeschluss nach Art. 34 Abs. 2c EU-Vertrag ersetzt werden soll. Der Beschluss des Rates zur Errichtung des Europäischen Polizeiamts (EUROPOL) ist nunmehr verabschiedet (ABl. 2009 L 121/37) und gilt ab 1. Januar 2010.

Anders als bei den neuen Rechtsvorschriften für SIS II (s. oben Ziff. 2.1.1) bleibt die GK für EUROPOL bestehen.

Art. 34 Abs. 1 des EUROPOL-Beschlusses

Es wird eine unabhängige Gemeinsame Kontrollinstanz eingesetzt, deren Aufgabe darin besteht, nach Maßgabe dieses Beschlusses die Tätigkeit von EUROPOL daraufhin zu überprüfen, ob durch die Speicherung, Verarbeitung und Verwendung der bei EUROPOL vorhandenen Daten die Rechte des Einzelnen verletzt werden. Darüber hinaus kontrolliert die Gemeinsame Kontrollinstanz die Zulässigkeit der Übermittlung der von EUROPOL stammenden Daten.

Die wichtigsten Änderungen der Rechtslage durch den EUROPOL-Beschluss habe ich im 36. Tätigkeitsbericht (Ziff. 3.2.1) dargestellt. Ich habe dort auch auf die kritische Stellungnahme der GK hingewiesen.

Die neuen Rechtsgrundlagen für EUROPOL führen dazu, dass eine ganze Reihe von Implementierungsvorschriften erarbeitet werden, zu denen die Stellungnahmen der GK eingeholt werden. Die GK hat sich u.a. geäußert zu den Durchführungsvorschriften für Analysedateien, zu Durchführungsbestimmungen für die Teilnahme von Drittstaaten in Analysegruppen und Vorschriften zur Regelung der Beziehungen zwischen EUROPOL und privaten Stellen.

2.3.2 Kontrolle des Internets

Im 36. Tätigkeitsbericht (Ziff. 3.2.3) hatte ich von dem unter deutscher Ratspräsidentschaft initiierten "Check-the-Web"-Projekt hinsichtlich islamistischem Terrorismus berichtet. Das Projekt wurde im Rahmen einer Inspektion durch die GK geprüft. Auch wegen der dabei aufgetretenen rechtlichen Probleme verfolgt EUROPOL nunmehr den Plan, die Informationen zu islamistischem Terrorismus in eine Analysedatei einzustellen. Die GK hat dies begrüßt, weil sich das Projekt dadurch in einem bestimmten rechtlichen Rahmen halten muss. Neu ist allerdings, dass EUROPOL mit der Analysedatei ein sog. Portal verbindet, das eine Auswahl von Informationen enthält. Zweck dieses Portals ist es, Drittstaaten schnell und unbürokratisch Zugriff auf bestimmte Informationen zu islamistischem Terrorismus zu geben. Die Arbeitsgruppe Analysedatei der GK, in der ich vertreten bin, hat mit EUROPOL zusammen dafür ein Verfahren entwickelt, das den rechtlichen Vorgaben genügt.

2.3.3 Austausch von Informationen mit Drittstaaten

Die GK hat Informationen erhalten, dass Informationen aus Drittstaaten an EUROPOL gelangen ohne dass EUROPOL mit diesen Staaten - wie im EUROPOL-Abkommen oder auch demnächst im Ratsbeschluss vorgesehen - Vereinbarungen getroffen hat. Diese Informationen sollen über einen EUROPOL-Mitgliedsstaat erfolgen, der die Informationen aus dem Drittstaat erhält. Auf diese Weise wird die Voraussetzung umgangen, dass der Drittstaat über ein adäquates Datenschutzniveau verfügen muss, und die GK hat keine Möglichkeit, eine Stellungnahme zu dem Datenschutzniveau abzugeben. Die GK wird bei EUROPOL prüfen, ob es dort Daten aus Drittländern ohne derartige Vereinbarungen gibt und ob dieser Austausch evtl. in einer strukturierten Form erfolgt.

2.3.4 Kontrolle von EUROPOL

Die GK hat im Jahr 2009 wieder eine Kontrolle bei EUROPOL durchgeführt. Der Bericht über diese Kontrolle ist vertraulich.

2.4 Koordinierungsgruppe für die Kontrolle von EURODAC

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

Im 37. Tätigkeitsbericht (Ziff. 2.2) hatte ich berichtet, dass die Koordinierungsgruppe Kontrollen von EURODAC in den Mitgliedsländern nach gemeinsamen Kriterien vornehmen will.

Zwei von den drei damals genannten Kontrollthemen sind abgeschlossen und in einem Kontrollbericht zusammengefasst (Eurodac Supervision Coordination Group, Second Inspection Report vom 24. Juni 2009, http://www.edps.europa.eu).

Die erste Kontrolle betrifft die Frage, inwieweit die Mitgliedsstaaten der in Art. 18 EURODAC-Verordnung enthaltenen Verpflichtung nachkommen, die Betroffenen über Einzelheiten des Fingerabdruckverfahrens zu informieren.

Art. 18 EURODAC-Verordnung

(1) Der Herkunftsmitgliedstaat unterrichtet die Personen, die unter diese Verordnung fallen, über
a) die Identität des für die Verarbeitung Verantwortlichen und ggf. seines Vertreters,
b) die Zwecke der Verarbeitung der Daten im Rahmen von Eurodac,
c) die Empfänger der Daten,
d) die Verpflichtung zur Fingerabdrucknahme bei Personen im Sinne des Artikels 4 oder Artikels 8,
e) die Auskunfts- und Berichtigungsrechte bezüglich sie betreffender Daten.

Die Koordinierungsgruppe stellte u.a. fest:

- dass die Qualität der Informationen verbessert werden muss, insbesondere den Betroffenen ihre Rechte auf Auskunft und Berichtigung der sie betreffenden Daten darzulegen sind,
- dass für die Informationen ein Standardformular in einfacher und verständlicher Sprache entwickelt werden sollte,
- dass bzgl. der Informationen nicht zwischen Asylsuchenden und sich illegal in den Mitgliedsstaaten aufhaltenden Personen unterschieden werden darf.

Bei der zweiten Kontrolle geht es um die Speicherung von Fingerabdrücken Minderjähriger und die Methode der Altersfeststellung. Die Kontrolle ergab u.a.:

- dass in den Mitgliedsländern sehr unterschiedliche Methoden zur Altersfeststellung (z.B. invasive Verfahren wie Röntgenaufnahmen von Zähnen und Handgelenken) angewandt werden,
- dass die Kommission eine Beurteilung der Zuverlässigkeit und Sicherheit dieser Methoden vornehmen soll mit dem Ziel, die Verfahren zu harmonisieren,
- dass die Weigerung des Asylbewerbers, sich einer medizinischen Untersuchung zu unterziehen, sich nicht negativ auf seine Stellung im Asylverfahren auswirken darf.

Die Ergebnisse der im 37. Tätigkeitsbericht (Ziff. 2.2) angesprochenen Kontrolle der Anwendung des Dubli-Net liegen noch nicht vor.

3. Bund

3.1 Bürgerportalgesetz

Der in der abgelaufenen Legislaturperiode vorgelegte und nicht mehr verabschiedete Entwurf zum Bürgerportalgesetz des Bundes, mit dem die rechtlichen Grundlagen für eine sichere Infrastruktur für E-Mail-Kommunikation geschaffen werden sollten, war aus datenschutzrechtlicher Sicht unausgereift.

Der Gesetzentwurf der Bundesregierung zur Regelung von Bürgerportalen hatte zum Ziel den Rechtsrahmen zu schaffen, der zur Einführung vertrauenswürdiger Bürgerportale im Internet benötigt wird. Mit den Bürgerportalen sollte eine zuverlässige und geschützte Infrastruktur eingeführt werden, die die Vorteile der E-Mail mit Sicherheit, Verbraucherschutz und Datenschutz verbindet. Es war geplant, dass im Rahmen eines Akkreditierungsverfahrens die Bürgerportaldiensteanbieter nachweisen sollten, dass die durch sie angebotenen E-Mail-, Identitätsbestätigungs- und Speicherdienste hohe Anforderungen an Sicherheit, Daten- und Verbraucherschutz erfüllen. Zur Entlastung der zuständigen Behörde sollte die Nachweiserbringung auch über anerkannte private Stellen erfolgen können. Nur die Akkreditierung selbst sollte ausschließlich durch die zuständige Behörde erfolgen.

Die Betreiber von Bürgerportaldiensten sollten verpflichtet werden, die Vertraulichkeit, die Integrität und die Authentizität der Nachrichten zu gewährleisten, so dass diese auf dem Transportweg nicht ausgespäht oder mitgelesen werden können. Auch sollte die Sicherheit der Speicherdienste ein hohes Niveau erreichen.

Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit hat den Landesdatenschutzbeauftragten schon sehr frühzeitig Gelegenheit gegeben, zu dem Gesetzentwurf Stellung zu nehmen. Ich habe diese Gelegenheit genutzt und meine Kritikpunkte sowohl gegenüber dem Bundesbeauftragten als auch gegenüber dem Hessischen Ministerium des Innern und für Sport vorgetragen. Im Wesentlichen handelte es sich dabei um folgende Punkte:

1. Die einzelnen Regelungen blieben in vielen Fällen äußerst vage und sind damit nicht normenklar. Die Entwurfsverfasser haben lediglich Grundgedanken formuliert, wie ein Bürgerportal aussehen könnte, ohne Detailfragen zu regeln. Die eigentlich wesentlichen inhaltlichen Punkte, die auch und gerade aus Datenschutzsicht bedeutsam sind, sollten erst in einer Rechtsverordnung geregelt werden, die nicht einmal der Zustimmung des Bundesrates bedurft hätte. Ich habe dies nicht für akzeptabel gehalten. Die Punkte, die für das informationelle Selbstbestimmungsrecht der Bürger besonders wichtig sind, sollten nach meiner Auffassung im Gesetz selbst geregelt werden. Dies betrifft insbesondere die Frage, zu welchem Zeitpunkt die Betroffenen für ihr Postfach den Zugang i.S.d. § 3a VwVfG eröffnet haben und damit für sie konkrete Rechtsfolgen eintreten können. Das gilt auch für die Aufklärungs- und Informationspflichten sowie für die Rolle und Aufgaben der sog. Dritten nach § 18 Abs. 3 und der Sachverständigen nach § 20 des Gesetzentwurfs. Im Übrigen waren viele relevante Einzelfragen im Begründungstext enthalten, die Bestandteil des Gesetzes sein sollten.

2. Der Gesetzentwurf sah vor, dass Nutzende grundsätzlich eine personenbezogene Hauptadresse haben müssen (§ 5 Abs. 1). Eine oder mehrere pseudonyme Adressen sollten nur zusätzlich auf Antrag erhalten werden können. Datenschutzfreundlicher wäre die Möglichkeit gewesen, gleich eine pseudonyme Adresse beantragen zu können.

3. Durch das Gesetz (und zusätzliche Erläuterungen im Internet) wurden der sichere Betrieb und dabei insbesondere die Vertraulichkeit des Postfach- und Versanddienstes sowie des Speicherdienstes, d.h. Speicherplatzes, hervorgehoben. Es wurde jedoch nicht ausreichend klar, dass der Diensteanbieter die gespeicherten Daten zur Kenntnis nehmen kann; dies ergibt sich aber aus dem Anspruch, die Verfügbarkeit sicherzustellen, obwohl Passwörter vergessen und Token verloren werden können. Damit war klar, dass eine Ende-zu-Ende–Sicherheit gerade nicht gegeben ist.

4. Für problematisch habe ich gehalten, dass das BSI Sachverständige für Datenschutz anerkennen kann und deren Feststellungen mit einem behördlichen Gütesiegel zertifiziert, das die Erfüllung des Datenschutzes bescheinigt.

5. Für Diensteanbieter war die Möglichkeit vorgesehen, sichere und unsichere Anmeldeverfahren anzubieten. Die jeweiligen Rechtsfolgen waren jedoch nicht dargestellt, so dass gänzlich unklar war, welchen Beweiswert auf diesem Weg abgegebene Willenserklärungen haben.

6. Das Verfahren hätte weder die fortgeschrittene noch die qualifizierte Signatur ersetzt.

7. Die technischen Einzelsachverhalte waren im Gesetz ganz unberücksichtigt und sollten erst durch die Rechtsverordnung nach § 25 des Gesetzentwurfs festgelegt werden.

Die Kritikpunkte waren auch Gegenstand einer Entschließung der Konferenz des Datenschutzbeauftragten des Bundes und der Länder vom 16. April 2009 (s. Ziff. 9.6).

Da das Gesetz vor der Bundestagswahl nicht mehr verabschiedet wurde, aber eine Wiederaufnahme des Projekts zu erwarten ist, sollten alle Bemühungen darauf gerichtet sein, auf datenschutzrechtliche Verbesserungen hinzuwirken.

3.2 Der Auskunftsanspruch Betroffener darf auch in Besteuerungsverfahren nicht verkürzt werden

Der voraussetzungslose Anspruch Betroffener auf Auskunft ist Ausfluss des Rechts auf informationelle Selbstbestimmung. Mit einer Verwaltungsanweisung, die den Auskunftsanspruch Steuerpflichtiger weitgehend einschränkt und ihn formell von einem berechtigten Interesse abhängig macht, hebelt das Bundesministerium der Finanzen dieses Grundrecht aus.

Das Verfahrensrecht in Besteuerungsverfahren (Abgabenordnung - AO) sieht einen Auskunftsanspruch Betroffener nicht vor. Da die AO vom Steuergesetzgeber als abschließende Regelung betrachtet wird, wurde bislang auch die Anwendung des § 19 BDSG abgelehnt. Seit vielen Jahren setzen sich die Datenschutzbeauftragten des Bundes und der Länder - bislang erfolglos - dafür ein, eine bereichsspezifische Reglung zu erreichen.

Mit Beschluss vom 10. März 2008 (1 BvR 2388/03, NJW 2008, 2099) hat auch das Bundesverfassungsgericht nunmehr u.a. klargestellt, dass "das Interesse Betroffener von den sie betreffenden informationsbezogenen Maßnahmen des Staates Kenntnis zu erlangen grundrechtlich durch sein in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährtes Grundrecht auf Schutz der Persönlichkeit in der Ausprägung als Grundrecht auf informationelle Selbstbestimmung und ferner durch den Anspruch auf effektiven Rechtsschutz (Art. 19 Abs. 4 GG) geschützt wird".

Insbesondere heißt es in dem Urteil:
"Ist eine staatliche Stelle zu informationsbezogenen Eingriffen berechtigt, deren Vornahme oder Umfang der Betroffene nicht sicher abschätzen kann, da er in den Informationsverarbeitungsprozess nicht oder nicht stets einbezogen wird, und besteht zudem keine Pflicht dieser Stelle zur aktiven Benachrichtigung des Betroffenen, kommt einem Informationsrecht auf eigene Initiative zentrale Bedeutung für den Grundrechtsschutz zu".

Schließlich führt das BVerfG aus, dass § 19 BDSG als rechtmäßige Grundlage des Auskunftsanspruchs auch gegenüber den Bundesfinanzbehörden gilt.

Gleichwohl hat das BMF durch einen umfangreichen Erlass vom 17. Dezember 2008 an die Landesfinanzbehörden nicht auf § 19 BDSG verwiesen, sondern den Auskunftsanspruch grundsätzlich von einem berechtigten Interesse eines Anspruchstellers abhängig gemacht und ihn durch zahlreiche Vorgaben, wann ein solches Interesse gerade nicht anzunehmen sei, ausgehöhlt.

Diese einschränkenden Vorgaben widersprechen dem Beschluss des BVerfG. Denn die Auskunft soll gerade nicht an eine Pflicht zur Darlegung eines berechtigten Interesses des Steuerpflichtigen an der Auskunft geknüpft sein, sondern - umgekehrt - soll die Steuerverwaltung jeweils im Einzelfall etwaige gegenläufige Interessen nachprüfbar abwägen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer 77. Sitzung vom 26./27. März 2009 eine entsprechende Entschließung gefasst und den Bundesgesetzgeber aufgefordert, den Auskunftsanspruch durch eine, dem § 19 BDSG entsprechende Regelung in der AO klarzustellen (s. Ziff. 9.5). Der BfDI hat den Erlass des BMF mit Schreiben vom 15. Mai 2009 beanstandet.

Bislang wurde die Weisung nicht aufgehoben. Allerdings hat das BMF angekündigt, eine bereichsspezifische Regelung in der Abgabenordnung zu schaffen, die den vom BVerfG beschriebenen Anforderungen entspricht.

3.3 Abfrage von Steuerkonten über das Internet im Verfahren ELSTER (Elektronische Steuererklärung)

In diesem Jahr habe ich das Verfahren "Steuerkontoabfrage" geprüft, mit dem Bürger und von ihnen Bevollmächtigte, also Steuerberater, Firmenvertreter oder sonstige Bevollmächtigte, den aktuellen Stand von Steuerkonten abfragen können. Das Verfahren nutzt jetzt mit der Authentisierung die richtige Funktion, das Sicherheitsniveau wurde bei dieser Korrektur aber abgesenkt. Die bislang irreführende Information für die Bürger im Internet wurde korrigiert.

Bisher wurde für die Teilnahme an der Steuerkontoabfrage eine qualifizierte elektronische Signatur verlangt, obwohl es inhaltlich nicht um die Einhaltung eines Schriftformerfordernisses geht. Zweck sollte stattdessen sein sicherzustellen, dass nur eine befugte Person Zugriff auf diese Daten erhält. Dies kann nur mit einem Authentisierungsverfahren erreicht werden. Die Verwendung von falschen Funktionen im Zusammenhang mit ELSTER wurde von mir mehrfach kritisiert (s. 35. Tätigkeitsbericht, Ziff. 4.4; 32. Tätigkeitsbericht, Ziff. 18.5).

Inzwischen wurde dieses Verfahren geändert: Auf den Internet-Seiten von ELSTER wird jetzt für die Steuerkontoabfrage der Einsatz von "Signaturkarten für Authentifizierung" gefordert und die für das Verfahren zugelassenen Karten und ihre Herausgeber werden aufgelistet.

Im Hessischen Ministerium der Finanzen wurde mir die Steuerkontoabfrage im Detail demonstriert. Für die Steuerkontoabfrage wird jetzt die zutreffende Funktion eingesetzt. Auch das Verfahren, mit dem der Kontoinhaber Dritte zum Zugriff bevollmächtigen kann, ist plausibel. Unter Sicherheitsaspekten sollten die Authentisierungsschlüssel aber auf sicheren Signaturerstellungseinheiten nach SigG gespeichert sein und den aktuellen Algorithmen und Parametern für qualifizierte Signaturen entsprechen. Diese Anforderung wurde von ELSTER früher mit der Formulierung "qualifizierte Signaturkarte" beschrieben. Aktuell heißt es jetzt: "In Anlehnung an die Empfehlungen des BSI und der Bundesnetzagentur empfiehlt ELSTER zur Gewährleistung eines langfristigen Sicherheitsniveaus die Verwendung von Signaturkarten für Authentifizierung mit einer Schlüssellänge von 2048 Bit und des Hash-Algorithmus RipeMD-160 oder SHA256." Dies bedeutet, dass diese Empfehlung nicht durchgesetzt wird. Vielmehr werden für die Steuerkontoabfrage sowohl bei den Signaturkarten selbst als auch bei der Zuverlässigkeit der Identifizierung der Schlüsselinhaber bis hin zu den verwendeten Schlüssellängen und Algorithmen weniger sichere Varianten zugelassen.

4. Land

4.1 Querschnitt

4.1.1 Verdeckte Bildaufnahmen während der Räumung des Camps von Flughafenausbaugegnern im Kelsterbacher Wald

Die verdeckten Bildaufnahmen durch Fraport-Mitarbeiter während der Räumung des Camps im Kelsterbacher Wald waren rechtswidrig.

Flughafenausbaugegner hatten im Kelsterbacher Wald ein Camp errichtet, um Ihrem Protest gegen die Rodung des Waldes Nachdruck zu verleihen. Am 18. Februar 2009 wurde dieses Camp durch die Polizei geräumt. Während dieser Räumung hat ein Mitarbeiter des Sicherheitsdienstes der Fraport AG mit einer am Helm montierten Minikamera das Geschehen gefilmt. Davon betroffen waren auch über die Räumung berichtende Journalisten. Einer dieser Journalisten hat die Kamera entdeckt und sich an meine Dienststelle gewandt und um datenschutzrechtliche Prüfung des Vorgehens von Fraport AG gebeten.

Die Fraport AG hat sich zunächst hinsichtlich der Rechtmäßigkeit der Kameraüberwachung bei der Räumung des Camps auf die Befugnisnorm des § 6b Abs. 2 Bundesdatenschutzgesetz (BDSG) berufen; denn die Überwachungsmaßnahme habe sich auf das Gelände bezogen, das sich aufgrund eines Besitzeinweisungsbeschlusses des Regierungspräsidiums Darmstadt im Besitz der Fraport AG befand.

Dieser Argumentation habe ich Folgendes entgegengehalten:

1. Die Stellungnahme gab als Rechtsgrundlage für die Kameraüberwachung § 6b Abs. 2 BDSG an, der jedoch nur eine zusätzliche Voraussetzung für die aus anderen Gründen zulässige Beobachtung öffentlich zugänglicher Räume normiert. Befugnisnorm konnte allenfalls § 6b Abs. 1 BDSG sein. Keine der dort aufgeführten Fallgruppen wurde jedoch den Ereignissen vom 18. Februar 2009 gerecht.

   - Der Fraport-Schutzdienst könnte zwar als öffentliche Stelle angesehen werden (wenn etwa - mir mitzuteilende - Beleihungstatbestände gegeben wären). Dann entfiele jedoch die Anwendbarkeit des BDSG (vgl. § 1 Abs. 2 Nr. 2 BDSG). Maßgeblich wäre den Datenschutz regelndes Landesrecht.

   - Die Wahrnehmung des Hausrechts ist auf das konkret befriedete Besitztum beschränkt. Die Beobachtungsbefugnis des Hausrechtsinhabers endet grundsätzlich an den Grenzen seines Grundstücks.

   - Die Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erfordert die ausdrückliche Zweckbestimmung. Vorliegend war aber nicht einmal eine schlüssige Bekanntmachung erfolgt.

   § 6b BDSG war somit schon tatbestandlich nicht erfüllt. Obendrein schied das BDSG ohnehin als Rechtsgrundlage aus, da Landesrecht maßgeblich ist.

2. Landesrechtlich in Betracht gekommen wäre die Bildübertragung nach § 14 Abs. 4 HSOG. Das umzäunte, rechtswidrig besetzte Gelände der Fraport AG war zwar wohl kaum ein öffentlicher Platz, auf dem wiederholt Straftaten begangen worden sind oder drohten. Möglich war aber die Qualifizierung als besonders gefährdete öffentliche Einrichtung. Die Beobachtungsbefugnis käme der Gefahrenabwehrbehörde zu, was der Sicherheitsdienst der Fraport AG aber gerade nicht ist. Gefahrenabwehrbehörde ist nach § 14 Abs. 4 Satz 2 auch der Inhaber des Hausrechts. Weitergehendes Recht als die staatlichen Gefahrenabwehrbehörden hat der Inhaber des Hausrechts indessen nicht. Diese müssen offen beobachten. Der Inhaber des Hausrechts ist zudem auf die räumlichen Grenzen seines Hausrechts beschränkt. Damit schied § 14 Abs. 4 HSOG als Eingriffsbefugnis ebenfalls aus.

3. Die vorzeitige Besitzeinweisung begründet unmittelbarem Besitz (vgl. § 27g Abs. 4 Satz 4 LuftVG). Beim öffentlichen Raum obliegt das Hausrecht dem unmittelbaren Besitzer des Grundstücks. Die Besitzeinweisung erfolgt aber nur, soweit sie für den Beginn der Bauarbeiten geboten ist. Sie schließt das Waldbetretungsrecht nach § 24 Abs. 1 ForstG nicht aus.

Aus alledem folgte, dass bereits keine Überwachungsbefugnis bestand und dass zumindest auf die Überwachungsmaßnahmen hätte hingewiesen werden müssen.

Der Vorstand der Fraport AG hat mir daraufhin mitgeteilt, dass er meine Rechtsauffassung teilt, wonach der Einsatz einer "Head-Set-Kamera" jedenfalls außerhalb des umzäunten Geländes mit dem geltenden Datenschutzrecht nicht vereinbar war, nachdem sich herausgestellt hatte, dass an dem fraglichen Tag keine für alle potentiell Betroffenen sichtbaren Hinweise in Form der im gesamten Flughafenbereich üblichen Piktogramme vorhanden waren. Es wurde versichert, die von mir vertretene Rechtsansicht zukünftig zu beachten.

4.1.2 Einsatz von Videotechnik zu Planungszwecken

Die Verarbeitung personenbezogener Daten zu Planungszwecken unter Einsatz von Videotechnik ist datenschutzrechtlich dann nicht zu beanstanden, wenn die Daten nach Erreichung des Planungsziels sofort wieder gelöscht werden.

Im vergangenen Berichtszeitraum erreichten mich mehrere Anfragen von Bürgern, die beobachtet hatten, dass an einer Ausfallstraße einer hessischen Kommune verschiedene Videokameras installiert worden waren und baten um rechtliche Überprüfung der Maßnahme. Meine Rückfrage bei der Kommune ergab, dass die Daten zu Zwecken der Verkehrsplanung erhoben wurden.

Unter den in § 32 HDSG formulierten Voraussetzungen ist eine Verarbeitung von personenbezogenen Daten für Planungszwecke zulässig.

§ 32 HDSG

(1) Für Zwecke der öffentlichen Planung können personenbezogene Daten gesondert verarbeitet werden. Die Verarbeitung soll von der übrigen Verwaltung personell und organisatorisch getrennt erfolgen.

(2) Die zu Planungszwecken gespeicherten personenbezogenen Daten dürfen nicht für andere Verwaltungszwecke genutzt werden. Sobald es der Zweck der Planungsaufgabe erlaubt, sind die zu diesem Zweck verarbeiteten personenbezogenen Daten so zu verändern, dass sie sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen. Eine Übermittlung von Daten, aus denen Rückschlüsse auf Einzelpersonen gezogen werden können, ist unzulässig.

Dies kann grundsätzlich auch durch den Einsatz von Videotechnik geschehen. So werden gerade zur Erstellung von Verkehrsflussanalysen häufig Videokameras eingesetzt. Dabei wird das personenbeziehbare Kennzeichen des Fahrzeugs erfasst und zur Messung von Verkehrsströmen evtl. ein weiteres Mal zum Datenbestand genommen. Eine derartige Verarbeitung fand auch im Falle der anfragenden Bürger statt.

Die Daten, die so zu Planungszwecken erhoben wurden, dürfen aber grundsätzlich nicht zu einem anderen Zweck verarbeitet werden. Die Spezialvorschrift des Abs. 2 verbietet deshalb auch die Berufung auf § 13 Abs. 2 i.V.m. § 12 Abs. 2 Nr. 2 bis 5 HDSG, wo geregelt ist, unter welchen Bedingungen Daten zweckändernd weiterverarbeitet werden dürfen. Andernfalls hätte es dieser besonderen Hervorhebung der Zweckbindung nicht bedurft.

Damit ist eine Verarbeitung dieser Daten zu anderen Zwecken nur auf der Grundlage der Einwilligung durch den Betroffenen oder einer gesetzlichen Regelung zulässig. Eine derartige Regelung müsste explizit die zweckändernde Verwendung der zu Planungszwecken erhobenen Daten erlauben.

Das erfasste Kennzeichen muss nach Auswertung der Zahlen aus dem Datenbestand unverzüglich wieder entfernt werden, weil die Erhebung nur den Zweck hatte festzustellen, wohin welche Fahrzeuge ihren Weg nehmen. Das Kennzeichen ist hier kurzfristig ein Hilfsmittel, das dann aber nicht mehr benötigt wird und deshalb im Moment der Erfüllung der Planungsaufgabe gelöscht werden muss.

Die Kommune hat zugesichert, die Vorgaben strikt einzuhalten. Aus Gründen der Akzeptanzsteigerung derartiger Maßnahmen sollte im Vorfeld umfassend über die geplante Analyse informiert werden.

4.1.3 Einsatz von Videotechnik zur Verkehrsüberwachung

Zur Dokumentation von Verkehrsverstößen kann auch Videotechnik eingesetzt werden, wenn sichergestellt ist, dass einzelne Fahrzeuge nur aufgenommen werden, wenn ein konkreter Verdacht für verkehrswidriges Verhalten besteht.

Das BVerfG hat mit einem Beschluss vom 11. August 2009 (2 BvR 941/08) zum Einsatz von Videotechnik im Rahmen von Verkehrskontrollen für erhebliche Diskussionen gesorgt.

Ausgangspunkt war ein Ordnungswidrigkeitenverfahren. Dem Führer eines Pkw war eine Geschwindigkeitsübertretung vorgeworfen worden. Grundlage des Vorwurfs waren Videoaufnahmen, die mit einem auf einer Brücke installierten System erstellt waren. Mit dieser Anlage sollte das Einhalten des Sicherheitsabstandes überwacht werden. Der Pkw-Fahrer hatte sich darauf berufen, dass eine Ermächtigungsgrundlage für einen solchen Einsatz nicht vorhanden sei und die Aufnahme deshalb nicht als Beweismittel zulässig wäre.

Das BVerfG hat in diesem Zusammenhang klargestellt, dass eine verdachtslose Verkehrsüberwachung mittels Videoaufzeichnungen einen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen darstellt. Mangels gesetzlicher Grundlage ist ein solcher Eingriff nicht zulässig.

Der Einsatz von Videotechnik ist damit allerdings auch im Zusammenhang von Geschwindigkeitskontrollen nicht völlig ausgeschlossen. Entsprechende Bildaufzeichnungen dürfen allerdings erst nach Vorliegen eines Anfangsverdachts erfolgen, d.h. eine Messung der Geschwindigkeit muss vorausgegangen sein.

Wiederholt haben bei mir sowohl Bürger als auch Kommunen nachgefragt, inwieweit die hessische Praxis von der Entscheidung betroffen sei. Auf Nachfrage hat mir das Innenministerium mitgeteilt, es habe alle betroffenen Polizeibehörden sowie die Kommunen über die Rahmenbedingungen zum Einsatz der entsprechenden Geräte informiert.

4.2 Justiz, Strafvollzug und Polizei

4.2.1 Novellierung des HSOG

Mit den Änderungen des HSOG sollen die Vorgaben der Rechtsprechung des BVerfG insbesondere zum Schutz des Kernbereichs privater Lebensführung umgesetzt werden. Nicht in allen Teilen ist dies gelungen.

In den letzten Jahren hat das BVerfG wiederholt Anforderungen an Sicherheitsgesetze formuliert, die den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger sichern sollen. So hatte das BVerfG u.a. die hessische Regelung zur Kennzeichenerkennung im Polizeirecht für nichtig erklärt und die Anforderungen an die Rasterfahndung als nicht verfassungskonform beurteilt. Schließlich gab es mehrere Entscheidungen, in denen das Gericht Anforderungen zum Schutz des Kernbereichs privater Lebensführung formuliert hatte. Über die einzelnen Entscheidungen und die Notwendigkeit der Überarbeitung des HSOG hatte ich in den letzten Jahren wiederholt berichtet (zuletzt 37. Tätigkeitsbericht, Ziff. 4.3.1), zur aktuellen Entwicklung der Rechtsprechung siehe auch Ziff. 1.2.1 sowie Ziff. 1.4.2.

Zu Beginn der neuen Legislaturperiode legten die Fraktionen von CDU und FDP einen Gesetzentwurf vor. Damit wurden den Polizeibehörden auch zusätzliche Instrumentarien, insbesondere im Zusammenhang mit der Nutzung von moderner Kommunikationstechnologie, an die Hand gegeben (so die Begründung des Gesetzentwurfes, LTDrucks. 18/861 S. 10).

Mit einigen Änderungen als Reaktion auf eine vom Innenausschuss des Hessischen Landtages durchgeführte Anhörung wurde das Gesetz im Dezember verabschiedet, so dass es mit Wirkung vom 1. Januar 2010 in Kraft treten konnte.

Aus meiner Sicht ist es nicht in allen Punkten gelungen, die selbst genannten Anforderungen zu erfüllen. Auf einige Aspekte, die auch schon Gegenstand der Anhörung im Landtag waren, möchte ich hier nochmals hinweisen.

4.2.1.1 Vertrauensschutz für Berufsgeheimnisträger

Im Rahmen der Gefahrenabwehr ist jedermann grundsätzlich zur Auskunft verpflichtet es sei denn, er kann sich auf ein Zeugnisverweigerungsrecht - wie im Strafverfahren - berufen. Diese Möglichkeit gibt es allerdings nicht, soweit die Auskunft zur Abwehr einer konkreten Gefahr erforderlich ist. Von dieser Verpflichtung werden nunmehr einzelne Berufsgeheimnisträger befreit.

§ 12 Abs. 2 Satz 2 und 3 HSOG

Unter den in den §§ 52 bis 55 der Strafprozessordnung genannten Voraussetzungen ist eine betroffene Person, die nicht für die Gefahr verantwortlich ist, zur Verweigerung der Auskunft berechtigt. Außer für Rechtsanwälte und in den Fällen des § 53 Abs. 1 Satz 1 Nr. 1, 2, 4 und 5, auch in Verbindung mit § 53a der Strafprozessordnung gilt dies nicht, wenn die Auskunft für die Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist.

Auch wenn die Anforderungen im Rahmen der Gefahrenabwehr andere sind als bei der Strafverfolgung und damit der Gesetzgeber eigenständig differenzierte Regelungen treffen kann, muss nachvollziehbar sein, warum vergleichbare Sachverhalte anders beurteilt werden. Dies folgt aus dem Willkürverbot (vgl. BVerfG - 2 BvR 2438/08 - vom 15. Oktober 2009). Eine Begründung, warum hier zwischen den verschiedenen Gruppen der Berufsgeheimnisträger, denen im Rahmen der Strafprozessordnung ein Zeugnisverweigerungsrecht gewährt wird, differenziert wird, enthält weder der Gesetzentwurf noch ist eine solche im Rahmen des Gesetzgebungsverfahrens ersichtlich geworden.

4.2.1.2 Videoüberwachung

Bei dieser Novellierung bot sich nicht die Gelegenheit, die Vielfalt der Probleme, die sich in der Praxis bei der Umsetzung der vorhandenen Regelungen ergeben haben, aufzugreifen. Allerdings wurden für den Einsatz der Videotechnik durch Polizei und Gefahrenabwehrbehörden zwei Ergänzungen getroffen, die den Sinn dieser Regelungen - mögliche Störer bewusst abzuschrecken und gleichzeitig allen Passanten zu vermitteln, dass diese Örtlichkeit besonders geschützt ist - weiter verstärken.

Die aufgenommene Verpflichtung, mindestens im Abstand von zwei Jahren die Notwendigkeit von festinstallierten Anlagen zu überprüfen, verdeutlicht für die Praxis, dass die Begründung für eine einmal getroffene Entscheidung zur Notwendigkeit einer Videoanlage nicht auf unbestimmte Zeit Geltung haben kann. Selbstverständlich galt auch bisher im Prinzip schon, dass die Erforderlichkeit für die vollständige Dauer des Einsatzes vorhanden sein musste und nicht nur zum Zeitpunkt der Entscheidung über die Errichtung. Die Praxis hat jedoch gezeigt, dass das Hinterfragen der Notwendigkeit des Einsatzes nach einer gewissen Zeit eher die Ausnahme war.

Inwieweit dies nunmehr zu einer geänderten Praxis und nicht nur zu einer routinemäßigen Verlängerung nach Ablauf der zwei Jahre führt, wird sich erweisen. Dazu beitragen können nicht zuletzt die noch zu erlassende Verwaltungsvorschrift zur Ausführung des HSOG sowie eine Überarbeitung der Handlungsempfehlungen des Landeskriminalamtes für die Errichtung von Videoüberwachungsanlagen.

Von Beginn an habe ich Transparenz für den Einsatz der Videotechnik verlangt: Der überwachte Bereich sollte kenntlich gemacht und auf den Schildern auch die Stelle bezeichnet werden, die den Einsatz verantwortet. In der Praxis wurde dies in aller Regel auch so umgesetzt. Nunmehr ist eine Verpflichtung dazu in das Gesetz aufgenommen worden.

4.2.1.3 Kernbereichsschutz bei der Wohnraumüberwachung

Bei aller Schwierigkeit, die vom BVerfG formulierten Anforderungen zum Umgang mit Daten aus dem Kernbereich privater Lebensführung in die gesetzlichen Grundlagen für Eingriffsmaßnahmen umzusetzen, erscheint mir die für den Bereich der Wohnraumüberwachung nunmehr geltende Regelung als nicht ausreichend.

§ 15 Abs. 4 S. 4 HSOG

Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Bestehen insoweit Zweifel, darf die Datenerhebung ausschließlich durch eine automatische Aufzeichnung erfolgen und fortgesetzt werden.

Eine Konstellation, dass beim Abhören gar keine Inhalte erfasst werden, die nicht dem Kernbereich zuzuordnen sind, ist kaum vorstellbar. Dies wäre etwa der Fall, wenn davon auszugehen ist, dass innerhalb einer Wohnung nur gebetet und ansonsten geschwiegen wird - selbst bei der Begrüßung von Gästen. Die als Beschränkung formulierte Anforderung wird in der Praxis vermutlich dazu führen, dass es nie zur Ablehnung eines Einsatzes aus diesem Grund kommen wird.

4.2.1.4 Telekommunikationsüberwachung an informationstechnischen Systemen (Quellen-TKÜ)

Das HSOG enthält nunmehr eine Rechtsgrundlage für den heimlichen technischen Eingriff in ein informationstechnisches System (sog. Quellen-TKÜ). Dabei gibt es ersichtlich Parallelen zur umstrittenen Online-Durchsuchung. Denn auch wenn (nur) das gesprochene Wort im Rahmen einer bestehenden Telekommunikationsverbindung aufgezeichnet werden soll, bevor es (verschlüsselt) über das Internet weitergegeben wird, ist die eingesetzte Technik vergleichbar, wenn nicht identisch. Meine Bedenken zum Einsatz solcher Technologien durch den Staat habe ich schon mehrmals zum Ausdruck gebracht (vgl. 37. Tätigkeitsbericht, Ziff. 1.3 und 9.1 sowie 36. Tätigkeitsbericht, Ziff. 1.3.3 und 4.1). Dabei bin ich mir durchaus bewusst, dass die weiter entwickelten Technologien und der Einsatz solcher Möglichkeiten durch Störer die Tätigkeit der Gefahrenabwehr vor immer neue Herausforderungen stellt, und dabei die Frage, ob überhaupt abgehört werden darf, in dem rechtlich vorgegebenen Rahmen entschieden werden soll.
Angesichts der Problematik des heimlichen Eindringens in die Hardware der Überwachten macht es für mich allerdings grundsätzlich keinen Unterschied, ob damit Zugriff auf die Inhalte eines Telekommunikationsvorgangs genommen wird oder auf andere auf dem überwachten Gerät vorhandene Informationen.

§ 15b HSOG

(1) Wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist, kann die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(3) Bei jedem Einsatz des technischen Mittels sind zum Zwecke der Datenschutzkontrolle und der Beweissicherung zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um der betroffenen Person oder einer hierzu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme nach Abs. 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, wenn sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

(4) Die Maßnahme darf sich nur gegen eine Person richten, die nach den §§ 6 oder 7 verantwortlich ist. Sie darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(5) § 15 Abs. 4 Satz 2 bis 5 und Abs. 5 gilt entsprechend mit der Maßgabe, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist.

4.2.1.5 Rasterfahndung

Das Gesetz hat im Prinzip die Formulierung des BVerfG aufgenommen und als Schwelle für den Einsatz einer Rasterfahndungsmaßnahme die konkrete Gefahr definiert. Damit ist klargestellt, dass die Rasterfahndung nicht mehr als eine - vom Bundesverfassungsgericht für unzulässig erklärte - Vorfeldmaßnahme eingesetzt werden kann.

§ 26 HSOG

Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn dies zur Abwehr der Gefahr erforderlich ist.

Das BVerfG hatte zudem formuliert, dass eine Sachlage vorausgesetzt wird, bei der im konkreten Fall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ein Schaden für diese Rechtsgüter eintreten wird. Die für die Feststellung einer konkreten Gefahr erforderliche Wahrscheinlichkeitsprognose müsse sich dabei auf Tatsachen beziehen. Vage Anhaltspunkte oder bloße Vermutungen ohne greifbaren, auf den Einzelfall bezogenen Anlass reichen nicht aus. Der Entwurf der FDP-Fraktion aus der letzten Legislaturperiode hatte daher noch eine Ergänzung vorgesehen: "wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich und dies auf andere Weise nicht möglich ist". Damit wäre m.E. den vom BVerfG formulierten Anforderungen besser Rechnung getragen.

4.2.2 SoPart - Automationsunterstützung für Soziale Dienste in der Justiz

Das Verfahren SoPart habe ich im Einsatz bei der Bewährungshilfe überprüft. Daraus ergab sich Nachbesserungsbedarf. Durch den geplanten Einsatz auch für die Sozialen Dienste in den Vollzugsanstalten sind weitere Aspekte hinzugekommen.

In diesem Jahr habe ich mich über das Verfahren SoPart bei einer Bewährungshilfe informiert. Es ging auch um Art und Weise, wie die Tätigkeit von Bewährungshelfern unterstützt aber auch vorgegeben wird. Zu den Ergebnissen habe ich mit den beteiligten Stellen Gespräche geführt, die dann auch zu Änderungen am Verfahren und in den Abläufen geführt haben. Ende des Jahres hat man mich darüber in Kenntnis gesetzt, dass das Verfahren auch in Justizvollzugsanstalten eingesetzt werden soll. Durch die Integration ergeben sich neue Anforderungen.

4.2.2.1 Das Verfahren SoPart

4.2.2.1.1 Funktion

SoPart soll die Bewährungshelfer in der täglichen Arbeit unterstützen. Es soll einfach möglich sein, aktuelle Daten zu Personen und Institutionen zu erhalten, mit denen die Bewährungshelfer bei ihrer Arbeit Kontakt haben. Außerdem sollen die Bewährungshelfer in der Arbeit mit den Klienten nötige Hilfsmittel erhalten. Mit dem Verfahren SoPart sollen die Bewährungshelfer zudem ihre gesamte Tätigkeit im einzelnen Fall dokumentieren. Deshalb bietet das Verfahren sowohl die Möglichkeit, Statusinformationen zum Einzelfall, als auch unterschiedlichen Schriftverkehr sowie Notizen, beispielsweise zu Gesprächen, zu erfassen. Urteile oder Schreiben an den Bewährungshelfer werden weiterhin in einer Papierakte vorgehalten. Insofern arbeiten Bewährungshelfer mit einer Hybridakte aus dem in SoPart geführten elektronischen Teil und der Papierakte. Solchen Hybridakten sind Probleme immanent, z.B. die Abgabe von (vollständigen) Akten bei einem Wohnungswechsel in ein anderes Bundesland.

Um die elektronische Akte einer anderen Stelle in Hessen zur Verfügung stellen zu können, muss sie durch die bisher zuständige Stelle geschlossen werden. Dann können die Zugriffsrechte an den dann Zuständigen übergeben werden.

4.2.2.2 Basisdaten

Eine wesentliche Rolle spielt der behördenübergreifend allen hessischen Stellen der Bewährungshilfe zur Verfügung stehende Datenbestand, der als "Basisdaten" bezeichnet wird. Es sollen Doppelerfassungen vermieden werden und von einer Stelle der Bewährungshilfe einmal erfasste Informationen sollen bei einem Zuständigkeitswechsel nicht immer wieder neu erhoben werden müssen, sondern von der einen an die andere Stelle übergeben werden. Schließlich wurde von den Anwendern vorgetragen, sie müssten informiert sein, ob ein Klient auch schon bei einer anderen Stelle vorstellig geworden sei bzw. dort schon (früher) als Klient geführt wurde. Ob dies als Begründung für eine gemeinsame Datenbank der Bewährungshelfer bei allen Landgerichten ausreicht, ist immer noch Gegenstand der Erörterungen zu diesem Verfahren mit der Justizverwaltung. Für eine landesweite Suche ist es zunächst nötig, bestimmte Basisdaten behördenübergreifend zum Zugriff für alle Anwender zur Verfügung zu stellen. Dieser Kerndatensatz war sehr umfangreich. Er galt auch für sonstige Personen wie Rechtsanwälte oder Mitarbeiter und für Institutionen.
Gespeichert werden beispielsweise Name, Adressen und Telefonnummern sowie Geburtsdaten bei Klienten. Auf weitere Daten zu Klienten oder Mitarbeitern können nur zuständige und berechtigte Nutzer zugreifen.

Da der Datenbestand hessenweit verschiedenen Stellen zur Verfügung steht, handelt es sich um ein gemeinsames Verfahren nach § 15 HDSG. Das deshalb notwendige Verfahren einschließlich der Festlegungen der Verantwortlichkeiten ist noch nicht abgeschlossen.

4.2.2.3 Technik des Verfahrens

Eine vollständige Beschreibung der Technik des Verfahrens kann und soll hier nicht gegeben werden. Ich möchte jedoch einige Themen skizzieren.

Grundstruktur
SoPart ist eine Terminalserver-Anwendung. Die Daten werden in Hünfeld in einer Oracle-Datenbank gespeichert. Auch die Programme laufen dort auf Terminalservern. Ein Bewährungshelfer greift von seinem Arbeitsplatz aus mit der Kommunikationssoftware Citrix über das Justiznetz auf die Programme zu. Die Datenübertragung wird durch Citrix verschlüsselt. Damit sind Datenschutzforderungen umgesetzt.

Anmeldung am Verfahren
Um mit dem Verfahren arbeiten zu können, muss sich ein Benutzer zuerst am Terminal-Server anmelden und als zweiten Schritt an der Anwendung selbst. In der Version von Anfang 2009 wurde für SoPart ein 8-stelliges Passwort verlangt, das im Unterschied zur Terminalserveranmeldung nicht alle Anforderungen aus den Grundschutzkatalogen des BSI erfüllte. Jetzt ist beabsichtigt, die bei der Anmeldung am Terminalserver geprüfte Benutzerkennung an SoPart weiterzureichen und das Programm ohne weitere Passwortabfrage zu starten. Dieser Ansatz ist akzeptabel, solange die Anmeldung am Terminalserver die Anforderungen aus den Grundschutzkatalogen des BSI erfüllt und die Anzahl der gestarteten Programme nicht zu hoch ist. Dies wäre zurzeit erfüllt. Zusätzlich wird der passwortgeschützte Bildschirmschoner nach 15 Minuten aktiviert.

Protokollierung
Alle Lesezugriffe auf die Falldaten werden protokolliert. Dies gilt für Zugriffe bei der Sachbearbeitung innerhalb der Behörde, aber auch für Lesezugriffe durch andere Behörden, die eine Datenübermittlung darstellen. Eine Aufstellung der Lesezugriffe auf Probanden eines Bewährungshelfers wird nicht automatisch erstellt, sondern muss jeweils durch ihn angestoßen werden.
Das Ergebnis wird als Dokument zur Verfügung gestellt. Die Protokolldaten lagen von mehr als zwei Jahren vor. Die Speicherdauer wird dahingehend präzisiert, dass die Dokumentation von Datenübermittlungen bis zum Ende des auf die Über-

mittlung folgenden Kalenderjahres vorliegt, während Protokolle zu dienststelleninternen Zugriffen maximal sechs Monate vorliegen.

Suchanfragen werden nicht protokolliert. Da die Anzeige von Treffern beispielsweise Name, Geburtsdatum und Anschrift von Probanden anderer Stellen umfasst, handelt es sich bereits vor dem Zugriff über das "i"-Icon um eine Datenübermittlung. (s. Ziff. 4.2.2.5)

Ändernde Zugriffe werden in der Änderungshistorie protokolliert.

4.2.2.4 Organisatorisches Umfeld

Die HZD betreibt das Verfahren nach den Vorgaben der Justizverwaltung. Insbesondere das Anlegen von Benutzern, das die Behördenleitung des jeweiligen Landgerichts veranlassen kann, oder neuen Mandanten wird durch die Gemeinsame IT-Stelle der Justiz vorgenommen. Die Abläufe mussten noch überarbeitet werden, da nicht dokumentiert war, wann welcher Benutzer aufgrund welchen Auftrags angelegt wurde und welche Zugriffsrechte dieser erhalten hat. So war es möglich, telefonisch einen Auftrag zu geben. Selbst wenn in Eilfällen diese Möglichkeit vorgesehen sein sollte, muss eine schriftliche Bestätigung folgen. Im System waren die Eintragungen nachvollziehbar dokumentiert.

4.2.2.5 Problempunkt Suchfunktion

Zur Unterstützung der Bewährungshelfer ist eine Suchfunktion vorhanden. In der ursprünglichen Ausgestaltung konnte ein Benutzer über den gesamten Bestand an gespeicherten Personen suchen und auf die Stammdaten zugreifen. Personengruppen waren neben den Klienten auch Bewährungshelfer, Anwälte und andere Personen. Die Suche konnte über alle Gruppen erfolgen oder auf einzelne Gruppen eingeschränkt werden. Die Suchfunktion selbst war praktisch nicht eingeschränkt. Es war beispielsweise möglich, sich unter Eingabe eines Buchstabens alle Personen anzeigen zu lassen, deren Familienname mit dem Buchstaben beginnt. Die Trefferliste zeigt die Namen gespeicherter Personen. Weitergehende Daten sind in dieser Anzeige nicht vorhanden. Die Suchanfrage wird bis zu diesem Zeitpunkt nicht protokolliert.

Aus der Trefferliste kann dann ein Eintrag ausgewählt werden. Durch Anklicken eines Icons ("i" für Information) werden weitere Stammdaten angezeigt. Hierzu gehören:

- Adresse inkl. einer Adresshistorie,
- Kommunikationsdaten wie E-Mail, Handynummer (auch mit Notizen) nicht nur des Probanten, sondern auch von Kontaktpersonen wie Partner, Freunde oder Verwandte,
- zuständige Behörde und Bewährungshelfer,
- Änderungshistorie. Es wird bei Änderungen nicht der Name des Bearbeiters, sondern die PID vermerkt. Die PID (Personal Identifier) ist die Nummer des Datenbankeintrags mit den Stammdaten des Mitarbeiters.

Dieser Zugriff, auch dienststellenintern, auf die Stammdaten wird protokolliert.

Es gab technisch die Möglichkeit, Daten auszublenden. Dies war beispielsweise bei den Daten zu Mitarbeitern der Fall. Ich habe gefordert, generell den Umfang der angezeigten Daten zu reduzieren.

Die Begründung für eine Suche nach Klienten war die Vermeidung von Doppelerfassungen. Wenn ein Bewährungshelfer die Daten zu einem Klienten erfasst, der vor ihm sitzt, soll er erkennen können, ob er schon erfasst wurde. Ich stehe noch in Diskussionen mit dem Justizministerium, ob hier die oben beschriebene Suchfunktion sinnvoll ist, oder bei der Erfassung an Hand bestimmter Datenbankfelder wie Namen und Geburtsdatum automatisch auf mögliche "Dubletten" hingewiesen wird; dabei müssten natürlich Zahlendreher oder einfache Schreibfehler erkannt werden.

4.2.2.6 Erweiterung auf die Sozialen Dienste im Justizvollzug

Zukünftig soll das Verfahren auch in den Justizvollzugsanstalten zum Einsatz kommen. Die von den Mitarbeitern der sozialen Dienste zu führenden Teile der Gefangenenpersonalakte sollen im Verfahren SoPart verarbeitet werden. Damit werden nicht nur zahlenmäßig mehr Stellen an diesem Verfahren beteiligt sein.

Der geplante Einsatz des Verfahrens im Justizvollzug sieht darüber hinaus - neben der Suchfunktion - weitere gemeinsame Zugriffe vor. Die derzeit im Landtag beratenen neuen Vollzugsgesetze sehen im Rahmen der Entlassungsvorbereitung eine verstärkte Zusammenarbeit der Sozialen Dienste in den Anstalten mit den Bewährungshelfern vor. Zukünftig sollen diese schon sechs Monate vor der vermutlichen Entlassung mit einbezogen werden. In diesem Kontext benötigen sie dann auch - zumindest teilweise - die in SoPart gespeicherten Informationen über den einzelnen Gefangenen. Durch diese gesetzliche Aufgabenzuweisung ist grundsätzlich die Notwendigkeit des Zugriffs auf ein gemeinsames Verfahren im Rahmen des § 15 HDSG gegeben. Für die konkrete Ausgestaltung des Verfahrens muss jedoch differenziert analysiert werden, wer zu welchem Zeitpunkt auf welche Dokumente einer anderen Stelle zugreifen darf. Als Anhaltspunkt können zum einen die derzeit auf herkömmlichem Wege stattfindenden Informationsaustausche zwischen den Beteiligten diesen. Für die erweiterte Tätigkeit der Bewährungshelfer im Rahmen der Entlassungsvorbereitung muss die Notwendigkeit des Zugriffs auf die einzelnen Dokumente noch analysiert werden. Im Übrigen muss auch differenziert werden zwischen dem Zugriff während der Entlassungsvorbereitung und in der Zeit danach. Da die von den Sozialen Diensten gespeicherten Unterlagen als Teil der Gefangenenpersonalakte anzusehen sind, darf nach der Entlassung aus der Anstalt ein Zugriff auf diese Dokumente nicht mehr erfolgen. Soweit notwendig muss eine Transformation der Dokumente in die Dokumentation des dann zuständigen Bewährungshelfers erfolgen.

4.2.3 Neue Formen der Zusammenarbeit zum Umgang mit "Gewalt-Kids"

Auch in Hessen hat die Diskussion um die zunehmend wahrgenommene Kriminalität Jugendlicher dazu geführt Modelle zu entwickeln, um diese effektiver zu bekämpfen. Wiederholt bin ich um Beratung gebeten worden, wie man mit veränderten Formen der Zusammenarbeit diesem Thema besser gerecht werden kann.

Eine Vielzahl von Institutionen und Behörden beschäftigt sich mit Problemen von Kindern und Jugendlichen. Das reicht von der Schule, dem Jugendamt und den unterschiedlichsten freien Trägern bis hin zu Polizei und Gericht. Der Vielzahl dieser Stellen korrespondiert eine Vielzahl rechtlicher Regelungen. Diese betreffen u.a. das Zusammenwirken der verschiedenen Stellen. Dabei setzten datenschutzrechtliche Regelungen der Zusammenarbeit Grenzen. So ist einerseits gerade im Bereich der Jugendhilfe der Gedanke der ganzheitlichen Betreuung ein wesentlicher Gesichtspunkt. Andererseits wirken vor allem die Regelungen des Sozialdatenschutzes und das sog. Sozialarbeitergeheimnis (abgeleitet aus § 203 Abs. 1 Nr. 5 StGB) wie ein enges Korsett, das eine Zusammenarbeit nicht einfach macht.

§ 203 Abs. 1 Nr. 5 StGB

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
…
5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
…
anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Für Polizei und Strafverfolgungsbehörden als klassische Eingriffsverwaltung gilt zudem, dass für ihr Tätigwerden immer eine gesetzliche Grundlage vorhanden sein muss. Auch die Erhebung von Daten darf nur jeweils zur Erfüllung einer konkreten Aufgabenstellung erfolgen. Erst recht für diesen Bereich gilt zudem der Grundsatz, dass eine Erhebung von Daten auf Vorrat unzulässig ist. Dies läge etwa vor, wenn ein Mitarbeiter eines Jugendtreffs seine Erkenntnisse über einen Jugendlichen einem Staatsanwalt erzählt, nur weil es sein könnte, dass der Jugendliche seine Streiche irgendwann übertreibt und dann strafbare Handlungen begeht.

Andererseits hat die Entwicklung gezeigt, dass auch neue oder andere Wege gesucht werden müssen, um mit den auftretenden Fragestellungen umzugehen - Jugendlichen Hilfe anzubieten ist dabei ebenso relevant wie die Durchsetzung des staatlichen Strafanspruchs, auch im Interesse aller Bürgerinnen und Bürger.

Nicht immer gelingt es ohne Weiteres, Überlegungen und Ansätze, die von den jeweiligen Fachleuten für sinnvoll erachtet werden, in die vorgegebenen Strukturen einzupassen.

Ein in diesem Kontext häufig verwendetes Instrument ist die Fallkonferenz. Dabei ist jedoch zu beachten, dass sich dahinter die unterschiedlichsten Ideen verbergen. Deshalb kann auch eine für das Projekt A gefundene Lösung nicht ohne Weiteres auf andere Projekte übertragen werden.

Für alle diese Projekte können abstrakt nur zwei Maßgaben formuliert werden: Zunächst muss sorgfältig analysiert werden, ob es eine Rechtsgrundlage für den konkret gewünschten Informationsfluss gibt - wenn nicht, kann allenfalls mit allen dabei auftretenden Schwierigkeiten das Instrument der Einwilligung weiterhelfen. Und schließlich ist für jeden einzelnen Kontakt zwischen den beteiligten Institutionen, ebenso wie für die einzelnen konkret agierenden Personen, immer zu fragen, ob gerade das, was im Moment getan wird, erforderlich für diesen konkreten Fall/für diese Situation ist.

In diesem Kontext haben meine Mitarbeiter in der Vergangenheit u.a. zwei konkrete Projekte näher begleitet:

4.2.3.1 Haus des Jugendrechts

In anderen Bundesländern arbeiten solche Einrichtungen schon seit einigen Jahren in unterschiedlicher Art und Weise.
Im Jahre 2008 wurde federführend durch das HMDJ eine Arbeitsgruppe gebildet, die beispielhaft für Frankfurt die Möglichkeiten und die Struktur einer solchen Einrichtung erarbeiten sollte. Ich war gebeten worden, diese Arbeit von Anfang an zu begleiten. Dazu hatte ich u.a. in einem Arbeitspapier die Anforderungen aus Sicht des Datenschutzes für die Zusammenarbeit in einem Haus des Jugendrechts zusammengefasst.

Grds. gilt für die Zusammenarbeit aller beteiligten Stellen: Ein konkreter personenbezogener Informationsaustausch ist immer dann zulässig, wenn er im Rahmen der (auch jetzt schon) anzuwendenden Rechtsgrundlagen erfolgt (insbesondere SGB VIII, SGB X, JGG, StPO; HDSG).
Bei der Gestaltung der Zusammenarbeit sind daher zwei Komplexe zu betrachten:

1. Die allgemeine konzeptionelle Arbeit aller Beteiligter
   Diese kann sich in unterschiedlicher Form organisieren, der Kreis der Beteiligten kann variieren, kann auch Personen/Institutionen umfassen, die nicht in konkreten Fällen mitarbeiten. In diesen Kontext gehört auch die allgemeine Präventionsarbeit im Stadtteil an Schulen etc.
   Wichtig ist, dass in diesem Bereich in der Regel keine personenbezogenen Daten von Jugendlichen in der Diskussion benötigt werden.

2. Die Arbeit am einzelnen Fall
   Ein Austausch über einen Jugendlichen kann jeweils (nur) zwischen den zuständigen Mitarbeitern der Institution erfolgen, die (zu diesem Zeitpunkt) für die Bearbeitung des Falles zuständig sind. Es kann daher nicht eine allgemeine Fallkonferenz geben, sondern die Zusammensetzung/Beteiligung ist für jeden Einzelfall festzulegen. (Was nicht ausschließt dass es eine Vorgabe für die Regelzusammensetzung - Polizei-, StA-, JGH-Mitarbeiter - gibt, im Rahmen ihrer örtlichen Zuständigkeit für alle Fälle in diesem Komplex.)
   Auswirkungen bzw. jeweils im Einzelfall konkreter Entscheidungsbedarf ergeben sich daraus insbesondere für die Einschaltung der freien Träger zur Frage, ob und welche Maßnahmen für einen bestimmten Jugendlichen sinnvoll und möglich sind.
   Die grundsätzliche Frage, ab welchem Zeitpunkt und in welchem Umfang die Beteiligung eines freien Trägers bzw. die Übermittlung von Daten an diesen erfolgen kann, stellt sich für jeden Einzelfall unabhängig davon, ob immer ein bestimmter Träger für alle Fälle oder für bestimmte Fallkonstellationen herangezogen wird, genauso aber auch für die angedachte Bündelung über eine "Kopfstelle".
   Bei allen Besprechungen - aber auch bei der Weitergabe von Akten - ist zu beachten, dass im Einzelfall auch Daten weiterer Beteiligter - sei es aus dem Tatkomplex, der zu bearbeiten ist, sei es aus der Familie der Jugendlichen - Gegenstand sein könnten. Auch deren Interesse auf Schutz ihrer persönlichen Daten ist zu beachten.

Für die Einrichtung eines Hauses des Jugendrechts gibt es zudem auch in der Planungsphase eine Vielzahl von Fragestellungen, bei denen von Anfang an auch datenschutzrechtliche Aspekte zu berücksichtigen sind.

- Bauliche Gestaltung - Zimmerbedarf
  Gibt es gemeinschaftlich genutzte Büros, Geschäftstelle?
  Büros, in denen Einzelgespräche geführt werden können?
  Räumlichkeiten/Schränke zur Aufbewahrung der Akten

- Organisatorische Fragen
  Schließanlage - gemeinsam, getrennt,
  Putzdienst - wer ist verantwortlich für die notwendigen Vereinbarungen zur Vertraulichkeit etc.
  IT-Infrastruktur, getrennte Netze?; Gemeinsamer Serverraum?

Die Arbeitsgruppe hat zunächst die grobe Konzeption einer solchen Einrichtung beschrieben. Darin waren zwar noch keine konkreten Maßnahmen zur Sicherstellung des Rechts auf informationelle Selbstbestimmung enthalten. Es war jedoch festgehalten, dass jeweils alle Beteiligten selbst für die Einhaltung der für sie geltenden Datenschutznormen verantwortlich bleiben. Zudem ist vorgesehen, dass zeitnah zur Eröffnung des Hauses eine gemeinsame Schulung zum Thema Datenschutz erfolgen soll.

Im Berichtsjahr hat nunmehr die Arbeit zur konkreten Umsetzung begonnen. Dazu gehören, neben dem Umbau der Immobilie und den sich daraus ergebenden - vor allem technischen - Fragen, Überlegungen zum konkreten Umgang miteinander bzw. zur (gemeinsamen) Fallbearbeitung. Derzeit versuchen daher die Mitarbeiter, die zukünftig für die beteiligten Ämter im Haus des Jugendrechts tätig sein sollen, Vorschläge für die alltägliche Arbeit zu formulieren: wer ist wann zu beteiligen, wann ist er erreichbar, wie wird der Umlauf der Akten organisiert und Ähnliches. Auch hier bin ich wieder beratend beteiligt.

4.2.3.2 Vorschlag einer Fallkonferenz als Ergebnis der Arbeit eines kommunalen Präventionsrates

In einem Landkreis hatte sich - angestoßen vom Präventionsrat - eine Arbeitsgruppe gebildet, die sich schwerpunktmäßig mit Jugendlichen und Kindern beschäftigen will, die (noch) nicht straffällig geworden sind oder bei denen derzeit keine aktuellen Verfahren laufen, die aber in vielfältiger Weise auch schon mit den beteiligten Stellen in Kontakt gekommen sind. Beteiligt waren u.a. Jugendamt, Bewährungshilfe, Polizei, Jugendrichter, Kreisjugendring und Sozialarbeiter der Caritas.

Vorgesehen war ein Angebot an die betroffenen Jugendlichen/Kinder und auch an deren Eltern. Ziel war ein schnelles, unbürokratisches Hilfsangebot durch die enge Zusammenarbeit der beteiligten Stellen und die Bündelung von Maßnahmen und Hilfen. Am Ende einer solchen Fallkonferenz sollte idealiter ein Konzept stehen, welchem der oder die Betroffene freiwillig zustimmt. Er bzw. sie soll dies als Chance begreifen, um den "üblichen" negativen Entwicklungen entgegenzuwirken. Daher war nicht ausgeschlossen, dass die Betroffenen zumindest zeitweise direkt beteiligt werden könnten.

Dieses Modell ist eng an das Instrument der Hilfeplanung im Rahmen der Jugendhilfe angelehnt. Allerdings sollte hier verstärkt der Aspekt der Verhinderung von (weiteren) Delikten mit einbezogen und deshalb auch die Teilnahme etwa der im Rahmen der Prävention örtlich tätigen Polizeibeamten vorgesehen werden.

Von Anfang an war klar, dass in aller Regel das Instrument der Einwilligung zum Tragen kommen muss. Der gemeinsame Austausch ist sonst kaum möglich. Denn eine wirkliche Anonymisierung, um abstrakt über ein Hilfeangebot sprechen zu können, ist kaum vorstellbar; zumal gerade im ländlichen Raum die Betroffenen bzw. auch ihre Familien häufig in den Institutionen bekannt sind.

Bei der Ausgestaltung der Einwilligung wurden dann die Schwierigkeiten deutlich: Es ist eine Differenzierung notwendig, die die Verständlichkeit der Einwilligungserklärung nicht unbedingt erleichtert.
Notwendig ist die konkrete Beschreibung der Personen, zu deren Gunsten eingewilligt werden soll. Nicht außer Acht zu lassen ist zudem - gerade im Bereich der Jugendlichen - die Frage, wer muss einwilligen. Dabei ist die Einwilligungsfähig-

keit ebenso wie die besondere Problematik der Einbeziehung der Eltern - die in aller Regel ja auch inhaltlich betroffen sind - nie abstrakt zu beantworten.

Einwilligungserklärung zur Verwendung meiner Daten

Hiermit willige ich ein, dass meine personenbezogenen Daten im Rahmen einer Fallkonferenz den unten genannten Teilnehmern mitgeteilt werden.

Zu den personenbezogenen Daten gehören: Name, Anschrift, Telefonnummer, Alter, Name der Eltern und Geschwister, Schule oder Ausbildungsbetrieb, ...

(nicht zutreffendes streichen ggfs. weitere Daten ergänzen)

Ich möchte, dass die Teilnehmer der Fallkonferenz auch ohne mein Beisein über diese Daten verfügen und sich darüber austauschen können.

Die Daten sind nur für die Dauer der Fallkonferenz und anschließend zeitlich begrenzter und mir bekannter Maßnahmen der Teilnehmer verwendbar, danach werden sie vernichtet.

Teilnehmer der Fallkonferenz sind:

–	Jugendamt	–	Jugendhelfer
–	Bewährungshilfe	–	
–	Polizei	–	

Sollten sich Änderungen in der Teilnehmerliste, den verwendeten Daten oder dem Datenumfang ergeben, so kann ich erneut über die Einwilligung entscheiden. Entsprechende Änderungen müssen dokumentiert werden. Ich weiß, dass ich diese Einwilligungserklärung und die Entbindungserklärung jederzeit widerrufen kann und auch die Unterschrift verweigern könnte.

O Insbesondere befreie ich aber auch folgendeTeilnehmer widerruflich von der ihnen obliegenden Schweigepflicht:

O	Jugendamt/Sozialarbeiter	O	Suchtberater
O	Bewährungshelfer	O	
O	Jugendberater	O	

Einwilligungserklärende/r: Gesetzlicher Vertreter:

Ort/Datum:

(Jugendliche ab 14.Lebensjahr können diese Erklärung selbst abgeben, wenn sie die notwendige Einsichtsfähigkeit in die Bedeutung der Erklärung besitzen. Andernfalls müssen die gesetzlichen Vertreter, wie bei den Kindern unter 14 Lebensjahren die Erklärung unterzeichnen.)

Nicht zuletzt wegen der beschriebenen Komplexität ist es bis jetzt noch nicht zu einer Umsetzung des Konzepts gekommen.

4.3 Verfassungsschutz

4.3.1 Neues Datenverarbeitungssystem HARIS beim Hessischen Landesamt für Verfassungsschutz

Das Hessische Landesamt für Verfassungsschutz plant den Einsatz eines neuen Datenverarbeitungssystems. In die Planung und Umsetzung werde ich einbezogen.

Neben dem Nachrichtendienstlichen Informationssystem (NADIS), an dem sich das Bundesamt für Verfassungsschutz und alle Landesämter für Verfassungsschutz beteiligen, betreibt das Hessische Landesamt für Verfassungsschutz seit vielen Jahren eigene Amtsdateien. Während NADIS bis jetzt in erster Linie zum Auffinden der zu einer Person angelegten Akte dient, also vor allem ein Aktenhinweissystem darstellt, können in den Amtsdateien die zu einer Person oder zu einem Objekt gehörenden Texte und Informationen direkt eingespeichert werden. In Hessen war die wichtigste Arbeitsdatei lange Zeit LARGO, über die ich zuletzt im 31. Tätigkeitsbericht (Ziff. 8.4.1) berichtete. Während LARGO zunächst für die Speicherung von Informationen für alle Aufgaben des Verfassungsschutzes zur Verfügung stand, kam dann später für den Aufgabenbereich der Beobachtung von Bestrebungen der Organisierten Kriminalität das Datenverarbeitssystem CRIME hinzu.

Mit dem nunmehr geplanten Hessischen Analyse- und Recherchesystem (HARIS) soll wieder ein einheitliches Datenverarbeitungssystem geschaffen werden. Mit Ausnahme des Bereichs der Mitwirkung des HLFV bei der Sicherheitsüberprüfung bei Personen des öffentlichen Dienstes werden Daten aus allen anderen Aufgabenbereichen des Verfassungsschutzes in HARIS eingespeichert. Aus Sicht des Verfassungsschutzes bietet HARIS im Vergleich zu seinen beiden Vorgängersystemen CRIME und LARGO durch den Einsatz einer neuen Technologie, die auf einem Wissensnetz basiert, beträchtliche Vorteile. Durch variable Verknüpfungsmöglichkeiten und insbesondere deren graphischer Darstellung werden die erforderlichen Auswertungen wesentlich effizienter.

Derzeit ist nicht vorgesehen, die Papierakte des HLFV durch HARIS zu ersetzen. Vor jeder Entscheidung eines Mitarbeiters des Verfassungsschutzes ist nach wie vor die Akte zu der betreffenden Person oder Organisation heranzuziehen.

HARIS läuft seit Sommer d.J. als Pilotprojekt mit Echtdaten. Ich werde in die Planung und Umsetzung einbezogen.

4.3.2 Verwaltungsvorschriften des Hessischen Landesamtes für Verfassungsschutz

Das Hessische Landesamt für Verfassungsschutz erarbeitet im Zusammenhang mit dem Hessischen Innenministerium neue untergesetzliche Vorschriften, die seine Tätigkeit regeln. Daran werde ich von Anfang an beteiligt.

Gründe für die Überarbeitung bestehender und die Erarbeitung neuer Vorschriften sind zum einen Änderungen des zuletzt im Jahr 2007 novellierten Gesetzes über das Hessische Landesamt für Verfassungsschutz (36. Tätigkeitsbericht, Ziff. 3.1) aber auch Anpassungen an die praktische Tätigkeit des Hessischen Landesamtes für Verfassungsschutz. Zudem bedingt die Einführung der Amtsdatei HARIS (s.o.) eine Reihe neuer Regelungen.

Bisher wurden mir Vorschriften sowohl für den Bereich der Auswertung als auch den der Beschaffung von Informationen durch das HLFV vorgelegt.

In den Vorschriften über die Auswertung werden die Voraussetzungen, unter denen Informationen erhoben, gespeichert und gelöscht werden - unterhalb der gesetzlichen Normen - geregelt.

Die Vorschriften über die Beschaffung regeln Einzelheiten der Gewinnung von Informationen durch die Nutzung nachrichtendienstlicher Mittel, also insbesondere Observationen, Einsatz von Vertrauenspersonen und Einsatz technischer Maßnahmen, wie z.B. Abhörvorrichtungen. Da die Vorschriften als Verschlusssachen eingestuft sind, beschränke ich mich auf die Feststellung, dass der größte Teil meiner datenschutzrechtlichen Verbesserungsvorschläge akzeptiert wurde.

4.4 Verkehrswesen

4.4.1 Anlassunabhängige personenbeziehbare Kontrollen der Prüfer von Kfz durch staatliche Aufsichtsbehörden

Amtlich anerkannte Überwachungsorganisationen zur Durchführung von Hauptuntersuchungen und Sicherheitsprüfungen nach der Straßenverkehrszulassungsordnung müssen der Aufsichtsbehörde auf Verlangen ihren jährlichen Revisionsbericht mit pseudonymisierten Angaben über die Tätigkeit der einzelnen Prüfingenieure in elektronischer Form vorlegen.

Zur Überwachung der ordnungsgemäßen und gleichmäßigen Durchführung der amtlichen Fahrzeuguntersuchungen verlangte das Regierungspräsidium Darmstadt vom DEKRA e.V., den jährlichen Revisionsbericht in elektronischer Form vorzulegen. Der Bericht enthält für jeden Prüfingenieur eine Auflistung der von ihm im Revisionszeitraum festgestellten Fahrzeugmängel. Die Prüfingenieure sind in dem Bericht zwar nicht mit Namen, sondern mit Nummern aufgeführt. Der DEKRA e.V. kann jedoch jederzeit die dahinter verborgene Person identifizieren. Der Gesamtbetriebsrat der DEKRA sah in der beabsichtigten Datenerhebung des Regierungspräsidiums eine unzulässige Leistungs- und Verhaltenskontrolle und bat mich um datenschutzrechtliche Überprüfung.

4.4.1.1 Verarbeitung personenbezogener Daten

Der DEKRA e.V. als amtlich anerkannte Überwachungsorganisation freiberuflicher Kfz-Sachverständiger nach Anlage VIIIb StVZO und die durch ihn betrauten Prüfingenieure sind mit der Wahrnehmung hoheitlicher Aufgaben Beliehene und unterliegen als solche staatlicher Aufsicht (Nr. 9 Anlage VIIIb StVZO). Dies hat freilich nicht zur Folge, dass im Verhältnis zur Aufsichtsbehörde keine Datenschutzvorschriften gelten, wie der Technische Leiter des DEKRA e.V. in einer Stellungnahme gegenüber dem Gesamtbetriebsrat meinte.

Nr. 9 Anlage VIIIb StVZO

9.1 Die oberste Landesbehörde oder die von ihr bestimmten oder nach Landesrecht zuständigen Stellen üben die Aufsicht über die Inhaber der Anerkennung aus. Die Aufsichtsbehörde oder die zuständigen Stellen können selbst prüfen oder durch von ihnen bestimmte Sachverständige prüfen lassen, ob insbesondere
9.1.1 die Voraussetzungen für die Anerkennung noch gegeben sind,
9.1.2 die HU, AU und SP sowie die Abnahmen ordnungsgemäß durchgeführt und die sich sonst aus der Anerkennung oder aus Auflagen ergebenden Pflichten erfüllt werden,

Voraussetzung für die Anwendbarkeit der Datenschutzvorschriften ist allerdings, dass die Daten, die der DEKRA e.V. dem Regierungspräsidium mit dem Revisionsbericht übermittelt, personenbezogen oder personenbeziehbar sind. Das Regierungspräsidium erhält für jeden Prüfingenieur eine Auflistung der von ihm im Revisionszeitraum erkannten Mängel. Der Name des Prüfers ist durch ein Kennzeichen ersetzt. Da nur der DEKRA e.V. die Zuordnungsregel kennt, kann das Regierungspräsidium nur mit seiner Hilfe die Daten den Betroffenen zuordnen. Das Regierungspräsidium erhält somit nur pseudonymisierte Daten der Prüfingenieure (vgl. Legaldefinition in § 3 Abs. 6a BDSG). Ob pseudonymisierte Daten für Dritte, welche die Zuordnungsregel nicht kennen, anonym sind und damit ihre Verarbeitung nicht den datenschutzrechtlichen Vorschriften unterliegt, ist umstritten. Da das Regierungspräsidium durch aufsichtsrechtliche Maßnahmen von der Überwachungsorganisation die Aufdeckung der Identität des Betroffenen verlangen kann, z.B. bei Verdacht auf ungenügende Prüftätigkeit, ist im vorliegenden Fall eine Personenbeziehbarkeit der Mängelliste gegeben. Die Datenerhebung und Datenspeicherung des Regierungspräsidiums bedarf deshalb einer Rechtsgrundlage (§ 7 Abs. 1 HDSG).

§ 3 Abs. 6a BDSG

Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

§ 7 Abs. 1 HDSG

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn
1. eine diesem Gesetz vorgehende Rechtsvorschrift sie vorsieht oder zwingend voraussetzt,
2. dieses Gesetz sie zulässt oder
3. der Betroffene ohne jeden Zweifel eingewilligt hat.

4.4.1.2 Kritik des Gesamtbetriebsrats

Nach Ansicht des Gesamtbetriebsrats fehlte eine ausreichende Rechtsgrundlage. Er war der Auffassung, dass die Aufsicht des Regierungspräsidiums sich zunächst auf den Technischen Leiter der amtlich anerkannten Überwachungsorganisation zu richten habe, um zu prüfen, ob dieser seinen gesetzlichen Aufgaben nachkomme. Bevor die Behörde personenbeziehbare Daten erhalte, habe sie zunächst die Aufsicht der beliehenen Organisation zu prüfen. Die Aufsicht habe sich auf die Überwachung zu beschränken und dürfe sich nicht selbst an die Stelle der beliehenen Organisation setzen.

Es sei völlig ausreichend, wenn der Behörde Informationen über die Fahrzeuge, ihre Altersstruktur, Fahrzeugort und Prüfort übermittelt würden, ohne dass gleichzeitig pseudonymisierte Daten der Prüfingenieure zur Verfügung gestellt würden. Das Regierungspräsidium könne seine Aufsichtspflicht erfüllen, ohne dass dem Revisionsbericht eine Auflistung der von jedem Prüfingenieur im Revisionszeitraum erkannten Mängel beigefügt werde. Es genüge, dass die Behörde überprüfe, inwieweit die mitgeteilten Prüfergebnisse signifikant von den bekannten Mängelwerten in Bezug auf Fahrzeugtypen und Altersstruktur abweichen. Bemerke die Überwachungsbehörde beispielsweise, dass an einem Prüfort auffallend viele ältere Fahrzeuge die Prüfung ohne Feststellung erheblicher Mängel überstanden hätten, könne dies ein Anlass sein, bei der Überwachungsorganisation nähere Informationen einzuholen. Die Überwachungsorganisation teile der Behörde z.B. mit, dass es sich um eine bestimmte Werkstatt handelte, und dass in diesem konkreten Fall bezüglich dieses Fahrzeugtyps keine Auffälligkeiten bestünden. Erst wenn die Überwachungsorganisation mit den von ihr zusätzlich übermittelten Angaben den begründeten Verdacht des Regierungspräsidiums auf unzureichende Prüfungen nicht ausräumen könne, dürften in diesem Fall aus konkretem Anlass personenbezogene Daten des Prüfers angefordert werden. Für die ordnungsgemäße Überwachung durch das Regierungspräsidium sei es daher nicht erforderlich, dass vorab bereits personenbeziehbare Daten aller Prüfingenieure mitgeteilt würden. Die Speicherung der Daten verstoße gegen den Grundsatz der Datensparsamkeit und stelle eine unzulässige Vorratsdatenspeicherung dar.

Bei der Durchführung der Überwachungstätigkeit sei die Aufsichtsbehörde verpflichtet, zunächst kritische Bereiche aufgrund der übermittelten Daten zu identifizieren und zu versuchen, diese gemeinsam mit der Überwachungsorganisation zu klären. Erst wenn dies nicht gelinge oder sich der Verdacht auf nicht korrekte Prüfungen bestätige, sei der Zugriff auf personenbezogene Daten im Einzelfall gerechtfertigt. Die Untersuchungs- und Prüfqualität könne in einem ersten Schritt geprüft und nachvollzogen werden, ohne dass dazu eine personenbeziehbare Prüferliste benötigt werde. Die Prüfung richte sich dann auf die jeweilige HU, AU und SP sowie die Abnahmen.

Der Gesamtbetriebsrat machte außerdem geltend, selbst wenn man seine Auffassung nicht teile, müsse die Aufsichtsbehörde zumindest konkrete Kriterien benennen, nach denen sie bei ihrer Prüftätigkeit von einer Auffälligkeit ausgehe. Sei die Aufsichtsbehörde beispielsweise der Meinung, dass beim Überschreiten einer bestimmten Anzahl täglicher Prüfungen der Verdacht auf eine nichtordnungsgemäße Prüfung bestehe, ließe sich der Eingriff auf diejenigen Fälle beschränken, in denen diese Anzahl überschritten werde. Aber auch in diesen Fällen müsse die Überwachungsorganisation zunächst die Möglichkeit haben, die große Anzahl zu erklären und das Ergebnis der eigenen Untersuchung mitzuteilen, ob ordnungsgemäß geprüft wurde oder nicht.

4.4.1.3 Zulässigkeit der Datenerhebung

Die Rechtsgrundlage für die Vorlage des Revisionsberichts findet sich in der aufgrund § 6 Abs. 1 Nr. 2 Buchstabe n StVG erlassenen Anlage VIIIb StVZO. Gemäß Nr. 2.4 Anlage VIIIb StVZO sind die Ergebnisse der Hauptuntersuchungen, Abgasuntersuchungen und Sicherheitsüberprüfungen für die Aufsichtsbehörden so zu sammeln und auszuwerten, dass jederzeit die Untersuchungs- und Prüfqualität für einen beliebigen Zeitraum innerhalb der letzten drei Jahre nachvollzogen werden kann. Die Aufsichtsbehörde kann gem. Nr. 9.1.2 Anlage VIIIb StVZO selbst prüfen, ob die Hauptuntersuchung, Abgasuntersuchung und Sicherheitsprüfung sowie die Abnahmen ordnungsgemäß durchgeführt und die sich sonst aus der Anerkennung oder aus Auflagen ergebenden Pflichten erfüllt werden. Der Gesamtbetriebsrat verkannte die rechtliche Stellung des Beliehenen. Das Demokratieprinzip verlangt, dass bei der Übertragung von Staatsaufgaben auf Private im Wege der Beleihung die Aufgabenverantwortung und die daraus folgende Garantenstellung für die Aufgabenerfüllung beim Staat verbleibt und durch eine effektiv genutzte umfassende Fach- und Rechtsaufsicht ausgeübt wird.

Anlage VIIIb StVZO

2. Voraussetzungen für die Anerkennung
Die Anerkennung kann erteilt werden, wenn

Nr. 2.4
die Organisation durch Einrichtung eines innerbetrieblichen Revisionsdienstes sicherstellt, dass die Ergebnisse für die Innenrevision und die Aufsichtsbehörde so gesammelt und ausgewertet werden, dass jederzeit die Untersuchungs- und Prüfqualität für einen beliebigen Zeitraum innerhalb der letzten drei Jahre nachvollzogen werden kann und dass die Ergebnisse mit denjenigen anderer Überwachungsorganisationen und denen der Technischen Prüfstellen einwandfrei vergleichbar sind.

Das Regierungspräsidium hatte in seiner Stellungnahme überzeugend dargelegt, dass aggregierte Daten über die von den Prüfingenieuren des DEKRA e.V. durchgeführten amtlichen Fahrzeuguntersuchungen für eine effiziente aufsichtsbehördliche Überwachung nicht ausreichen, sondern Angaben darüber benötigt werden, welche Fahrzeuge (Altersstruktur der geprüften Fahrzeuge und Fahrzeugart) von welchem Prüfingenieur an welchen Prüforten (Werkstätten oder Prüfstellen) mit welchen Ergebnissen geprüft wurden (wie viele und wie schwere Mängel wurden erkannt). Aufgrund ihrer Erfahrung könne die Behörde aus diesen Daten kritische Bereiche erkennen und genauer überprüfen. Falls diese Informationen nicht zur Verfügung stünden, könnten die Verursacher von Qualitätsproblemen nicht gezielt aufsichtsrechtlich behandelt werden, sondern es müsse gleich die amtliche Anerkennung des DEKRA e.V. in Frage gestellt werden, wenn die Ergebnisse befürchten ließen, dass die Aufgaben nicht ordnungsgemäß wahrgenommen würden.

Die unmittelbare Kontrolle der Arbeit der Prüfingenieure vor Ort durch die Aufsichtsbehörde mittels Auswertung der pseudonymisierten Daten geschehe aus zwei Gründen: Zum einen sei es zur Gewährleistung der Sicherheit des Straßenverkehrs notwendig, dass Mängel bei der der amtlichen Prüfung von Fahrzeugen sofort abgestellt würden, dass z.B. fehlerhafte oder unvollständige Prüfberichte gleich korrigiert oder zurückgezogen würden. Zum anderen ließen sich aus der Beobachtung der Arbeitsweise von Prüfingenieuren und der anschließenden Auswertung der statistischen Daten des jeweiligen Prüfingenieurs Rückschlüsse auf die Qualität der Arbeit der technischen Leitung gewinnen, die anders nicht zu erlangen seien. Wenn beispielsweise im Zuge einer Aufsichtsmaßnahme vor Ort ein Prüfingenieur durch sehr schnelle oder oberflächliche Arbeitsweise auffalle und die Auswertung seiner Prüftätigkeit über die letzten Monate erkennen lasse, dass dies auch schon seit längerem aus den statistischen Daten erkennbar gewesen wäre, ergäben sich daraus Zweifel an der Qualität der Arbeit der technischen Leitung, die das hätte erkennen und gegensteuern müssen. Eine Aufsicht über die Arbeit der technischen Leitung ohne eigene Qualitätskontrollen, die sich nur auf die von der technischen Leitung gelieferten Berichte stütze, wäre weitgehend wirkungslos.

Plausibel begründete das Regierungspräsidium außerdem, weshalb es nicht ausreicht, lediglich die Daten der Prüfstützpunkte zu betrachten. Qualitätsprobleme würden durch das Handeln der Prüfingenieure und nicht durch bestimmte Prüfstützpunkte verursacht. Es habe sich gezeigt, dass die absolute Zahl der von einem Prüfingenieur durchgeführten Prüfungen ein wichtiges Indiz für mögliche Qualitätsprobleme sei, insbesondere wenn diese Prüfungen an relativ alten Fahrzeugen vorgenommen wurden. Diese Information ließe sich aus den Prüfstützpunktdaten nicht ableiten. Wenn nur die Prüfergebnisse der Stützpunkte vorlägen, würde dies die Identifizierung kritischer Bereiche erschweren und dazu führen, dass Mitarbeiter in den Fokus von Aufsichtsmaßnahmen gerieten, die aufgrund der pseudonymisierten Prüfergebnisse nicht auffällig wären. Läge z.B. ein Prüfstützpunkt hinsichtlich des Durchschnittsalters der geprüften Fahrzeuge kritisch hoch und wäre die Mängelquote ebenfalls relativ hoch wäre der Stützpunkt unauffällig. Dies wäre unproblematisch, solange der Prüfstützpunkt nur von einem Mitarbeiter betreut würde. Bei mehreren Prüfingenieuren könne es allerdings durchaus sein, dass von diesen einer seine Arbeit mangelhaft erledige, was aber durch die anderen statistisch ausgeglichen werde. Das Qualitätsproblem bliebe somit unbemerkt. Wenn umgekehrt ein Prüfstützpunkt statistisch auffällig wäre, der von mehreren Mitarbeitern betreut wird, und dies nicht durch besondere Merkmale des Prüfstützpunktes erklärbar wäre, müssten von allen Mitarbeitern die kompletten Daten personenbezogen geprüft werden, obwohl vielleicht nur einer die Qualitätsprobleme verursacht hat.

Das Regierungspräsidium beachtete somit auch den Grundsatz der Datensparsamkeit, in dem es zunächst nur pseudonymisierte Daten der Prüfingenieure verlangte, die lediglich bei Bedarf einer konkreten Person zugeordnet werden sollten.

4.4.1.4 Verfahrensregelung

Unter dem Vorsitz eines Vertreters meines Hauses haben sich das Regierungspräsidium Darmstadt und der DEKRA-Gesamtbetriebsrat u.a. auf folgendes Verfahren verständigt:

- "Der DEKRA e.V. stellt der Aufsichtsbehörde den jährlichen Revisionsbericht mit pseudonomymisierten Daten (§ 3 Abs. 6a BDSG) in elektronischer Form zur Verfügung. Im Revisionsbericht des DEKRA e.V. enthaltene Daten für Prüfingenieure mit weniger als 100 Hauptuntersuchungen im Jahr werden der Aufsichtsbehörde nicht übermittelt.

- Stellt die Aufsichtsbehörde im Rahmen der Auswertung des Revisionsberichts bei einzelnen Prüfingenieuren Auffälligkeiten fest, fordert sie zunächst den Technischen Leiter des DEKRA e.V. unter Nennung der Kennung des Prüfingenieurs zur Stellungnahme auf. Der Technische Leiter kann vor Abgabe seiner Stellungnahme den betroffenen Prüfingenieur zur Anfrage der Aufsichtsbehörde hören. Ergibt sich aus der Stellungnahme des Technischen Leiters für die Aufsichtsbehörde ein Anlass für aufsichtsbehördliche Maßnahmen gegen den Prüfingenieur, deckt der DEKRA e.V. auf Verlangen der Aufsichtsbehörde das Pseudonym auf und teilt ihr den Klarnamen des Prüfingenieurs mit. Über diesen Vorgang wird der betroffene Prüfingenieur informiert, es sei denn, die Aussichtsbehörde erklärt die Information im Ausnahmefall für unzweckmäßig und vertraulich. In diesem Fall erfolgt die Information des Prüfingenieurs im Nachgang."

4.5 Schulen und Schulverwaltung

4.5.1 Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen

Das Hessische Kultusministerium hat eine neue Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen in Kraft gesetzt. Bei der Erarbeitung der Verordnung war ich beteiligt. Den Belangen des Datenschutzes ist hinreichend Rechnung getragen.

Unter dem Titel "Datenschutz" enthält § 83 des HSchulG bereichsspezifische Regelungen zum Datenschutz für den Schulbereich. Absatz 9 der Vorschrift enthält die Ermächtigung Umfang und Einzelheiten der personenbezogenen Datenverarbeitung in der Schule näher zu regeln.

§ 83 Abs. 9 HSchulG

Umfang und Einzelheiten der personenbezogenen Datenverarbeitung in der Schule werden durch Rechtsverordnung näher geregelt; dabei ist zu bestimmen, welche Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten außerhalb der Schule zu berücksichtigen sind.

Eine weitere Ermächtigung enthält § 85 HSchulG. Danach können durch Rechtsverordnung u.a. die öffentlichen Schulen verpflichtet werden, für statistische Zwecke Daten über schul- und ausbildungsbezogene Tatbestände zur Evaluierung, Bildungsberichterstattung und Bildungsplanung an das Kultusministerium und an das Statistische Landesamt zu übermitteln.

Auf der Grundlage dieser beiden Ermächtigungen erging durch das Hessische Kultusministerium am 4. Februar 2009 die "Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen" (ABl. 2009 S. 131). Sie löst eine frühere Verordnung aus dem Jahre 1993 ab.

Die neue Verordnung konkretisiert zahlreiche datenschutzrelevante Sachverhalte. Dabei wird dem verfassungsrechtlichen Gebot der Transparenz und Normenklarheit datenschutzrechtlicher Bestimmungen entsprochen. Nur beispielhaft sind hier einige Einzelregelungen aufgezählt:

- Es wird vorgegeben, dass medizinische und psychologische Gutachten nur in verschlossenen Umschlägen in die Schülerakte einzuheften und Einsichtnahmen zu protokollieren sind (§ 1 Abs. 6).

- Eine automatisierte Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungseinrichtungen außerhalb der Schule darf nur nach schriftlicher Anzeige der Lehrkraft erfolgen (§ 3).

- Bereits das HDSG (§ 5 Abs. 1) enthält die Verpflichtung jeder Daten verarbeitenden Stelle einen behördlichen Datenschutzbeauftragten zu bestellen. Die Verordnung weist dem schulischen Datenschutzbeauftragten neben den Aufgaben nach dem Datenschutzgesetz bestimmte weitere Aufgaben zu (§ 11).

- Drei Anlagen der Verordnung zählen detailliert die Daten auf, die über Schüler und Lehrer zum Zwecke der Erfüllung des Bildungs- und Erziehungsauftrages der Schule oder zum Zwecke von statistischen Erhebungen verarbeitet und wie lange sie aufbewahrt werden dürfen.

4.5.2 Digitale Schwarze Bretter in Schulen und Veröffentlichungen auf der Schul-Homepage

Schulen können gedruckte Aushänge auch in Form eines elektronischen Aushangs auf Digitalen Schwarzen Brettern anzeigen. Die weitergehenden Möglichkeiten der elektronischen Verarbeitung werfen neue Fragestellungen auf.

Im Berichtszeitraum wurden erstmals Fragen zur datenschutzrechtlich korrekten Nutzung von sog. "Digitalen Schwarzen Brettern" in Schulen an mich herangetragen.

Solange der elektronische "Aushang" nicht für zusätzliche Aufgaben verwendet werden soll, lassen sich die Systeme unter Beachtung einiger technischer und organisatorischer Rahmenbedingungen, wie der herkömmliche Aushang, datenschutzgerecht betreiben. Da aber die moderne Plattform zu einer weitergehenden Nutzung einlädt und sich die einmal aufbereiteten Daten leicht auf das Internetangebot der Schul-Homepage übertragen lassen, ergeben sich doch einige neue Probleme.

Obwohl bis zur Mitte des Jahres 2009 keine nennenswerten Erfahrungen mit dem Betrieb der Systeme vorlagen, habe ich auch in Abstimmung mit dem Hessischen Kultusministerium einen Beitrag in meinem Internetangebot veröffentlicht, der die grundlegenden Fragen von Betroffenen wie Verantwortlichen zu beantworten sucht.

Den Schulen wird derzeit von verschiedenen Herstellern ein System zur Ablösung bzw. multimedialen Ergänzung des althergebrachten Aushangs angeboten. Unter Beachtung der datenschutzrechtlichen und technisch-organisatorischen Rahmenbedingungen können Digitale Schwarze Bretter in den Schulen eingesetzt werden.

Der Artikel soll betroffenen Schülern, Eltern und Lehrkräften als auch den Verantwortlichen der Schulen und Schulträger als erste Orientierung dienen.

Systembeschreibung
Die Mehrzahl der Anbieter Digitaler Schwarzer Bretter offerieren mit ihren Systemen den Schulen eine Plattform, die von einem beliebigen Arbeitsplatz über einen sicheren Internetzugang mit verschiedenen Informationen durch ein standardisiertes Verfahren gespeist werden kann. Die hinterlegten Informationsangebote werden dann von den Digitalen Schwarzen Brettern automatisch von dieser Plattform übernommen, in einem Intervall aktualisiert und in der Schule auf einem entsprechend großen Monitor zur Anzeige gebracht. Insofern entsprechen Digitale Schwarze Bretter vom Prinzip dem bekannten Aushang bzw. Schwarzen Brett, und die hier veröffentlichten Informationen sind wie bisher dem gleichen Personenkreis zugänglich.

Das auf den Digitalen Schwarzen Brettern zur Verfügung gestellte Informationsangebot gliedert sich nach den derzeit vorliegenden Systembeschreibungen zumeist in drei verschiedene Informationsbereiche, die in den Beschreibungen der Hersteller z.T. als Module bezeichnet werden:

Vertretungsplan
Mit dem Vertretungsplan am Digitalen Schwarzen Brett soll eine schnellere und flexiblere Verteilung der Information innerhalb der Schule gerade bei verteilten Standorten gewährleistet werden. Der Vertretungsplan kann in der Regel aus einer bereits an der Schule vorhandenen Spezial-Software übernommen werden.

Multimediales Informationsangebot
Hier können Grafiken, Bilder, Videos aber auch ganze Berichte über Veranstaltungen der Schule stehen.

Einfache Textnachrichten ("Newsticker").

Rechtlicher Rahmen/Abgrenzung zum Internet-Angebot der Schule
Der datenschutzrechtliche Ausgangspunkt ist § 83 Abs. 1 HSchG.
Danach dürfen Schulen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern sowie von Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrages der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist.

Die Beurteilung, welche personenbezogenen Daten im Rahmen des Schulbetriebs notwendigerweise verarbeitet werden müssen, obliegt in erster Linie der Schule vor Ort.

Ist die Notwendigkeit der Datenverarbeitung zu bejahen, bedarf es insoweit auch keiner Einwilligung der Betroffenen.

Das bedeutet bspw., dass durch das "Digitale Schwarze Brett" auf dem Vertretungsplan bekannt gegeben werden darf, durch welche Lehrkraft eine Unterrichtsstunde (Angaben zu Tag, Uhrzeit, Klasse/Kurs) vertreten wird. Nicht erforderlich erscheint hingegen, in diesem Fall zusätzlich darauf hinzuweisen, welche Lehrkraft gerade nicht zur Verfügung steht und den Vertretungsfall ausgelöst hat. Deshalb ist auch nur die Bekanntgabe der vertretenden Lehrkräfte vorzusehen.

Der Vertretungsplan kann ggf. zusätzlich auf einer Plattform einer geschlossenen Benutzergruppe (Schüler, Eltern und Lehrer) aber keinesfalls öffentlich im Internet zur Verfügung gestellt werden.

Grundsätzlich nicht erforderlich und damit von einer Einwilligung abhängig sind bspw. Präsentationen am Digitalen Schwarzen Brett, die Abbildungen oder Videos mit Lehrkräften oder Schülern enthalten.

Einer gesonderten Einwilligung bedarf es darüber hinaus, wenn solche Präsentationen nicht nur in der Schule veröffentlicht, sondern auch über das Internet der Allgemeinheit zugänglich gemacht werden sollen.

Technisch-organisatorische Maßnahmen

Bei der Systemauswahl haben Schulen und Schulträger folgende Punkte besonders zu beachten:

Da es sich bei den Plattformangeboten um eine Datenverarbeitung im Auftrag handelt, müssen die Verträge mit den Systemanbietern den Erfordernissen des § 4 HDSG entsprechen. Dies schließt gemäß § 4 Abs. 3 HDSG unter anderem ein, dass der Auftraggeber vertraglich sicherzustellen hat, dass der Auftragnehmer die Bestimmungen des Hessischen Datenschutzgesetzes befolgt. Das bedeutet insbesondere auch, dass dem Auftragnehmer eine Verarbeitung der Daten zu einem anderen als dem zur rechtmäßigen Aufgabenerfüllung gehörenden Zweck untersagt ist (§ 9 HDSG). Außerdem muss sich der Auftragnehmer gemäß § 4 Abs. 3 HDSG der Kontrolle des Hessischen Datenschutzbeauftragten unterwerfen.

Die Zugänge zur angebotenen Plattform müssen über eine verschlüsselte Verbindung erfolgen. Bei einer Produktauswahl ist daher darauf zu achten, dass bei den ggf. zum Einsatz kommenden SSL-Zertifikaten eine sichere Erstellung gegeben und für den angegebenen Gültigkeitszeitraum eine Sperrlistenprüfung möglich ist.

Die schulspezifische Anmeldung an der zentralen Plattform, die auch von verschiedenen berechtigten Personen mit persönlichen Kennungen und Passwörtern erfolgen kann, muss den allgemeinen Ansprüchen an Authentisierungssysteme genügen. D.h. die Passwörter müssen mindestens 8 Zeichen lang sein und sich komplex aus Buchstaben, Ziffern und Sonderzeichen zusammensetzen.

Soweit die eingesetzte Digitale Schwarze Brett-Software nicht über automatisierte Löschfunktionen verfügt, muss die Schule die notwendigen organisatorischen Maßnahmen zur Löschung nicht länger benötigter Daten treffen.

Darüber hinaus sind beim Anschluss der Digitalen Schwarzen Bretter je nach Anbindung auch noch Aspekte der Netzwerksicherheit zu berücksichtigen:

Separate Internetanbindung

Werden Einzelgeräte bzw. die Digitalen Schwarzen Bretter einer Schule zusammengefasst über einen eigenen Internet-Zugang mit der Plattform verbunden, sind die Geräte mit allen Schnittstellen gegen unbefugte Zugriffe zu sichern.

Geräte im pädagogischen Netz

Da auch in den Unterrichtsnetzen personenbezogene Daten verarbeitet werden, sollte zusätzlich zum Gerät der unbefugte Zugang zu den Netzwerkanschlüssen verhindert werden. In Fällen, in denen dies nicht gewährleistet werden kann, ist der Schutz des Netzwerks auch durch eine entsprechende Konfiguration des Ports am Netzwerk-Switch möglich, der dann nur mit Geräten mit zugelassenen IP- und Mac-Adressen kommuniziert.

Geräte im Verwaltungsnetz

Hier sollten wenn möglich beide Maßnahmen umgesetzt werden. Dem Schutz der Netzwerkverbindungen des Digitalen Schwarzen Bretts kommt dabei vorrangige Bedeutung zu, da es sonst durchaus möglich ist, die am Switch zugelassenen IP- und Mac-Adressen auszuforschen, mit einem anderen Gerät zu simulieren und über diesen Anschluss das Verwaltungsnetz anzugreifen.

Insbesondere die Einschränkungen, die für eine Veröffentlichung in einem allgemein zugänglichen Internet-Angebot von Schulen gelten, haben bei den Verantwortlichen verschiedener Schulen für Diskussionsstoff gesorgt. Zum Teil war man der Auffassung, dass der Vertretungsplan allein schon deswegen im Internet verfügbar sein müsse, damit Eltern die notwendige Betreuung ihrer Sprösslinge außerhalb der Unterrichtszeiten sicherstellen können und Berufsschüler, die nach dem Blockmodell unterrichtet werden, wissen, ob sie zum vermeintlichen Beginn des Unterrichtsblocks die Schule oder doch ihren Ausbildungsbetrieb anfahren müssen. Um diese organisatorischen Fragen zu regeln, reicht es aber vollkommen aus, Unterrichtsbeginn und -ende bzw. im Falle der Berufsschüler den ersten Unterrichtstag für die jeweiligen Klassen auf der Homepage der Schule zu hinterlegen. Der Vertretungsplan der detailliert ausweist, welche Unterrichtsstunde durch welche Lehrkraft übernommen wird, ist dafür jedenfalls nicht erforderlich. Die Beispiele zeigen, dass es durchaus möglich ist, entsprechend aufbereitete, d.h. von Personenbezügen befreite Daten für die Veröffentlichung auf der Internet-Präsenz der Schule zu übernehmen.

Weitaus schwieriger wird es, wenn die Schule am Digitalen Schwarzen Brett und darüber hinaus auf der "Homepage" personenbezogene Daten, Bilder oder Videos im Zusammenhang mit Schulveranstaltungen veröffentlichen will. Hier benötigen die Schulen zwingend die Einwilligungen der betroffenen Schüler bzw. Eltern und Lehrer, die sich auch deutlich auf den Verbreitungsweg - Digitales Schwarzes Brett, Internet-Angebot, Schülerzeitung - beziehen muss. Dieses Vorgehen ist den Schulen nicht allein wegen der datenschutzrechtlichen Erfordernisse zwingend zu empfehlen, sondern auch weil die Rechtsprechung Klägern, die sich gegen eine ungenehmigte Veröffentlichung wenden, regelmäßig einen Schadenersatzanspruch zubilligt.

4.5.3 Neue Schulbroschüre

Gegen Ende des Berichtszeitraumes habe ich eine aktualisierte Auflage meiner erstmals im Jahre 1995 vorgestellten Broschüre "Datenschutz in Schulen" herausgegeben. Die Broschüre kann bei meiner Behörde angefordert werden.

Im Jahre 1992 hatte der Gesetzgeber das Schulrecht neu geordnet und die Verarbeitung personenbezogener Daten in Schulen an eine Reihe von Bedingungen geknüpft. Danach erschien erstmals eine von meiner Behörde aufgelegte Schulbroschüre mit allen schulrechtlich relevanten Datenschutzbestimmungen.

Inzwischen ist das Schulgesetz mehrfach geändert worden. Die Änderung vom 29. November 2004 (GVBl. I S. 330) betraf auch datenschutzrechtliche Bestimmungen. Die Fassung vom 14. Juni 2005 (GVBl. I S. 442) wurde zuletzt geändert durch Gesetz vom 14. Juli 2009 (GVBl. I S. 265). Ergänzt werden die Vorschriften durch die vom Hessischen Kultusminister erlassene Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 (ABl. 3/2009 S. 131). Mit Erlassen vom 21. August 2009 (ABl. 9/2009 S. 726 ff.) und 27. November 2009 (ABl. 1/2010 S. 11) hat das Hessische Kultusministerium Details für die IT-Sicherheit und für den heimischen Arbeitsplatz der Lehrkräfte festgelegt.

Wegen der umfangreichen Änderungen war eine Überarbeitung der Schulbroschüre dringend notwendig. Die aktualisierte Auflage enthält die schulspezifischen Vorschriften ergänzt um die verfassungsrechtlichen Grundlagen zum Datenschutzrecht, das Hessische Datenschutzgesetz und das Bundesdatenschutzgesetz. Die Broschüre enthält aber nicht nur die für den Schulbereich wichtigsten Vorschriften. Sie legt auch die Regelungssystematik von allgemeinem und bereichsspezifischem Datenschutzrecht dar, erläutert und kommentiert datenschutzrechtliche Einzelregelungen.

Die neue Broschüre soll Schülerinnen und Schülern, Erziehungsberechtigten, Lehrerinnen, Lehrern und Schulleitungen einen Überblick über das aktuelle Datenschutzrecht geben. Sie wurde über die Staatlichen Schulämter allen hessischen Schulen zur Verfügung gestellt. Weitere Einzelexemplare können bei meiner Behörde angefordert werden.

4.6 Gesundheitswesen

4.6.1 Probleme bei der Umsetzung des Kindergesundheitsschutzgesetzes

Infolge des 2007 vom Landtag beschlossenen Kindergesundheitsschutzgesetzes konnte die Zahl der an den sog. U-Untersuchungen teilnehmenden Kinder deutlich erhöht werden. Allerdings sind bei der Umsetzung des Gesetzes auch Probleme aufgetreten. Eine erhebliche Anzahl von Eltern hat Erinnerungsschreiben vom Kindervorsorgezentrum bzw. Anfragen eines Jugendamtes erhalten, obwohl ihr Kind zur Vorsorgeuntersuchung gebracht wurde bzw. obwohl ihr Kind bereits vorher verstorben war. Ich habe mich dafür eingesetzt, dass die Probleme genau analysiert und notwendige Maßnahmen zur Beseitigung der Probleme getroffen werden. Einige Fragen sind noch offen.

4.6.1.1 Einleitung

Mit dem Kindergesundheitsschutzgesetz wird eine Verbesserung des Gesundheitsschutzes von Kindern und ihres Schutzes vor Vernachlässigung, Misshandlung und Missbrauch angestrebt. Seit 1. Januar 2008 sind in Hessen die Vorsorgeuntersuchungen für Kinder verbindlich vorgeschrieben (Hessisches Gesetz zur Verbesserung des Gesundheitsschutzes für Kinder vom 14. Dezember 2007, GVBl. I S. 856). Zum einen ist 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. Kinderrichtlinien) verbindlich. Zum anderen ist auch die Teilnahme an den Früherkennungsuntersuchungen auf behandelbare Stoffwechsel- und Hormonerkrankungen, das sog. Neugeborenen-Screening (s. Anlage 2 der o.a. Kinder-Richtlinien) verbindlich.

Durch Verordnung vom 21. Dezember 2007 (GVBl. I S. 962) wurde als Hessisches Kindervorsorgezentrum (HKVZ) das Universitätsklinikum Frankfurt bestimmt. Die gesetzlichen Regelungen sehen vor, dass die Kinder, die nicht innerhalb einer Frist an den jeweiligen Früherkennungsuntersuchungen teilgenommen haben, im HKVZ durch Abgleich mit den Meldedaten herausgefunden werden, die Eltern (bzw. Personensorgeberechtigten) dieser Kinder über die erforderlichen Früherkennungsuntersuchungen informiert und an die Teilnahme erinnert werden und - sofern weiterhin keine Teilnahme der die Früherkennungsuntersuchungen durchführenden Personen an das HKVZ gemeldet wird - das zuständige Jugendamt informiert wird (zu den Details der datenschutzrechtlichen Aspekte des Gesetzes s. 36. Tätigkeitsbericht, Ziff. 5.8.2). Nach dem Konzept der Landesregierung soll das HKVZ über die im Kindergesundheitsschutzgesetz geregelten Aufgaben auf der Basis einer Einwilligung der Eltern auch weitere Aufgaben im Hinblick auf weitere Früherkennungsuntersuchungen haben, z.B. hinsichtlich eines Hör-Screenings.

4.6.1.2 Probleme mit fehlerhaften Erinnerungs- und Mahnschreiben an die Eltern

Dem HKVZ zufolge konnte die Quote derjenigen Kinder, bei denen die U-Untersuchungen durchgeführt wurden, deutlich erhöht werden. Bei der Umsetzung des Gesetzes sind allerdings auch erhebliche Probleme aufgetreten. Nach dem Kindergesundheitsschutzgesetz sollen die Kinder, die nicht innerhalb einer Frist an den jeweiligen Früherkennungsuntersuchungen teilgenommen haben, im HKVZ durch einen Abgleich mit den Meldedaten herausgefunden werden. Eine zentrale Voraussetzung für die korrekte Durchführung des gesetzlich vorgesehen Abgleichsverfahrens ist die Aktualität der betroffenen Meldedaten im Melderegister. Bei den Diskussionen vor der Verabschiedung des Gesetzes gingen alle Beteiligten stillschweigend davon aus, dass die Aktualität der Meldedaten gewährleistet ist. Es sind jedoch in Hessen 2008 und 2009 Fälle bekannt geworden, in denen das HKVZ sowohl Erinnerungs- als auch Mahnschreiben wegen nicht durchgeführter Untersuchungen an Eltern verstorbener Kinder versandte. In einigen Fällen wurde sogar das Jugendamt benachrichtigt, welches dann Kontakt zu den Eltern der verstorbenen Kinder aufnahm. In diesen Fällen lag im Kindervorsorgezentrum offenbar keine Information über den Tod des betreffenden Kindes vor.

Nachdem ich im Herbst 2008 durch Beschwerden von Eltern verstorbener Kinder und auch durch Informationen des HMDIS und des HKVZ von dem Problem Kenntnis erhalten hatte, habe ich mehrere Gespräche mit dem HMDIS, dem HKVZ sowie weiteren Stellen initiiert, damit die Ursachen für die mangelnde Aktualität des Meldedatenbestandes schnell analysiert werden und anschließend geeignete Maßnahmen zur möglichst weitgehenden Beseitigung des Problems vereinbart werden können. Die Probleme konnten nicht im HKVZ gelöst werden. Es musste daher der gesamte Prozess der Datenverarbeitung vom Tod des Kindes bis zur Datenübermittlung an das HKVZ analysiert werden. Konkret heißt dies, dass die einzelnen Verfahrensschritte vom Tod eines Kindes, der Meldung des Todes an das zuständige Standesamt, der Beurkundung des Todes durch das Standesamt, der Datenübermittlung vom Standesamt an das zuständige Meldeamt und der Datenübermittlung vom Meldeamt an das HKVZ, die jeweils mindestens benötigte Zeit, möglicherweise auftretende Verzögerungen und deren Vermeidbarkeit im Detail untersucht werden mussten, um die Fehlerquellen zu finden und den Prozess zu optimieren.

Soweit die Ursachen geklärt werden konnten, lagen sie insbesondere in

- Fehlern bei der Software der Meldeämter,
- Fehlern bei der Kommunikation zwischen Standes- und Meldeamt,
- Fehlern bei der ekom21,
- verspäteten Meldungen des Todes im Meldeamt,
- verspäteten Meldungen des Todes beim Standesamt.

In der Folgezeit wurde dann eine Reihe von Maßnahmen zur möglichst weitgehenden Vermeidung der Probleme getroffen. Es wurden Maßnahmen zur Vermeidung von technischen Problemen bei der Datenübertragung festgelegt. Ein wesentlicher Schritt zur Verbesserung der Situation war dann der Erlass des Hessischen Ministeriums des Innern und für Sport vom 2. März 2009 betr. die Verbesserung der Datenübermittlung zwischen Standesämtern, Meldebehörden und dem HKVZ. In dem Erlass wurde im Einvernehmen mit dem HMDIS und in Absprache mit mir eine Reihe von Maßnahmen zur Vermeidung von Problemen vorgesehen.

Erlass vom 2. Januar 2010 - Az. LPP 22 - B - 023 - a - 02

Aufgaben der Standesämter und Meldebehörden:

Für die Wahrnehmung der Aufgaben ist das HKVZ auf die Daten der Standesämter und Meldebehörden angewiesen. Sicherzustellen ist eine regelmäßige und zeitnahe Datenübermittlung aller in Hessen wohnhafter Kinder im Alter bis zu fünfeinhalb Jahren an das HKVZ.

Durch eine Änderung der Meldedatenübermittlungsverordnung (MeldDÜVO) wurde die erforderliche Datenübermittlung an das HKVZ geregelt (vgl. § 18a MeldDÜVO). Danach sind die Meldebehörden verpflichtet, automatisiert die notwendigen Daten von Kindern bis zu einem Alter von fünfeinhalb Jahren dem HKVZ zu übermitteln.

Im Falle der Speicherung einer Geburt im Melderegister, des Zuzugs eines Kindes unter fünfeinhalb Jahren oder der Fortschreibung der zu übermittelnden Daten (z.B. ein Sterbefall) übermitteln die Meldebehörden wöchentlich die Änderungen an das HKVZ.

Sterbefälle sind nach § 28 PStG durch Personen mündlich (§ 29 Abs. 1 PStG) und von Einrichtungen sowie von registrierten Bestattungsunternehmen schriftlich (§§ 30, 29 Abs. 2 PStG) spätestens am dritten auf den Tod folgenden Werktag dem zuständigen Standesamt anzuzeigen. Nach § 38 PStV soll mit der Sterbefallanzeige eine Geburtsurkunde, ein Nachweis über den letzten Wohnsitz und eine ärztliche Bescheinigung über den Tod (Leichenschauschein oder vorläufige Todesbescheinigung) vorgelegt werden. Nach der Beurkundung des Sterbefalls hat das Standesamt u.a. eine Mitteilung an die Meldebehörde zu richten (§ 60 Abs. 1 Nr. 6 PStV), die wiederum die Information an das HKVZ übermittelt.

Bedauerlicherweise ist es in der Vergangenheit zu verzögerten sowie fehlerhaften bzw. unvollständigen Veränderungsmeldungen an das HKVZ gekommen. Dies betraf etwa die Übermittlung von Sterbedaten von Kindern mit der Folge, dass von Seiten des HKVZ Aufforderungen zur Durchführung der Untersuchungen an die Personensorgeberechtigten versandt wurden, obwohl das Kind bereits verstorben war.

Um derartige Fehler in Zukunft zu vermeiden und eine möglichst schnelle und korrekte Übermittlung der Daten an das HKVZ sicherzustellen, bitte ich im Einvernehmen mit dem hessischen Sozialministerium sowie in Absprache mit dem Hessischen Datenschutzbeauftragten Folgendes zu beachten:

1) Für den Bereich der Standesämter:

Die Mitteilung von Sterbefällen von Kindern bis zu einem Alter von fünfeinhalb Jahren an die Meldebehörden nach § 60 Abs. 1 Nr. 6 PStV hat so schnell wie möglich, in der Regel noch am Tage der Beurkundung, spätestens jedoch innerhalb von drei Werktagen zu erfolgen. Erfolgt die Übermittlung an die zuständige Meldebehörde postalisch, bitte ich um Versendung per Einzelpost.

Rückfragen von Seiten der Meldebehörde bzw. des HKVZ sind von den Standesämtern unverzüglich zu bearbeiten.

2) Für den Bereich der Meldebehörden:

Die Bearbeitung von Sterbefällen und sonstigen Veränderungen im Datenbestand von Kindern bis zu einem Alter von fünfeinhalb Jahren hat vorrangig und mit besonderer Sorgfalt zu erfolgen. Sämtliche Änderungen von Daten, insbesondere aber Sterbefälle, werden täglich - und nicht erst wie bisher wöchentlich - dem HKVZ übermittelt.

Rückfragen von Seiten des Standesamtes bzw. des HKVZ sind von den Meldebehörden unverzüglich zu bearbeiten.

Das HKVZ wird sich im Falle von Zweifeln an der Plausibilität bei der Datenübermittlung und Datenzuordnung unverzüglich an die zuständige Meldebehörde bzw. das zuständige Standesamt wenden, um eine rasche Klärung zu erreichen.

Entsprechend wurde auch § 18a der MeldDÜVO hinsichtlich der Datenübermittlungen von den Meldebehörden an das HKVZ geändert.

Aufgrund der Analyse des gesamten Datenverarbeitungsprozesses wurde aber auch klar, dass infolge der Komplexität der Verwaltungsabläufe das Problem nicht vollständig gelöst werden kann, vielmehr damit gerechnet werden muss, dass in Einzelfällen das HKVZ immer wieder Kontakt mit Eltern verstorbener Kinder aufnimmt, weil es vom Tod des Kindes noch nichts weiß. Für diese auch künftig voraussichtlich auftretenden Restfälle wurde in den gemeinsamen Besprechungen Folgendes vorgesehen:

- Jedenfalls für 2009 wird jeder neue Einzelfall analysiert, um festzustellen, ob alle Möglichkeiten zur Optimierung des Prozesses ausgeschöpft wurden.

- Der Text des Erinnerungs- bzw. Mahnschreibens des HKVZ an die Eltern wird um einen Zusatz ergänzt, aus dem für die Eltern ersichtlich ist, dass das Schreiben auf den dem HKVZ zur Verfügung gestellten Meldedaten basiert und evtl. fehlerhafte bzw. nicht aktuelle Meldedaten zu fehlerhaften Schreiben führen können.

Auf meine Nachfrage nach dem aktuellen Sachstand hat mir das HKVZ Ende Oktober 2009 mitgeteilt, dass teilweise nach wie vor die Gründe für Erinnerungs- und Mahnschreiben an Eltern verstorbener Kinder nicht klar sind und das HKVZ diese Gründe auch nicht selbst klären kann, da sie nicht im Bereich des HKVZ liegen.

Darüber hinaus gibt es immer wieder Fälle, in denen Eltern Erinnerungs- oder Mahnschreiben oder auch einen Anruf des Jugendamts erhalten, obwohl ihr Kind rechtzeitig zur Untersuchung gebracht wurde. Auch in meiner Dienststelle sind Beschwerden mit diesem Inhalt eingegangen. Als mögliche Ursachen werden insbesondere eine Nichtbeachtung der Berichtspflicht durch einzelne Ärzte (von einzelnen Ärzte wird der Ablauf des Verfahrens, insbesondere die Unentgeltlichkeit der Berichte, kritisiert) und/oder Fehler von Praxismitarbeitern bei der Erstellung/Versendung der Bescheinigung sowie Verluste beim Postversand angesehen.

Ich sehe es als notwendig an, dass das HMAFG und das HMDIS die Gründe für fehlerhafte Anschreiben an Eltern und evtl. mögliche Maßnahmen zur Problembehebung noch weiter aufklären und werde die Entwicklung weiter verfolgen.

4.6.1.3 Weiterverarbeitung der Daten im Jugendamt

Aufgrund von Anfragen betroffener Eltern, ob ihre Akte im Jugendamt vernichtet wird, wenn sich herausstellt, dass die Untersuchung rechtzeitig durchgeführt wurde, haben meine Mitarbeiterinnen und Mitarbeiter stichprobenhaft in verschiedenen Jugendämtern Gespräche darüber geführt, auf welche Weise die beim Jugendamt eingegangenen Meldungen des HKVZ dort weiterverarbeitet werden. Insbesondere ging es auch um die weitere Verfahrensweise, wenn das Jugendamt feststellt, dass das betroffene Kind rechtzeitig zur U-Untersuchung gebracht wurde.

Nach Eingang einer Meldung wird in der Regel vom Jugendamt ein standardisierter Brief an die Eltern versendet mit dem Inhalt, dass das Jugendamt das Kind sehen möchte bzw. - wenn die Untersuchung entgegen der Meldung des HKVZ bereits durchgeführt wurde - das Jugendamt um Vorlage des U-Heftes oder einer Kopie der Bescheinigung des Arztes bittet. In der weit überwiegenden Anzahl der Fälle von Mitte 2008 bis Mitte 2009 hat sich nach Darstellung der Jugendämter herausgestellt, dass die Untersuchung des betroffenen Kindes bereits rechtzeitig durchgeführt wurde. Hintergrund der Meldungen waren neben nicht korrekt erfolgtem Bericht durch den Arzt an das HKVZ insbesondere nicht (mehr) zutreffende Meldedaten (z.B. Umzug, Auslandsaufenthalt von Eltern und Kind, uneinheitliche Schreibweise des Namens bei der Meldebehörde einerseits und dem Arzt andererseits, Tod des Kindes). In den Fällen, in denen eine Untersuchung nicht rechtzeitig durchgeführt wurde, treffen die Jugendämter die jeweils im Einzelfall als erforderlich angesehenen Maßnahmen.

Da die Jugendämter nach Eingang einer Meldung des HKVZ auf jeden Fall tätig werden, um die jeweilige Situation aufzuklären, sehen sie auch die Notwendigkeit, ihre Tätigkeit zu dokumentieren und die Akte u.a. zum Nachweis der durchgeführten Tätigkeit zumindest für sechs Jahre aufzubewahren, z.B. für den Fall, dass später evtl. Vorwürfe wegen unzureichender Tätigkeit erhoben werden oder dass bei der nächsten U-Untersuchung derselbe Fehler (z.B. falsche Meldedaten) passiert und das Jugendamt nach Vernichtung der Akte den Sachverhalt evtl. nochmals aufwendig recherchieren müsste.

Ich sehe es einerseits als ein nachvollziehbares Anliegen der Eltern an, dass über sie und ihr Kind nicht längerfristig eine Akte geführt wird, wenn sie sich korrekt verhalten haben, bzw. zumindest sichergestellt wird, dass die Dokumentation des Vorgangs ihnen nicht zum Nachteil gereichen wird. Andererseits ist mir auch nachvollziehbar, dass die Jugendämter eine Dokumentation ihrer Tätigkeit als notwendig ansehen. Die Dokumentation der Tätigkeit ist zur Aufgabenerfüllung erforderlich und steht im Einklang mit §§ 7, 11 HDSG. Was die Dauer der Speicherung der Dokumentation anbelangt, so erscheint mir eine einheitliche transparente Verfahrensweise in den Jugendämtern in Hessen wünschenswert, die beiden Interessen möglichst weitgehend gerecht wird. Die Speicherung bzw. Aufbewahrung der Unterlagen sollte im Jugendamt so erfolgen, dass kein Risiko für die Eltern entsteht, in einen falschen Verdacht zu geraten. Gemäß § 7 Abs. 5 HDSG steht betroffenen Eltern ein Widerspruch gegen die weitere Speicherung ihrer Daten zu, wenn ihr im konkreten Einzelfall schutzwürdige Gründe entgegenstehen. Unabhängig davon, dass die Speicherung der Dokumentation rechtmäßig ist, können Eltern daher eine zusätzliche Prüfung durch das Jugendamt veranlassen, ob die Daten aufgrund der besonderen persönlichen Lage der Betroffenen frühzeitig gelöscht werden können.

4.6.2 Ausgestaltung der Zugriffe auf Krankenhausinformationssysteme

Der Aufbau elektronischer Patientenakten in den Krankenhäusern erfordert eine differenzierte Ausgestaltung der Zugriffsmöglichkeiten des Personals. Bei der Umsetzung der datenschutzrechtlichen Vorgaben sind u.a. auch in Hessen Defizite bekannt geworden. Sowohl Krankenhäuser als auch Softwarehersteller sind gefordert, den Datenschutz zu verbessern. Die Datenschutzbeauftragten des Bundes und der Länder haben eine Arbeitsgruppe eingerichtet, um diesen Prozess zu unterstützen.

4.6.2.1 Rechtliche Ausgangspunkte

Ein Krankenhaus ist keine rechtliche Einheit, innerhalb derer personenbezogene Patientendaten beliebig offenbart werden dürfen. Dies gilt insbesondere vor dem Hintergrund, dass Krankenhausinformationssysteme (KIS) zu unverzichtbaren

Hilfsmitteln der Behandlung in Krankenhäusern geworden sind. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist technisch jederzeit ortsungebunden und sekundenschnell möglich. Dies ermöglicht einerseits eine schnelle und effiziente Information und Entscheidung durch das Personal, macht andererseits aber auch eine differenzierte Ausgestaltung der Zugriffsmöglichkeiten zwingend erforderlich. Z.B. rechnet ein Patient eines Universitätsklinikums nicht damit und muss auch nicht damit rechnen, dass die mehreren tausend Mitarbeiterinnen und Mitarbeiter des Universitätsklinikums seine sensitiven detaillierten medizinischen Daten während seiner Behandlung - vielleicht sogar noch Jahre danach - zur Kenntnis nehmen können. Sowohl in Deutschland wie auch international sind immer wieder Fälle bekannt geworden, in denen zu weit gehende Zugriffsrechte dazu geführt haben, dass Klinikmitarbeiter Behandlungsdaten von Bekannten, Kollegen oder Prominenten unzulässig eingesehen und weitergegeben haben.

4.6.2.1.1 Rechtslage in Hessen

Im Detail sind die datenschutzrechtlichen Vorgaben in den Bundesländern unterschiedlich geregelt. Nicht alle Bundesländer haben z.B. Landeskrankenhausgesetze verabschiedet. Im Grundsatz gilt aber bundesweit, dass ein Zugriff auf die Daten eines Patienten nur denjenigen Krankenhausmitarbeiterinnen und -mitarbeitern möglich sein darf, die in diese Behandlung einbezogen sind oder die Behandlung verwaltungsmäßig abwickeln. In Hessen ist im Hessischen Krankenhausgesetz (HKHG) ausdrücklich vorgeschrieben, dass die in § 12 Abs. 2 HKHG festgelegten rechtlichen Voraussetzungen für Datenübermittlungen entsprechend auch für die Weitergabe von Patientendaten zwischen Fachabteilungen Anwendung finden (§ 2 Abs. 3 HKHG).

§ 12 HKHG

(1) Für Krankenhäuser gelten die Bestimmungen des Hessischen Datenschutzgesetzes vom 11. November 1986 (GVBl. I S. 309) in der jeweils geltenden Fassung ohne die Einschränkung für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, nach Maßgabe der nachfolgenden Absätze.

(2) Die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses ohne die Einwilligung der oder des Betroffenen ist abweichend von den Vorschriften des Hessischen Datenschutzgesetzes nur zulässig, soweit dies erforderlich ist

1. zur Erfüllung des mit der Patientin oder dem Patienten oder für diese geschlossenen Behandlungsvertrages einschließlich der Durchsetzung oder Abwehr von Schadensersatzansprüchen;
2. zur Durchführung einer Mit- oder Nachbehandlung, soweit die Patientin oder der Patient nach Hinweis auf die beabsichtigte Übermittlung nichts anderes bestimmt hat;

.....

(3) Abs. 2 und § 33 HDSG gelten in Krankenhäusern mit Behandlungseinrichtungen verschiedener Fachrichtungen (Fachabteilungen) auch zwischen diesen.

Diese rechtlichen Vorgaben müssen auch bei der Ausgestaltung der Zugriffsberechtigungen des Krankenhausinformationssystems beachtet werden. Ein Zugriff auf personenbezogene Daten ist jeweils nur in dem Umfang zulässig, in dem die personenbezogenen Daten tatsächlich zur Erfüllung der jeweiligen konkreten Aufgabe der Beschäftigten erforderlich sind. So darf insbesondere eine Fachabteilung, die einen Patienten nicht behandelt, dessen detaillierte medizinische Daten grundsätzlich nicht zur Kenntnis erhalten, es sei denn, sie übernimmt die Mit- oder Nachbehandlung. Soweit die Organisation im Krankenhaus sich nicht mehr an Fachabteilungen orientiert, sind diese Vorgaben entsprechend umzusetzen, d.h. die Zugriffsausgestaltung muss dem Grundsatz der Erforderlichkeit entsprechen (zu weiteren Details s. auch das Arbeitspapier "Rechtsfragen der Kommunikation innerhalb des Krankenhauses" http://www.datenschutz.hessen.de/dg002.htm).

4.6.2.1.2 Rechtliche Vorgaben der EU-Datenschutzrichtlinie

Entsprechende rechtliche Vorgaben enthält auch die EU-Datenschutzrichtlinie (Richtlinie der EG 1995/46 vom 24. Oktober 1995). Zu den rechtlichen Anforderungen der Richtlinie an die Ausgestaltung von elektronischen Krankenakten hat die Art. 29 - Datenschutzgruppe der EU (ein in Art. 29 der Richtlinie vorgesehenes unabhängiges Beratungsgremium, in dem die Datenschutzbeauftragten aller EU-Mitgliedstaaten vertreten sind) 2007 ein Arbeitspapier veröffentlicht, in dem u.a. dargelegt wird, dass Ausgangspunkt der Ausgestaltung der Zugriffsberechtigungen der Behandlungszusammenhang sein sollte; Zugriff sollte nur haben, wer an der aktuellen Behandlung mitwirkt. Weitere Differenzierungen werden empfohlen, z.B. nach Art der medizinischen Fachkraft und nach Art der Daten. (Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 2007http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm.)

4.6.2.1.3 Entscheidung des Europäischen Gerichtshofs für Menschenrechte

2008 hat sich auch erstmals der Europäische Gerichtshof für Menschenrechte (EGMR) mit der Ausgestaltung und Kontrolle von Zugriffen auf Krankenhausdaten befasst (Rechtssache I v. Finland, Application No. 20511/03, Urteil vom 17. Juli 2008). Die Entscheidung betrifft den Fall einer Klägerin, die in einem öffentlichen Krankenhaus arbeitete und in diesem Krankenhaus auch als Patientin behandelt wurde. Auf das Krankenhausinformationssystem konnten zum Zeitpunkt ihrer Behandlung alle dort Beschäftigten zugreifen. Nachdem ihr Arbeitsvertrag nicht verlängert worden war, verklagte sie den Krankenhausträger als Arbeitgeber auf Schadensersatz und Schmerzensgeld, weil dies aus ihrer Sicht die Folge eines unbefugten Zugriffs auf ihre Krankheitsdaten durch ihren Arbeitgeber war. Sie verlor in allen Instanzen. Die finnischen Zivilgerichte wiesen sie mit der Begründung ab, sie habe nicht beweisen können, dass auf ihren Datensatz unbefugt zugegriffen wurde. Diesen Beweis konnte sie aber wegen einer unzureichenden Protokollierung der Zugriffe nicht führen. Auf ihre Klage hin hat nun der EGMR Finnland sowohl zur Zahlung von Schadensersatz als auch von Schmerzensgeld verurteilt,

und zwar mit folgender Begründung: In der fehlenden Protokollierung der Zugriffe liege ein Verstoß gegen das Menschenrecht auf Achtung des Privatlebens (Art. 8 Europäische Menschenrechtskonvention), weil dies der Grund dafür sei, dass die Klägerin nicht habe beweisen können, dass zu Unrecht auf ihre medizinischen Befunde zugegriffen wurde (zur Verarbeitung der Daten von Mitarbeiterinnen und Mitarbeitern als Patientinnen und Patienten im Krankenhaus s. auch Ziff. 4.6.3).

4.6.2.1.4 Konkrete Anforderungen

Was die Einzelheiten der Zugriffsausgestaltung in den Krankenhäusern anbelangt, so hängt die konkrete Umsetzung der rechtlichen Forderungen auch von organisatorischen und technischen Aspekten im jeweiligen Krankenhaus ab. Die folgenden Anforderungen müssen in jedem Fall berücksichtigt werden:

- Notwendig ist eine klare und differenzierte Festlegung der Zugriffsrechte je nach Behandlungsrolle, -ort und -zeit. Abhängig von der jeweiligen Behandlungsrolle (z.B. Chefarzt, Arzt, Krankenschwester, Mitarbeiter in der Rechtsabteilung, im Sozialdienst, im Controlling etc.) benötigt ein Mitarbeiter eines Krankenhauses in unterschiedlichem Umfang Zugriffsberechtigungen. Nicht für alle Mitarbeiter ist nach Abschluss der Behandlung noch jahrelang eine Zugriffsmöglichkeit notwendig. Der Zugriff auf die Krankenakten entlassener Patienten muss daher nach Ablauf eines angemessenen Zeitraums nach Abschluss einer Fallbehandlung auf einen eingeschränkten Personenkreis reduziert werden (z.B. für die Beantwortung von Befundanfragen, für eine evtl. Wiederaufnahme, für die Forschung).

- Lesende und ändernde Zugriffsberechtigungen sind zu unterscheiden.

- Die Zugriffe müssen grundsätzlich nachvollziehbar und kontrollierbar sein (§ 12 HKG i.V.m. § 10 HDSG). Eine nachträgliche Überprüfung und Aufklärung von Zugriffen muss mit verhältnismäßigem Aufwand möglich sein.

- Es müssen angemessene technisch-organisatorische Datensicherheitsmaßnahmen getroffen werden.
  Ein Datenschutz- und Datensicherheitskonzept ist ein wichtiger Schritt, um die Anforderungen umzusetzen. Dabei sind nicht nur Maßnahmen gegen unbefugte Zugriffe von außen und die Absicherung der Kommunikation mit anderen Stellen zu betrachten. Das Konzept muss auch beschreiben, wie die Zugriffe der Mitarbeiter des Krankenhauses auf das zulässige Maß eingeschränkt werden sollen. Ein weiterer wesentlicher Teil betrifft die Frage, wie die Nachvollziehbarkeit (Revision) der Datenverarbeitung gewährleistet werden soll. Dazu gilt es u.a. zu regeln, wie die Vergabe von Benutzerkennungen und Zugriffsrechten dokumentiert wird. Außerdem müssen Art und Umfang der Protokollierung und die Auswertung festgelegt werden (zu Details siehe Ziff. 10.1 Orientierungshilfe zur Protokollierung).

- Das System muss für die Fälle, in denen mehrere rechtlich unabhängige Stellen Daten verarbeiten, deren Daten sicher trennen. Dazu muss es möglich sein technisch sicherzustellen, dass eine Benutzerkennung nicht nur auf der Anwendungsebene, sondern auch bereits durch Prüfungen auf der Netzwerk-, Betriebssystem- oder Datenbankebene am Zugriff auf die Daten einer anderen Stelle gehindert wird.

- Die Zugriffsmöglichkeiten der Administratoren müssen soweit wie möglich eingeschränkt sein. Insbesondere in größeren Krankenhäusern folgt daraus auch eine personelle Trennung zwischen der Systemadministration und der Administration der Fachanwendungen. Gerade die Tätigkeit der Administratoren muss nachvollziehbar sein. Deshalb sollte dieser Punkt im o.g. Datenschutz- und Datensicherheitskonzept explizit aufgegriffen werden.

4.6.2.2 Defizite in der Praxis und Konsequenzen

4.6.2.2.1 Überprüfung einer Beschwerde

Im Zusammenhang mit Überprüfungen der Datenübermittlungen zwischen Krankenhäusern und Medizinischen Versorgungszentren habe ich bereits in meinem Tätigkeitsbericht für 2008 festgestellte Probleme dargestellt (37. Tätigkeitsbericht, Ziff. 4.7.4). Im Berichtszeitraum habe ich eine Beschwerde zum Anlass genommen, die Ausgestaltung der Zugriffsberechtigungen auf das KIS der betroffenen Klinik vor Ort zu überprüfen. Im Rahmen der Prüfung habe ich erhebliche Defizite bei der Ausgestaltung der Zugriffsberechtigungen und Abläufe festgestellt.

- Für mehrere Benutzergruppen innerhalb des Klinikums waren zu pauschale Zugriffsmöglichkeiten eingerichtet, d.h. die festgelegten Zugriffsberechtigungen auf Dokumente im KIS waren nicht auf den für die jeweilige Aufgabenerfüllung und den jeweiligen Zweck erforderlichen Umfang eingegrenzt.
  - So konnten z.B. nahezu alle im Klinikum beschäftigen Ärztinnen und Ärzte mit einer speziellen Suchanfrage auf alle medizinischen Daten aller aktuellen und ehemaligen Patientinnen und Patienten des Klinikums zugreifen. Aufgrund meiner Stellungnahme wurden die Zugriffsmöglichkeiten kurzfristig bereits reduziert. Darüber hinaus ist ein neues Rollenkonzept geplant, das die Eröffnung fachbereichsübergreifender allgemeiner Zugriffsberechtigungen weitgehend ablösen soll. Grundsätzlich sollen alle Ärztinnen und Ärzte die Berechtigung zum Zugriff auf die Daten ihrer eigenen Fachabteilung haben. Bei Bedarf kann die Zugriffsberechtigung auch für mehrere Fachabteilungen gewährt werden (z.B. beim Nachtdienst). Hierzu kann ein Arzt bei der Anmeldung am KIS entsprechend seiner aktuellen Funktion ein Profil mit korrespondierenden Zugriffsrechten auswählen. Es gibt sein normales Profil und es können für ihn weitere Profile, beispielsweise für den Nachtdienst in zwei Abteilungen oder einen Notdienst, vorgegeben sein. Diese Profile werden Sonderuser genannt. Wird ein Sonderuser ausgewählt, erfolgt ein Protokolleintrag. Im Protokoll wird mit Datum und Uhrzeit gespeichert, mit welchem Sonderuser, und somit anderen Zugriffsrechten, der Arzt mit seiner Benutzerkennung arbeitet. Die Zugriffe auf die Patientendaten anderer Fachabteilungen als der im normalen Profil aufgeführten Fachabteilung werden protokolliert. Bei elektronischen Leistungsanforderungen von anderen Fachabteilungen sollen nur noch die Daten des aktuellen betroffenen Falls eingesehen werden können, nicht

mehr die gesamten Daten der anfordernden Fachabteilung. Nur noch in begründeten Einzelfällen soll ein Arzt ein Sonderuser-Profil erhalten, das eine fachübergreifende Patientensuche in vorgegebenen anderen Abteilungen möglich macht.

- Wesentlich reduziert wurden auch die Zugriffsmöglichkeiten der Chefarztsekretariate, des Bereichs Recht und Organisation und des Patientenbeschwerdemanagements. Der Sozialdienst wird künftig nur noch bei Bedarf eine Zugriffsmöglichkeit auf den konkreten Fall erhalten.

- Verschiedene rechtlich selbstständige externe Stellen (Arztpraxen, Medizinisches Versorgungszentrum, privates Schreibbüro) hatten pauschale Zugriffsmöglichkeiten, die rechtlich und technisch nicht den Anforderungen des Datenschutzes entsprachen.
- Die Zugriffsmöglichkeit einer externen Praxis wurde bereits am Tag meiner Prüfung vollständig deaktiviert. Insgesamt wird für externe Praxen und MVZ auch vom Klinikum die Notwendigkeit weitreichender organisatorischer und technischer Änderungen gesehen und derzeit ein Konzept erarbeitet. Was das private Schreibbüro anbelangt, so wurden die Zugriffsmöglichkeiten kurzfristig verändert.

- Die Diskussion über einige weitere Bereiche ist noch nicht abgeschlossen. Teilweise ist eine Lösung der Probleme dadurch wesentlich erschwert, dass das eingesetzte KIS die Umsetzung der datenschutzrechtlichen Anforderungen nicht hinreichend technisch unterstützt.

– Trotz der ursprünglich sehr umfangreichen pauschalen Zugriffsmöglichkeiten wurden lesende Zugriffe auf die Patientendaten im Klinikum unzureichend protokolliert, die entsprechenden Funktionen im KIS waren nicht vollständig aktiviert. Aus diesem Grund konnte auch bezüglich der Beschwerde ein Datenschutzverstoß weder festgestellt noch ausgeschlossen werden. Bereits kurz vor meiner Prüfung wurden alle Protokollierungsmöglichkeiten des Systems eingeschaltet.

  Aus datenschutzrechtlicher Sicht habe ich eine Protokollierung aller lesenden Zugriffe der bettenführenden Fachabteilung auf die "eigenen" medizinischen Daten nicht als notwendig angesehen. Für alle darüber hinausgehenden Zugriffsberechtigungen ist eine Protokollierung lesender Zugriffe geboten. Dabei ist zu beachten, dass eine Protokollierung nur zielführend sein kann, wenn eine stichprobenhafte Überprüfung und die Kontrolle von Einzelfällen in effektiver Weise gewährleistet ist. Eine Überprüfung sollte auch dazu beauftragten Personen möglich sein, die nicht über Fachkenntnisse bezüglich der Datenbank verfügen. Diese Anforderungen waren zu dem Zeitpunkt, auf den sich die Beschwerde bezog, nicht erfüllt. Ein Konzept zur Ausgestaltung der Protokollierung wird erarbeitet; auf Basis des Konzepts soll dann ein eigenes Tool programmiert werden.

  Eine wesentliche Kontrollfunktion ist dann theoretisch vorhanden. Zur vollständigen Umsetzung ist es erforderlich, dass die Klinikleitung dem internen Datenschutzbeauftragten den expliziten Auftrag erteilt, die Zugriffe bei konkretem Anlass und stichprobenhaft nachzuvollziehen und auf ihre Erforderlichkeit zu überprüfen, soweit notwendig auch durch Befragung der betroffenen Mitarbeiter.

– Die Verwaltung der Benutzer des KIS durch das Klinikum war lückenhaft. So war z.B. nicht sichergestellt, dass nach dem Wechsel eines Mitarbeiters zu einer privaten Praxis die Benutzerdaten und die damit verbundenen Berechtigungen korrigiert werden.
  Die Ablauforganisation der Benutzerverwaltung wurde komplett für jegliches Login überarbeitet.

– Die Datenbestände der rechtlich unabhängigen Stellen sollen auch technisch weitgehend getrennt werden. Es ist beabsichtigt, die Daten in getrennten Systemumgebungen mit jeweils eigenen Datenbanken zu verarbeiten. Benutzerkennungen sollen je Systemumgebung eingerichtet werden. Dieser Ansatz erfüllt die Anforderungen, die an ein mandantenfähiges System gestellt werden.

4.6.2.2.2 Bundesweite Aktivitäten

Auch in anderen Bundesländern wurden teilweise erhebliche Defizite festgestellt. So hat z.B. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in seiner Presseerklärung vom 2. Juni 2009 darauf hingewiesen, dass Prüfungen in Krankenhäusern erhebliche Missbrauchsgefahren bei der Nutzung elektronischer Patientenakten offenbarten (http://www.hamburg.de/datenschutz/aktuelles/1506372/pressemeldung-2009-06-02.html) und gemeinsam mit behördlichen und betrieblichen Datenschutzbeauftragten der Hamburger Krankenhäuser "Normative Eckpunkte für Zugriffe auf elektronische Patientendaten im Krankenhaus" für die weitere Diskussion entworfen (http://www.hamburg.de/contentblob/1722358/data/normative-eckpunkte-patientendaten.pdf).

Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer 78. Konferenz am 8. und 9. Oktober 2009 mit diesem Thema befasst und eine Entschließung dazu verabschiedet: "Krankenhausinformationssysteme datenschutzgerecht gestalten!" (s. Ziff. 9.12). Darüber hinaus haben die Datenschutzbeauftragten des Bundes und der Länder eine gemeinsame Arbeitsgruppe eingerichtet, die auf eine generelle Verbesserung des Datenschutzes in den Krankenhäusern abzielt. Sie wollen gemeinsame Diskussionen u.a. mit Krankenhausvertretern und auch mit Software-Herstellern initiieren. Wenn Software-Hersteller auf dem Markt langfristig durchsetzbare datenschutzgerechte Produkte anbieten wollen, müssen sie in ihren Systemen die Abbildung einer behandlungs- und patientenbezogenen Zugriffslogik sowie die notwendigen Funktionen für eine effiziente Protokollierung und Auswertung der Protokolle unterstützen. Der Hessische Datenschutzbeauftragte wird sich an dieser Arbeitsgruppe beteiligen.

4.6.3 Krankenhausmitarbeiter als Patienten im Krankenhaus

Immer wieder richten Krankenhausmitarbeiter Anfragen an mich, wie ihre eigenen Behandlungsdaten im Krankenhaus effektiv geschützt werden können. Die datenschutzrechtlichen Regelungen schreiben vor, dass die Krankheitsdaten ausschließlich zweckgebunden verwendet werden dürfen. Insbesondere darf die Personalabteilung keine Kenntnis der Behandlungsdaten erhalten.

Offensichtlich kommt es relativ oft vor, dass sich Krankenhausmitarbeiter bei einer Erkrankung in dem Krankenhaus, in dem sie arbeiten, auch als Patient behandeln lassen. Hintergrund kann z.B. sein, dass ihnen ein kompetenter Krankenhausarzt persönlich bekannt ist und sie sich von ihm behandeln lassen möchten, oder dass eine Behandlung in diesem Krankenhaus für sie zeitlich leichter einzurichten ist. Immer wieder erhalte ich jedoch zu dieser Situation Anfragen: Krankenhausmitarbeiter fragen nach, wie ihre Behandlungsdaten geschützt sind, weil sie befürchten, dass Informationen über ihre Krankheit ihrem Arbeitgeber zur Kenntnis gelangen könnten und sich dies nachteilig für sie auswirken könnte. Auch interne Datenschutzbeauftragte erkundigen sich häufig, ob es für diese Situation spezielle Regelungen gibt und/oder spezielle Verfahrensabläufe realisiert werden können.

4.6.3.1 Rechtliche Vorgaben für eine zweckgebundene Verwendung der Behandlungsdaten im Krankenhaus

Für die Verarbeitung personenbezogener Patientendaten im Krankenhaus gelten die speziellen Regelungen in § 12 Abs. 2 HKG; ergänzend sind gemäß § 12 Abs. 1 HKG die Bestimmungen des Hessischen Datenschutzgesetzes (HDSG) anzuwenden. Gemäß §§ 13 Abs. 1 und 2, 12 Abs. 2 und 3 HDSG dürfen die Patientendaten grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind, d.h. konkret für die Durchführung des Behandlungsvertrages. Ein Zugriff auf personenbezogene Daten ist jeweils nur in dem Umfang zulässig, in dem die personenbezogenen Daten tatsächlich zur Erfüllung der jeweiligen konkreten Aufgabe der Beschäftigten erforderlich sind. Ein Krankenhaus ist daher keine rechtliche Einheit, innerhalb derer personenbezogene Patientendaten beliebig offenbart werden dürfen. Auch innerhalb des Krankenhauses gilt die ärztliche Schweigepflicht im Sinne der Berufsordnung und des Strafgesetzbuchs. So darf insbesondere eine Fachabteilung, die einen Patienten nicht behandelt, dessen detaillierte medizinische Daten grundsätzlich nicht zur Kenntnis erhalten, es sei denn, sie übernimmt die Mit- oder Nachbehandlung. Das Verwaltungspersonal hat Zugriff auf die Patientendaten, soweit dies für seine Aufgabenerfüllung und für den jeweiligen Zweck erforderlich ist im Rahmen der Durchführung des Behandlungsvertrages (z.B. Abrechnung mit den Kostenträgern, Daten i.S.v. § 301 SGB V).

Spezielle Regelungen für den Umgang mit den Patientendaten der eigenen Krankenhausmitarbeiter gibt es nicht. Gerade in diesen Konstellationen ist jedoch die strikte Einhaltung der Zweckbindung der Behandlungsdaten von besonderer Bedeutung für die Betroffenen. Weder die Personalabteilung noch möglicherweise persönlich interessierte Kolleginnen oder Kollegen dürfen die Behandlungsdaten zur Kenntnis erhalten. Die Krankenhäuser müssen sich - auch in ihrem eigenen Interesse - überlegen, wie sie die Behandlungsdaten ihrer Mitarbeiterinnen und Mitarbeiter angemessen schützen können. Dabei kommt es entscheidend auf die Situation vor Ort an. Grundsätzlich ist es z.B. möglich, dass ein Krankenhaus auf freiwilliger Basis einen über die dargelegten Vorschriften hinausgehenden Schutz einführt, indem es eine Pseudonymisierung der Patientendaten aller Krankenhausmitarbeiter vornimmt. Allerdings ist dies organisatorisch zumindest während des Zeitraums der Behandlung sehr schwierig, weil während einer Behandlung im Regelfall Dokumente zu dem Behandlungsfall empfangen und auch an externe Dritte versandt werden müssen und zu diesem Zweck ständig pseudonymisiert und depseudonymisiert werden müsste. Dem Hessischen Datenschutzbeauftragten ist bisher leider keine effektive Pseudonymisierungslösung in einem Krankenhaus zu diesem Zweck bekannt. Die o.a. dargelegten rechtlichen Vorgaben zur Zweckbindung der Daten können bei entsprechender Umsetzung (s. hierzu auch den Beitrag Ziff. 4.6.2) einen weitgehenden Schutz der Patientendaten gewährleisten. Zu Fragen der Vorgaben kann ein Mitarbeiter bei Bedarf den internen Datenschutzbeauftragten des Krankenhauses oder auch den Hessischen Datenschutzbeauftragten einschalten. Wenn einem Krankenhausmitarbeiter dies nicht ausreicht, bleibt ihm die Möglichkeit, für seine Behandlung ein anderes Krankenhaus aufzusuchen.

4.6.3.2 Zur Problematik eines Abgleichs der Daten neu aufgenommener Krankenhauspatienten mit den Personaldaten des Klinikums für Genesungswünsche

Im Berichtszeitraum erreichte mich die Anfrage eines Klinikums, das jedem im Klinikum stationär einliegenden Krankenhausmitarbeiter Genesungswünsche und einen Blumenstrauß zukommen lassen wollte. Um dies lückenlos gewährleisten zu können, wurde überlegt, die im Krankenhausinformationssystem gespeicherten Patientendaten mit den Daten der Personaldatenbank abzugleichen. In der von mir erbetenen Stellungnahme zu dieser geplanten Maßnahme habe ich mich kritisch dazu geäußert:

Die Intention, den in der Klinik behandelten Mitarbeiterinnen und Mitarbeitern Genesungswünsche und einen Blumenstrauß zukommen zu lassen, war vom Klinikum zweifelsohne als freundliche Geste gemeint. Die jahrelange Erfahrung des Hessischen Datenschutzbeauftragten ist es aber, dass Patienten, die zugleich Mitarbeiter des sie behandelnden Krankenhauses sind, oft in Sorge sind, dass ihr Arbeitgeber Krankheitsdaten über sie erfährt und eine Kenntnisnahme des Arbeitgebers bzw. der Personalabteilung von ihrer Behandlung im Krankenhaus definitiv nicht wünschen, sondern vielmehr auf eine strikte Abschottung ihrer Behandlungsdaten von der Personalabteilung dringen. Ein Abgleich der Behandlungsdaten mit der Personaldatenbank des Klinikums wäre eine **Änderung der Zweckbestimmung** der im Krankenhausinformationssystem gespeicherten Daten. Gemäß §§ 13 Abs. 1 und 2, 12 Abs. 2 und 3 HDSG dürfen die Patientendaten grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind. Im konkreten Fall wurden die Patientendaten zur Durchführung des Behandlungsvertrages erhoben und gespeichert. Die in § 12 Abs. 2 und 3 HDSG abschließend aufgeführten Voraussetzungen, unter denen eine Änderung der Zweckbestimmung der Daten zulässig ist, sind im vorliegenden Fall nicht einschlägig.

§ 12 Abs. 2 und 3 HDSG

(2) Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht, zwingend voraussetzt oder der Betroffene eingewilligt hat,

2. die Bearbeitung eines vom Betroffenen gestellten Antrags ohne Kenntnis der Daten nicht möglich ist oder Angaben des Betroffenen überprüft werden müssen; der Betroffenen ist darauf hinzuweisen, bei welchen Personen oder Stellen seine Daten erhoben werden können,

3. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit und persönliche Freiheit dies gebietet,

4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder

5. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(3) 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.

Überlegt wurde von der Klinik, für die geplante Maßnahme eine Einwilligung der Betroffenen einzuholen. Grundsätzlich ist eine Verarbeitung von Patientendaten mit Einwilligung der Betroffenen möglich. Allerdings muss die Freiwilligkeit der Einwilligung sichergestellt sein (was im Rahmen von Beschäftigungsverhältnissen durchaus problematisch sein kann) und es muss sich um eine informierte Einwilligung handeln, d.h. vor der Einwilligung müssten die betroffenen Mitarbeiterinnen und Mitarbeiter schriftlich darüber informiert werden, wer im Klinikum welche Daten von ihnen zu welchem Zweck erhält und auf welche Art und Weise und wie lange sie im Klinikum für diesen Zweck weiterverarbeitet werden.

Diskutiert wurde auch die Möglichkeit, einen Abgleich der Daten des Krankenhausinformationssystems mit der Personaldatenbank vorzusehen und den Krankenhausmitarbeitern ein Widerspruchsrecht gegen diese Maßnahme einzuräumen. Eine solche Verfahrensweise würde nicht die o.a. gesetzlichen Anforderungen an eine Änderung der Zweckbestimmung der Behandlungsdaten erfüllen und wäre daher unzulässig. Ein Widerspruchsrecht ist gegenüber einer Einwilligung ein deutlich begrenzteres Recht und ist nur dann ausreichend, wenn eine gesetzliche Regelung ausdrücklich ein Widerspruchsrecht statt einer Einwilligungslösung vorsieht.

4.6.4 Ausgestaltung der Zugriffsmöglichkeiten auf Patientendaten innerhalb eines Medizinischen Versorgungszentrums

In dem Berichtszeitraum habe ich die Diskussion über die Ausgestaltung der Zugriffsberechtigungen in MVZ fortgesetzt. Zu den von mir zusammengestellten zentralen Anforderungen hat die LÄK differenziert Stellung genommen. Es besteht in vielen Punkten Konsens. Einige Fragen sind noch offen.

4.6.4.1 Einleitung

Im 37. Tätigkeitsbericht hatte ich über verschiedene Rechtsfragen im Zusammenhang mit MVZ berichtet (Ziff. 4.7.4). Ich hatte zunächst die rechtlichen Voraussetzungen einer Übermittlung von Patientendaten zwischen Kliniken und MVZ dargelegt (s. Bilanzbeitrag Ziff. 8.3). Ein weiteres Thema dieses Tätigkeitsberichts war die Ausgestaltung der Zugriffsmöglichkeiten auf Patientendaten innerhalb eines MVZ. Bundesweit gibt es teilweise MVZ mit bis zu 70 Ärzten und Patienten haben ein berechtigtes Interesse daran, dass ihre Krankheitsdaten nur denjenigen Personen bekannt werden, die in ihre Behandlung einbezogen sind.

Stichprobenhafte Prüfungen hatten gezeigt, dass in MVZ
- nur teilweise verschiedene Rollen wie z.B. Administrator, Arzt, Arztgehilfin etc. unterschieden werden und
- Differenzierungen hinsichtlich des Zugriffs durch die Ärztinnen und Ärzte vielfach gar nicht getroffen werden.

Zu diesem Thema hat 2009 eine gemeinsame Besprechung mit dem RP Darmstadt, der LÄK und der KV Hessen stattgefunden. In den Gesprächen zeigte sich, dass die MVZ rechtlich und organisatorisch sehr verschieden aufgebaut werden können und dementsprechend die Anforderungen an die Ausgestaltung der Zugriffsmöglichkeiten auf Patientendaten auch differenziert formuliert werden müssen.

4.6.4.2 Zentrale Anforderungen an die Zugriffsausgestaltung

Aufgrund der Diskussionen habe ich die folgenden zentralen Anforderungen zusammengestellt:

- **Einwilligung/Widerspruchsrecht des Patienten**
  Die ärztliche Schweigepflicht und die Vorgaben des BDSG bzw. des LDSG zu den technischen Datensicherheitsmaßnahmen finden auch innerhalb von Kooperationspraxen und MVZ Anwendung. Die Vorstellung/Erwartung eines Patienten, der in eine Kooperationspraxis bzw. in ein MVZ geht, ist sicherlich unterschiedlich. In jedem Fall wird es auch Patienten geben, die gezielt zu einem Arzt in Behandlung gehen und gerade auch in großen Kooperationspraxen bzw. MVZ und/oder bei bestimmten Erkrankungen erwarten, dass nicht alle Ärzte ihre persönlichen medizinischen Daten zur Kenntnis nehmen können. Wenn in bestimmten Konstellationen von einer mutmaßlichen Einwilligung des Patienten in die Datenweitergabe innerhalb der Kooperationspraxis bzw. des MVZ ausgegangen wird, muss dem Patienten zumindest ein Widerspruchsrecht gegen eine allgemeine Kenntnisnahme seiner Daten innerhalb der Kooperationspraxis bzw. des MVZ eingeräumt werden. Jedenfalls bei großen Kooperationspraxen und MVZ bestehen aber erhebliche Zweifel, ob hier noch von einer mutmaßlichen Einwilligung des Patienten in eine allgemeine Kenntnisnahme der Daten durch alle Ärzte ausgegangen werden kann.

- **Möglichkeiten, mehr Transparenz für den Patienten sicherzustellen**
  Zwingend erforderlich ist mehr Transparenz für den Patienten, welche Stelle seine Daten verarbeitet (z.B. Klinik oder MVZ) und in welchem Umfang und für welchen Zweck seine Daten innerhalb der Kooperationspraxis bzw. dem MVZ anderen Ärzten, die ihm nicht als Behandler bekannt sind, zur Kenntnis gelangen können.

- **Differenzierung der Zugriffsrechte nach Rolle und Umfang der Zugriffsberechtigung**
  Wie für jede andere Daten verarbeitende Stelle auch besteht für Kooperationspraxen und MVZ die Notwendigkeit der Differenzierung nach Rollen und Umfang der Zugriffsberechtigung (Ärzte, Arztgehilfe, Aufnahme, Administrator …). Außerdem muss es für jeden Benutzer eine eigene Kennung geben, da nur so Protokolleinträge der richtigen Person zugeordnet werden können. Dies sind wesentliche Bestandteile der Revisionsfähigkeit der Datenverarbeitung und als solche unerlässlich auch unter Haftungsaspekten.

- **Alternativen der technischen Maßnahmen zur Gewährleistung der Revisionssicherheit und der Patientenrechte**
  Für die Umsetzung der o.a. Anforderungen (Revisionssicherheit, Widerspruchsrecht des Patienten) kommen grundsätzlich verschiedene technische Maßnahmen in Betracht.
  Unstreitig müssen ändernde Zugriffe nachvollziehbar sein. Soweit es sich um Zugriffe handelt, bei denen in Papierdokumenten eine Unterschrift des Arztes zwingend erforderlich ist, kann diese nur durch eine qualifizierte elektronische Signatur ersetzt werden; dies muss beachtet werden, wenn elektronische Dokumente die rechtlich verbindliche Behandlungsdokumentation darstellen.

  Wenn der Widerspruch eines Patienten gegen eine Einsichtnahme bestimmter Ärzte in seine Patientendaten technisch zwingend umgesetzt werden soll, dürfen diese Ärzte nicht auf die Daten zugreifen können. Die Möglichkeit eines allgemeinen lesenden Zugriffs durch diese Ärzte wäre in diesem Fall nicht akzeptabel. Wenn demgegenüber der Widerspruch eines Patienten gegen eine Einsichtnahme nur durch Protokollierung lesender Zugriffe, Durchsicht der Protokolle und bei Bedarf Aufklärung des Sachverhalts soweit wie möglich gewährleistet werden soll, können Ärzte technisch auf die Daten dieses Patienten zugreifen und ein unberechtigter Zugriff kann nur durch nachträgliche Kontrollen festgestellt und evtl. sanktioniert werden. In diesem Fall muss eine zeitnahe, technisch unterstützte effektive Auswertung der Protokolle gewährleistet werden.

4.6.4.3 Offene Fragen

In Absprache mit dem RP Darmstadt habe ich die in dem gemeinsamen Gespräch noch nicht abschließend geklärten Fragen zusammengefasst und die LÄK und die KV Hessen um schriftliche Stellungnahme gebeten. Die LÄK hat sich eingehend mit der Frage auseinandergesetzt, welche Ärzte innerhalb eines MVZ auf die Daten eines Patienten zugreifen dürfen und dabei folgendes Mehrstufenmodell vorgeschlagen:

- Überschaubarer Kreis von behandelnden Ärzten in einer ambulanten Einrichtung.
- Überschaubarer Kreis von behandelnden Ärzten in der jeweiligen Fachabteilung einer ambulanten Einrichtung.
- Größerer Kreis von behandelnden Ärzten sowohl in der ambulanten Einrichtung als auch in der jeweiligen Fachabteilung.

Je nach Konstellation befürwortet die LÄK eine unterschiedliche interne Verfahrensweise.

Stellungnahme der LÄK (Auszug)

Überschaubarer Kreis von behandelnden Ärzten in einer ambulanten Einrichtung

Grundsätzlich gehen wir davon aus, dass der Patient mit Abschluss des Behandlungsvertrages zumindest konkludent die datenschutzrechtliche Einwilligung abgibt, die Patientendaten in der jeweiligen Einrichtung zu erheben, zu nutzen und zu verarbeiten, sofern dies denn nach § 28 Abs. 7 BDSG erforderlich ist.

Hinsichtlich des Merkmals der Erforderlichkeit beziehen wir auch Vertretung während Urlaub und Krankheit sowie die Tätigkeit im Mehrschichtbetrieb mit ein.

Übertragen auf ein MVZ oder eine Gemeinschaftspraxis, in welchem eine überschaubare Anzahl von Ärzten fachübergreifend tätig ist, bedeutet dies, dass ein Patient aufgrund des Behandlungsvertrages Anspruch auf die gesamte Kompetenz

dieser Ärzte hat und jeden Arzt der dort vertretenen Fachrichtung erforderlichenfalls auch ermächtigt, in die Behandlungsunterlagen Einblick zu nehmen. Im Regelfall sucht der Patient eine solche ambulante Einrichtung gezielt wegen der dort vorhandenen Fachkompetenz aus. Wünscht er abweichend eine Behandlung durch einen bestimmten Arzt nicht, ist es an ihm, ausdrücklich zu widersprechen.

Sofern neben dem oder den Praxisinhabern angestellte Ärzte in einer Praxis tätig werden, hat die Landesärztekammer, auch um den Datenschutz des Patienten zu stärken, in die Berufsordnung die Verpflichtung aufgenommen, den Patienten über die Tätigkeit von angestellten Ärzten in angemessener Weise zu informieren (§ 19 Abs. 4 Berufsordnung).

Ein Beispiel eines MVZ mit aus unserer Sicht noch überschaubarer Anzahl von tätigen Ärzten kann wie folgt beschrieben werden: In einem MVZ sind acht Ärzte der Fachrichtung Radiologie und acht Ärzte aus der Fachrichtung Orthopädie und Unfallchirurgie tätig. Ein Patient bedarf nach Beratung eines Facharztes für Orthopädie und Unfallchirurgie zunächst einer radiologischen Untersuchung und anschließend eine orthopädischen Therapie mit abschließender radiologischer Untersuchung.

Sicher ist die im eben erwähnten Beispielsfall herausgegriffene Zahl von acht Ärzten pro Fachgebiet willkürlich. Da in einem MVZ jedoch ein Arztsitz durch vier Ärzte in Teilzeitbeschäftigung wahrgenommen werden kann, macht dieses Beispiel deutlich, dass der Patient bei entsprechender Behandlungsdauer in der Regel mit allen in diesem MVZ tätigen Ärzten in Kontakt treten wird.

Vorbemerkung zu Einrichtungen mit einem nicht mehr überschaubaren Kreis von behandelnden Ärzten

Sofern der Kreis der in einem MVZ tätigen Ärzte jedoch so groß ist, dass regelmäßig nicht mehr davon ausgegangen werden kann, dass die dort tätigen Ärzte auch unter Berücksichtigung von Urlaubs- und Krankheitsvertretung sowie Einsatz im Mehrschichtsystem im Regelfall mit der Betreuung eines bestimmten Patienten befasst sein können, kann die oben erwähnte Parallele zwischen behandlungsvertragsrechtlicher Willenserklärung und datenschutzrechtlicher Einwilligung fraglich sein.

Wann dieser Fall eintritt, kann in absoluten Zahlen unserer Ansicht nach nicht festgelegt werden. Hier kommt es auf die Organisation des MVZ im Einzelfall an. Sofern die hier vorgeschlagene Vorgehensweise anhand eines Mehrstufenmodells in der Praxis umgesetzt werden kann, kann zukünftig ggf. im Rahmen der Rechtsberatung einzelner Einrichtungen auf Erfahrungswerte zurückgegriffen werden.

Überschaubarer Kreis von behandelnden Ärzten in der jeweiligen Fachabteilung einer ambulanten Einrichtung

Bei einem überschaubaren Kreis von behandelnden Ärzten in der jeweiligen Fachabteilung sollte zunächst geprüft werden, ob eine datenschutzrechtliche Orientierung anhand von Fachabteilungen möglich ist. Gegebenenfalls kommt eine Anlehnung an den Grundgedanken des § 12 Abs. 3 Landeskrankenhausgesetz in Betracht. Insoweit kann eine Begrenzung der Einwilligung auf die jeweilige Facharztgruppe, welche der Patient zunächst aufsucht, nach den unter 1. genannten Voraussetzungen angenommen werden.

Wird beispielsweise die Behandlung des Patienten nach Aufnahme durch einen Facharzt für Orthopädie durch weitere Fachärzte notwendig, ist bei lebensnaher Betrachtung davon auszugehen, dass der zuvor behandelnde Facharzt den Patienten bspw. auf die Untersuchung und Behandlung durch Fachärzte für Radiologie hinweist. Folgt der Patient dieser Empfehlung ist zumindest eine konkludente Einwilligung zur Behandlung für die jeweilige in der ambulanten Einrichtung weiter tätige zahlenmäßig überschaubare Facharztgruppe anzunehmen.

Über die Verfahrensweise sollte der Patient zuvor schriftlich informiert werden. Für die interne Organisation ist zudem zu fordern, dass die Ärzte nur dann Zugriff auf die Patientenunterlagen nehmen, wenn deren Hinzuziehung für die medizinische Behandlung notwendig ist. Im Regelfall sollte dies dokumentiert werden.

Größerer Kreis von behandelnden Ärzten sowohl in der ambulanten Einrichtung als auch in der jeweiligen Fachabteilung

Erst wenn auch die einzelnen Fachgruppen in einer zahlenmäßigen Anzahl vorhanden sind, welche es ausschließt, dass alle in der jeweiligen Fachgruppe tätigen Ärzte die Behandlungsunterlagen für die Untersuchung oder Behandlung des Patienten benötigen, muss über weitere Einwilligungserfordernisse nachgedacht werden. Dies kann insbesondere bei einem MVZ in der von Ihnen beschriebenen Größe von bis zu 70 angestellten Ärzten der Fall sein.

In einem solchen Fall sollte der Patient aus unserer Sicht über die Notwendigkeit der datenschutzrechtlichen Einwilligung zur Datenerhebung und -verarbeitung zu Beginn einer Behandlung besonders informiert werden. Eine mögliche Formulierung könnte sein:

"In unserem MVZ sind …. Ärzte tätig. Um auch in Ihrem Interesse die Warte- und Behandlungszeiten kurz zu halten, wird der erstaufnehmende Arzt mit Ihnen die weiteren Untersuchungen und Behandlungen vereinbaren. Sie werden dann von unserem medizinischen Fachpersonal zum nachfolgenden Arzt geleitet. Dieser stellt sich mit Namen und Funktion vor. Sofern Sie mit der Weiterbehandlung oder Untersuchung nicht einverstanden sind, müssen Sie der Behandlung oder Untersuchung und der Nutzung ihrer Daten durch diesen Arzt widersprechen."

Für die interne Organisation ist auch hier zu fordern, dass die Ärzte nur dann Zugriff auf die Patientenunterlagen nehmen, wenn deren Hinzuziehung für die medizinische Behandlung notwendig ist. Im Regelfall sollte dies dokumentiert werden.

Die differenzierte und fundierte Stellungnahme der LÄK bietet aus meiner und aus Sicht des RP Darmstadt grundsätzlich einen geeigneten Orientierungsrahmen für Medizinische Versorgungszentren. Konkretisierungen der Verfahrensweisen müssen noch diskutiert werden.

Die KV Hessen hat zu den von mir zusammengestellten offenen Fragen keine konkreten schriftlichen Vorschläge unterbreitet.

4.6.5 Zentrale Datenbank für die Erforschung des chronischen Nierenversagens

Die KfH-Stiftung Präventivmedizin will eine nachhaltige Infrastruktur für die Forschung im Bereich der Nephrologie aufbauen, die für zukünftige wissenschaftliche Studien dauerhaft genutzt werden kann. Mit meiner Beratung wurde ein Datenschutzkonzept erstellt, das Umfang, Zweck sowie Art und Weise der Verarbeitung der Patientendaten und die den verschiedenen beteiligten Stellen jeweils obliegenden Verantwortlichkeiten festlegt. Diese Festlegungen sind Grundlage für die Patienteninformationen.

Die KfH-Stiftung Präventivmedizin in Neu-Isenburg (http://www.kfh-stiftung-praeventivmedizin.de) wurde von dem gemeinnützigen Verein "Kuratorium für Dialyse und Nierentransplantation e.V." (KfH) mit dem Ziel gegründet, Studien zur Erforschung des chronischen Nierenversagens (CKD) zu unterstützen, an der in Deutschland bis zu sechs Millionen Menschen leiden. Darüber hinaus ist es Ziel der Stiftung, eine zentrale Sammlung klinischer Daten (sog. Kerndatensatz) chronisch niereninsuffizienter Patienten aufzubauen, auf die auch im Rahmen künftiger Studien zugegriffen werden kann. Aufgrund einer Anfrage habe ich die Stiftung bei der Ausgestaltung des Datenschutzkonzepts für die Erhebung, Speicherung und künftige Nutzung der zentralen Datensammlung beraten. Dabei waren insbesondere die folgenden Punkte klärungsbedürftig:

- Verantwortlichkeit für die zentrale Datenbank (u.a. Rechtmäßigkeit der Speicherung, Verfahren bei Widerruf, Datensicherheitsmaßnahmen, Inhalt der Verträge mit Dienstleistern)
- Pseudonymisierungsverfahren
- Inhalt des Kerndatensatzes
  Wird für die Pseudonymbildung ein sicheres Verfahren eingesetzt? Besteht durch den Umfang der gespeicherten Einzelangaben ein Reidentifizierungsrisiko der Patienten?
- Wer ist Eigentümer der Proben und entscheidet über deren Weitergabe?
- Verfahrensweise bei Anträgen von externen Forschern auf Nutzung der Datensammlung: Durch wen und auf welche Weise werden Forscher autorisiert, Daten und/oder Proben zu nutzen?
- Inhalt der Information und Einwilligung der Patienten
  Der Kerndatensatz wird im Rahmen einer Einzelstudie erhoben. Dabei muss auch die langfristige zentrale Speicherung des Kerndatensatzes einschließlich der verantwortlichen Stelle (Stiftung) für die Patienten vor ihrer Einwilligung transparent sein.

In mehreren Gesprächen mit Vertretern der Stiftung, von beteiligten Universitäten und Dienstleistern wurde eine Verständigung über die Einzelheiten des Datenschutzkonzepts erzielt. Wegen der sich überschneidenden Zuständigkeiten wurde das Datenschutzkonzept auch mit dem Regierungspräsidium Darmstadt, Dezernat Datenschutz, als zuständige Aufsichtsbehörde für den privaten Bereich, abgestimmt. Das Konzept beinhaltet insbesondere die folgenden Punkte:

4.6.5.1 Gemeinsamer Kerndatensatz

Im Rahmen jeder von der Stiftung geförderten Studie muss für jeden Studienteilnehmer ein gemeinsamer sog. Kerndatensatz (insbesondere Stammdaten der Patienten, Daten zum Krankheitsverlauf, Ergebnisse der klinischen Untersuchungen, Laborergebnisse, Lagerungsort von Biomaterialproben) erhoben werden. Dieser Kerndatensatz ist Bestandteil der konkreten Studie und wird zugleich in pseudonymisierter Form in die von der Stiftung aufgebaute zentrale Datensammlung aufgenommen.

Die zentrale Datensammlung wird berechtigten Wissenschaftlern für weitere Studien im nichtkommerziellen, medizinischen und gesundheitsökonomischen Bereich im erforderlichen Umfang zur Verfügung gestellt, damit sie bisherige Forschungsergebnisse nutzen und erweitern können. Berechtigte Wissenschaftler sind Wissenschaftler, denen der Zugriff auf Daten der zentralen Datensammlung nach Begutachtung eines Antrages durch den wissenschaftlichen Beirat und Beschluss der Aufsichtsgremien der KfH-Stiftung Präventivmedizin genehmigt wurde. Sollte ein Wissenschaftler auch Zugriff auf Proben von Patienten benötigen, so kann anhand der in der zentralen Datenbank gespeicherten Daten festgestellt werden, ob und ggf. wo Proben vorhanden sind. Die Proben werden dezentral gelagert und verwendet und über ihre Weitergabe entscheidet die dezentrale Studienleitung, nicht die Stiftung.
Geplant ist, den Kerndatensatz in der zentralen Datenbank über maximal 20 Jahre nach Ende der jeweiligen Studie zu speichern.

4.6.5.2 Pseudonymisierung des Kerndatensatzes

Das Pseudonymisierungskonzept orientiert sich in wesentlichen Punkten an dem von den Datenschutzbeauftragten des Bundes und der Länder konsentierten generischen Datenschutzkonzept der Telematikplattform der medizinischen Forschungsnetze (TMF, http://www. tmf-ev.de). Sofern ein Patient an mehreren Studien teilnimmt, erhält er für jede Studie ein anderes Pseudonym. Dies ergibt sich aus der Art und Weise, wie nach dem TMF-Modell Pseudonyme erstellt und Daten zwi-

schen Studienzentrale und Datenbank übertragen werden. Studienzentrale, Betreiber des Pseudonymisierungsdienstes und Betreiber der Datenbank sind voneinander unabhängige Stellen.

Die Schritte sind wie folgt:

1.
Die Zentrale einer Studie vergibt in einem ersten Schritt einmalig für einen Patienten eine PID, d.h., einen studienspezifischen Identifikator. Nur die zuständigen Mitarbeiter der Studie können der PID die identifizierenden Daten des Patienten zuordnen.

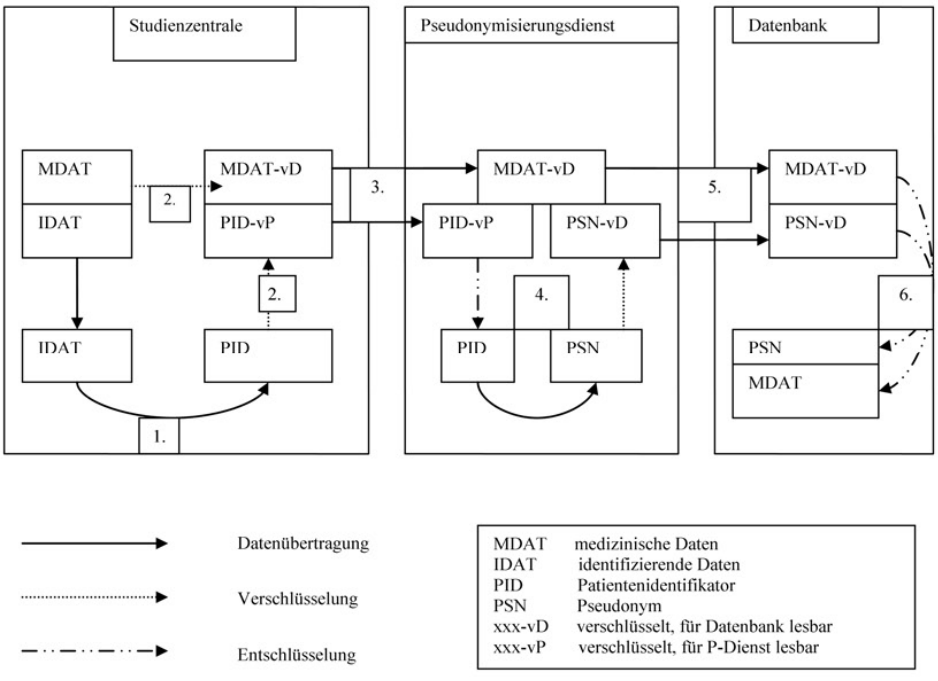
2.
Die Daten werden nach dem Prinzip des doppelten Umschlags übertragen. Dazu werden die medizinischen Daten ebenso wie die PID verschlüsselt. Die medizinischen Daten sind so verschlüsselt, dass nur der Betreiber der Datenbank sie entschlüsseln kann, während die PID vom Pseudonymisierungsdienst entschlüsselt werden kann.

3.
Beide Datenpakete werden an den Pseudonymisierungsdienst übertragen.

4.
Dort wird das Datenpaket mit der PID entschlüsselt. Aus der PID wird gemäß den Regeln, die zwischen Studienzentrale und Pseudonymisierungsdienst abgestimmt sind, das Pseudonym (PSN) generiert. Jetzt wird das PSN für den Betreiber der Datenbank verschlüsselt. Es liegen jetzt sowohl die medizinischen Daten als auch das PSN für den Betreiber der Datenbank verschlüsselt vor.

5.
Es werden die medizinischen Daten und das PSN in verschlüsselter Form übertragen.

6.
Der Betreiber der Datenbank entschlüsselt die medizinischen Daten und das PSN und speichert die Daten in der Datenbank.



Die PID wird durch die Studien unabhängig voneinander festgelegt. Oft handelt es sich um laufende Nummern. Ein Patient, der an mehreren Studien teilnehmen würde, erhält in der Regel verschiedene PIDs und damit auch verschiedene PSN. Das System erlaubt es auch, dass der Pseudonymisierungsdienst je Studie nach anderen Regeln das Pseudonym generiert.

Zweifache Pseudonymisierung

Eine zweifache Pseudonymisierung kommt zustande, wenn eine Studie Daten an die Kerndatensatz-Datenbank liefert, die bereits nach dem TMF-Modell arbeitet. Die entsprechenden Daten liegen bei der Studie in pseudonymisierter Form vor. In diesem Fall würde beim Pseudonymisierungsdienst keine PID, sondern bereits eine PSN angeliefert. Für das Verfahren ist es unerheblich, ob eine PID oder ein PSN übertragen wird; es wird nach den vorgegebenen Regeln ein Pseudonym gebildet. Es würde also von einem Pseudonym ein weiteres Pseudonym abgeleitet.

Der Pseudonymisierungsdienst wird im Auftrag der Stiftung von einem externen Dienstleister betrieben. Die Stiftung hat keinen Zugriff auf den Schlüssel zur Pseudonymbildung.

4.6.5.3 Patienteninformation und -einwilligung

Rechtsgrundlage für die Speicherung des Kerndatensatzes in der zentralen Datenbank ist die Einwilligungserklärung des Patienten. In die für die konkrete Studie notwendige Information und Einwilligung des Patienten wird ein separater Abschnitt zur Information und Einwilligung in die langfristige Speicherung eines pseudonymisierten Kerndatensatzes in der zentralen Datenbank der Stiftung einbezogen. Dabei ist es aus datenschutzrechtlicher Sicht wichtig, dass für die Patienten die unterschiedlichen Zwecke und Verantwortlichkeiten transparent werden, die einerseits für die Datenverarbeitung der konkreten Studie gelten und andererseits bei der Datenverarbeitung in der zentralen Datenbank. Da die Patientendaten in der zentralen Datenbank pseudonymisiert (und nicht anonymisiert) gespeichert werden, müssen die Patienten auch darüber informiert werden, unter welchen Voraussetzungen ihre Daten depseudonymisiert werden dürfen. Nach dem Konzept ist dies ausschließlich mit Einwilligung der Betroffenen zulässig. In gemeinsamen Gesprächen wurde der Wortlaut der Information und Einwilligung der Patienten bezüglich des Kerndatensatzes mit mir abgestimmt. Er soll künftig in allen Studien gleichlautend sein.

4.6.5.4 Rückverschlüsselung des Pseudonyms aus dem Kerndatensatz

Es gibt Fälle, in denen zu Zwecken der Qualitätssicherung ein Pseudonym aufgelöst werden muss oder in denen ein Forscher zu einem Patienten und dessen Arzt Kontakt aufnehmen will. Damit dies geschehen darf, müssen die Rahmenbedingungen für eine Depseudonymisierung festgelegt sein und die Technik muss es unterstützen.

Technisch betrachtet muss es eine Nachricht geben, bei der vom Betreiber der Kerndatenbank ein PSN verschlüsselt an den Pseudonymisierungsdienst übertragen wird. Dort wird das Pseudonym in die PID umgerechnet und die PID dann verschlüsselt an die Studie übertragen. Durch die Zentrale der Studie kann anhand der PID der Patient bestimmt werden. Wenn erforderlich kann es einen Datenteil geben, der verschlüsselt von der Datenbank zur Studienzentrale geht.

4.6.5.5 Löschung des Kerndatensatzes

Es ist zurzeit noch nicht endgültig geklärt, wie verfahren wird, wenn ein Patient die Teilnahme beendet und seine Daten in der Kerndatenbank gelöscht werden sollen. Es gibt den Wunsch, die Daten weiterhin anonymisiert vorzuhalten. Wenn die Daten hinreichend anonymisiert sind, bestehen dagegen keine Bedenken.

Falls eine vollständige Löschung der Daten stattfinden soll, muss es eine passende Nachricht geben. Dann würden auf dem unter Ziff. 4.6.5.2 beschriebenen Weg keine medizinischen Daten von der Studienzentrale an die Kerndatenbank übertragen, sondern eine Löschanweisung. Durch passende Sicherheitsvorkehrungen muss gewährleistet werden, dass nur authentische Löschanweisungen weiter bearbeitet werden. Wenn die Anweisung bestätigt ist, müssen die zu der PSN gespeicherten Daten gelöscht werden.

4.6.6 Zuweiserportale in Krankenhäusern

Viele Kliniken richten internetbasierte Zuweiserportale ein, über die die Kommunikation zwischen der Klinik und niedergelassenen Ärzten optimiert werden soll. Im Berichtszeitraum habe ich verschiedene Kliniken beraten, welche rechtlichen und technischen Aspekte zu berücksichtigen sind.

Im Gesundheitsbereich wird vielfach das Problem gesehen, dass die aktuellen, für die Behandlung notwendigen Patientendaten nicht zum richtigen Zeitpunkt am richtigen Ort vollständig zur Verfügung stehen. Insbesondere auch die Kommunikation zwischen verschiedenen an einer Behandlung beteiligten Ärzten bzw. Behandlungseinrichtungen wird als verbesserungsbedürftig angesehen. Einer der Ansätze hierfür ist die Einrichtung eines sog. Zuweiserportals in den Kliniken für die Kommunikation mit mit- oder nachbehandelnden Ärzten bzw. Behandlungseinrichtungen.

4.6.6.1 Was ist ein Zuweiserportal?

Der Begriff "Zuweiserportal" wird in der Praxis nicht immer einheitlich verwendet. Grundsätzlich sind zwei unterschiedliche Konstellationen zu unterscheiden:

- Der Aufbau einer einrichtungsübergreifenden Fallakte, d.h. die gemeinsame Nutzung einer Fallakte für die Dauer einer Behandlung durch die an dieser Behandlung beteiligten Behandlungseinrichtungen (z.B. Klinikum und Hausarzt und/oder Facharzt; zu den rechtlichen Anforderungen an einrichtungsübergreifenden Fallakten s. 37. Tätigkeitsbericht, Ziff. 4.7.1).
- Der Aufbau eines Zwischenspeichers für die Datenübertragung vom Klinikum an die anderen Behandler, d.h. eine zeitlich begrenzte Datenspeicherung in einem Zwischenspeicher bis zum Abruf.

Ganz überwiegend wird ein Zuweiserportal derzeit für eine Datenübertragung vom Klinikum an mit- oder weiterbehandelnde niedergelassene Ärzte aufgebaut. Teilweise ist dabei auch vorgesehen, dass die niedergelassenen Ärzte über das Einweiserportal ihre Patienten im Klinikum anmelden können.

4.6.6.2 Mögliche Ausgestaltungsformen

Je nach konkretem Zweck und Beteiligten können Zuweiserportale unterschiedlich ausgestaltet sein. Zwischen den Beteiligten muss die konkrete Ausgestaltung vereinbart werden. Dabei sind insbesondere auch die folgenden Fragen zu klären:

- Welcher Dokumententyp soll in den Zwischenspeicher eingestellt werden (z.B. Operationsbericht, Arztbriefe, Labordaten)?
- Erfolgt eine automatisierte Auswahl der im Zwischenspeicher gespeicherten Dokumente aus den im Krankenhauskommunikationssystem gespeicherten Dokumenten?
- Kann der behandelnde Arzt im Klinikum zusätzliche Dokumente für die Datenübertragung auswählen?
- Kann der behandelnde Arzt allgemein für die Datenübertragung vorgesehene Dokumente von der Datenübertragung im Einzelfall ausschließen?
- Ist die Übertragung bestimmter Dokumententypen technisch gesperrt?
- Wie lange bleiben Dokumente im Zwischenspeicher gespeichert? Ist die rechtzeitige Löschung der Daten im Speicher durch Löschroutinen sichergestellt?
- Sollen die Dokumente nur zur Einsicht oder auch zum Herunterladen für die externen Behandler zur Verfügung gestellt werden?

4.6.6.3 Rechte des Patienten

Die allgemeinen rechtlichen Voraussetzungen einer Übermittlung von Patientendaten vom Krankenhaus an externe mit- oder nachbehandelnde Ärzte bzw. Behandlungseinrichtungen sind in § 12 Abs. 2 Nr. 2 HKHG geregelt. Nach dieser Vorschrift ist eine Übermittlung zulässig, soweit dies erforderlich ist zur Durchführung einer Mit- oder Nachbehandlung und soweit der betroffene Patient nach Hinweis auf die beabsichtigte Übermittlung nichts anderes bestimmt hat. Diese Vorschrift gilt auch für die Übermittlung von Patientendaten über ein Zuweiserportal.

§ 12 Abs. 2 HKHG

(2) Die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses ohne die Einwilligung der oder des Betroffenen ist abweichend von den Vorschriften des Hessischen Datenschutzgesetzes nur zulässig, soweit dies erforderlich ist
….
2. zur Durchführung einer Mit- oder Nachbehandlung, soweit die Patientin oder der Patient nach Hinweis auf die beabsichtigte Übermittlung nichts anderes bestimmt hat;
….

Zwingend vorgeschrieben ist somit, dass jeder Patient vor einer Übermittlung personenbezogener Daten an mit- oder weiterbehandelnde Ärzte bzw. Behandlungseinrichtungen konkret zu informieren ist, d.h. insbesondere über den vorgesehenen Empfänger der Daten, ferner über Umfang und Zweck der Übermittlung, und dass der Patient das Recht hat, hinsichtlich der Übermittlung anders zu entscheiden.

Eine schriftliche Information und Einwilligung des Patienten ist grundsätzlich vom Hessischen Krankenhausgesetz nicht zwingend vorgeschrieben. Im Interesse aller Beteiligten und zur Vermeidung von späteren Kontroversen kann allerdings eine schriftliche Festlegung hilfreich sein. So kann z.B. dem Patienten im Aufnahmeformular die Möglichkeit gegeben werden, die Ärzte anzugeben, die einen Entlassungsbericht des Krankenhauses erhalten sollen. Erfolgt im Krankenhaus lediglich ein Gespräch mit dem Patienten über die beabsichtigten Datenübermittlungen, so sollte zumindest dies Gespräch in der Krankenakte dokumentiert sein.

Wenn beabsichtigt wird, Datenübermittlungen an mit- oder nachbehandelnde Ärzte bzw. Behandlungseinrichtungen über ein Zuweiserportal vorzunehmen, ist bei der Entscheidung über die Verfahrensweise zu berücksichtigen, dass über ein Zuweiserportal in der Regel ein umfangreicherer Datenaustausch stattfindet und die Modalitäten der Übermittlung für den Patienten zunächst schwerer nachvollziehbar sind. Bei der Errichtung von Zuweiserportalen ist daher in der Regel eine schriftliche Information des Patienten notwendig, damit das Verfahren für den Patienten transparent ist und auch das Krankenhauspersonal entlastet wird. Dabei muss selbstverständlich nicht jedes Dokument konkret erwähnt werden, aber der konkrete Zweck und der allgemeine Umfang der Datenübertragungen (z.B. Art der Dokumente) müssen für den Patienten transparent sein. Zur Unterstützung der Krankenhäuser habe ich eine Musterinformation entworfen und auf meiner Homepage unter http://www.datenschutz.hessen.de/dg004.htm veröffentlicht. Der Musterentwurf kann an die jeweilige Situation im Krankenhaus angepasst werden.

Das Einholen einer schriftlichen Einwilligung des Patienten in die Einrichtung eines Zuweiserportals ist zu empfehlen, damit die Einhaltung der Vorschrift des § 12 Abs. 2 Nr. 2 HKHG jederzeit nachvollziehbar ist.

In einem Krankenhaus enthielt der übliche Aufnahmevertrag vorübergehend folgenden Passus:

"Der Patient ist damit einverstanden, dass das … zur Verbesserung einer qualifizierten (Weiter-)Behandlung mit einigen einweisenden Ärzten und Krankenhäusern elektronisch kommuniziert. Dazu gehört auch, dass der behandelnde Vertragsarzt Einblick in Termine, Arztbrief und medizinische Dokumentationen nehmen kann. Der Patient entbindet das … insofern von der ärztlichen Schweigepflicht.
Das … wird nicht mit den einweisenden Ärzten elektronisch kommunizieren, wenn der Patient damit nicht einverstanden ist. Dies kann er durch handschriftliche Streichung dieses Absatzes kenntlich machen."

Eine solche pauschale Verfahrensweise entspricht nicht den datenschutzrechtlichen Anforderungen. Für den einzelnen Patienten ist nicht nachvollziehbar, ob und ggf. in welchem Umfang seine personenbezogenen Krankheitsdaten an Dritte übermittelt werden.

4.6.6.4 Technische Datensicherheitsmaßnahmen

In meinem 37. Tätigkeitsbericht (Ziff. 4.7.2) hatte ich von einem Projekt berichtet, bei dem Behandlungsinformationen in Form von Arztbriefen zwischen Krankenhäusern und Ärzten ausgetauscht werden. Die Dokumente werden vom Sender gezielt für den einzelnen Empfänger verschlüsselt, so dass nur dieser sie lesen kann. Sie werden dann auf einem Server gespeichert und stehen für den Empfänger bereit. Nachdem sich der Empfänger am Server angemeldet hat, kann er seine Dokumente herunterladen. Nur er ist in der Lage, sie auf seinem Rechner zu entschlüsseln. Während der gesamten Übertragung bleiben die Daten verschlüsselt und können nicht von Unbefugten zur Kenntnis genommen werden.

Dieser Ansatz wird bei den Zuweiserportalen aufgeweicht. Der Server, auf dem die Dokumente zwischengespeichert werden, wird vom Krankenhaus betrieben. Er befindet sich aber nicht mehr im besonders gesicherten inneren Kommunikationsnetz, sondern in einem vorgelagerten Netzsegment, einer sog. "demilitarisierten Zone" (DMZ). Über das Internet können die berechtigten Ärzte auf den Server zugreifen. Die eigentliche Datenübertragung zwischen dem Rechner beim Arzt und dem Server erfolgt verschlüsselt. Der entscheidende Unterschied zu dem o.g. Konzept besteht darin, dass die Dokumente unverschlüsselt gespeichert werden. Damit ein unbefugter Arzt, der ein Zugriffsrecht für den Server besitzt, sie nicht zur Kenntnis nehmen kann, müssen auch die Zugriffsrechte auf die Dokumente korrekt vergeben sein. Diese Rahmenbedingungen führen zu Konsequenzen, wenn angemessene technische Datenschutzmaßnahmen erreicht werden sollen.

- Die DMZ muss durch Firewalls und andere Maßnahmen gegen unbefugte Zugriffe geschützt werden; sie muss ein dem inneren Netz vergleichbares Sicherheitsniveau erreichen. Die Abwehr von Angriffen durch unzulässige Dateneingaben bei erlaubten Programmaufrufen muss berücksichtigt sein (Web-Application Firewalls, Application-Level-Gateways usw.).

- Bei der Softwareentwicklung muss die Datensicherheit Designziel sein.
  Insbesondere müssen fehlerhafte Dateneingaben erkannt und abgewiesen sowie Zugriffseinschränkungen korrekt umgesetzt werden. Dies ergänzt die Sicherheitsmaßnahmen der DMZ.

- Der Benutzer, der berechtigt ist, auf den Server zuzugreifen, muss sicher identifiziert werden und sich bei der Anmeldung am Server sicher authentisieren. Daraus resultieren zwei Maßnahmenkataloge.

  - Erstens müssen durch organisatorische Maßnahmen Interessenten zweifelsfrei als Ärzte identifiziert werden. Wenn sie am Zuweiserportal teilnehmen sollen, muss ihnen eine Benutzerkennung und ein Authentisierungsmittel so zugeschickt werden, dass ein Unbefugter es nicht abfangen und nutzen kann. Diese Vorgänge müssen dokumentiert werden.

  - Zweitens muss die Authentisierung, d.h. bei der Anmeldung am Server der Nachweis, dass der Arzt am Rechner sitzt, sicher ausgestaltet sein. Eine Anmeldung am Server mit Benutzerkennung und Passwort ist allein nicht ausreichend. Weitere Maßnahmen sind Zertifikate, die auf dem Rechner des Arztes installiert werden und vom Server geprüft werden können. Unbedingt empfehlenswert ist ein auf Besitz und Wissen basierendes Authentisierungsverfahren. Etabliert sind sog. Token, die Einmalpasswörter generieren.

    Sobald die Telematikinfrastruktur vorhanden ist, steht mit dem Heilberufeausweis (HBA) eine Technik zur Verfügung, die diese Anforderungen weitgehend umsetzen würde. Es bleiben aber organisatorische Maßnahmen wie die Zulassung zur Teilnahme und die Dokumentation der Abläufe umzusetzen.

- Die Datenübertragungen müssen verschlüsselt erfolgen und dem Stand der Technik entsprechen. Dies betrifft u.a. die eingesetzten Algorithmen und die Schlüssellängen.

- Die Vergabe der Zugriffsrechte von Ärzten auf die Dokumente eines Patienten muss dokumentiert werden.

- Die Zugriffe auf den Server und die Dokumente müssen nachvollziehbar sein. Dies erfordert eine entsprechende Protokollierung.

- Zusätzlich zu den Maßnahmen auf Seiten des Krankenhauses muss auch der Arzt in seiner Praxis sicherstellen, dass Unbefugte keinen Zugriff auf die Dokumente erhalten. Außerdem muss er die Kennung, Zertifikate und Token sorgfältig verwahren, damit Unbefugte keinen Zugang dazu erhalten.

4.6.7 Prüfung der DMP-Datenstelle

Im Berichtsjahr hat einer meiner Mitarbeiter zusammen mit dem Datenschutzbeauftragten der Arbeitsgemeinschaft DMP Hessen (ARGE Hessen) die von der Firma systemform MediaCard betriebene Datenstelle in Hallstadt bei Bamberg sowie den Hauptsitz von systemform in Prien aufgesucht. Hinsichtlich der Gebäudesicherheit sowie des administrativen und organisatorischen Datenschutzes wurden keine gravierenden Mängel festgestellt.

4.6.7.1 Ausgangssituation

Bereits im 34. Tätigkeitsbericht habe ich mich mit der Verarbeitung personenbezogener, medizinischer Daten im Rahmen sog. Disease-Management-Programme (DMP) befasst (34. Tätigkeitsbericht, Ziff. 5.8.4). Seinerzeit ging es dabei um die unzulässige Verarbeitung dieser Daten durch die DMP-Datenstelle in Hallstadt bei Bamberg in einem Rechenzentrum in Vietnam. Die Aufarbeitung der organisatorischen, administrativen und technischen Unzulänglichkeiten in der sog. "Datenstelle" sowie die Umsetzung erforderlicher Maßnahmen zu deren Beseitigung wurde von meiner Dienststelle seinerzeit angestoßen und in den folgenden Jahren von den Datenschutzbeauftragten der Arbeitsgemeinschaften DMP Hessen und Sachsen intensiv begleitet.

4.6.7.2 Erhebungsstelle in Hallstadt

Anlass der Prüfung war die ausgelaufene Zertifizierung der DMP-Datenstelle. Die Zertifizierung des Betriebs erfolgte im Jahre 2006 durch die TÜV Informationstechnik GmbH in Essen. Eine erneute Zertifizierung wurde durch die Arbeitsgemeinschaften DMP zwar nicht mehr gefordert. Jedoch war der aktuelle organisatorisch/administrative Ist-Zustand der Datenstelle ein Thema, das im Rahmen einer Überprüfung durch die TÜV-Informationstechnik GmbH behandelt wurde.

Die Prüfungsinhalte basierten auf diesem Prüfbericht aus dem Jahr 2008, in dem die Umsetzung der Auflagen aus dem Jahr 2006 bilanziert wurden und weitere Empfehlungen zum Datenschutz und der Datensicherheit formuliert waren.

Nach wie vor verarbeitet die Datenstelle eingehende DMP-Bögen, in denen medizinische Daten des Patienten zu einem bestimmten Krankheitsbild und dessen Behandlung dokumentiert werden. Diese Daten werden elektronisch aufbereitet und verschiedenen Stellen, wie z.B. dem Arzt oder der Krankenkasse, zur Verfügung gestellt. Mittlerweile werden die Daten vom Arzt auch in elektronischer Form und verschlüsselt übermittelt, so dass verschiedene Schritte zur Bearbeitung der Dokumente erforderlich sind. Das Volumen der Datenverarbeitung hat sich hinsichtlich der Krankheitsbilder ausgeweitet. So wurden zunächst nur die Daten von Diabetes-mellitus-Patienten verarbeitet. Mittlerweile sind Brustkrebs, koronare Herzerkrankungen, Asthma sowie COPD (eine spezielle Art von Lungenkrankheit) hinzugekommen.

4.6.7.3 Umsetzung der im TÜV-Prüfbericht geforderten Maßnahmen

Die im TÜV-Bericht aus dem Jahre 2006 geforderten Maßnahmen wurden durch den Datenstellen-Betreiber alle erfüllt. Empfehlungen aus dem TÜV-Bericht wurden jedoch zum Teil nicht umgesetzt. Einige dieser Maßnahmen werden exemplarisch nachfolgend dargestellt.

4.6.7.3.1 Zutritte zum Serverraum

Der Zutritt zum Serverraum ist nur mit einer Zutritt-Chipkarte möglich. Zusätzlich erfolgt eine Protokollierung des Zutritts. Eine Öffnung des Raumes per Schlüssel löst einen Alarm aus.

4.6.7.3.2 Regelmäßige Inventur der ausgegebenen Schlüssel

Die Schlüsselvergabe wird in regelmäßigen Abständen überprüft. Nicht ausgegebene Exemplare werden in einem Tresor aufbewahrt.

4.6.7.3.3 Einbeziehung der Notausgänge in das Alarmsystem

Die Notausgänge sind in das Alarmsystem eingebunden. Die akustische Warnung wurde optimiert. Die Einbeziehung des Archivraums und eine Schaltung zur Teamleitung Sachbearbeitung ist realisiert worden.

4.6.7.3.4 Besucherbuch/Verpflichtung auf das Datengeheimnis

Auch diese Auflagen wurden umgesetzt. Jeder Besucher der Datenstelle muss sich in ein Besucherbuch eintragen, in dem die Zeitpunkte des Kommens und Gehens hinterlegt werden.

4.6.7.3.5 Aufbewahrung der Sicherungsbänder

Der Empfehlung, für Hallstadt einen Tresor zu beschaffen und in einem anderen Brandabschnitt zu montieren, wurde aus Kostengründen nicht gefolgt. Im Gegenteil: die Bänder mit Sicherungen für sieben Arbeitstage wurden im Serverraum selbst gelagert. Die unmittelbar geäußerte Kritik wurde von dem Datenschutzbeauftragten der Datenstelle aufgegriffen. Künftig werden die Bänder in einem separaten Raum eines anderen Gebäudeteils verwahrt.

4.6.7.4 Verarbeitungsstelle in Prien

Im Hauptsitz in Prien erfolgt die Druckverarbeitung und Versendung von Arztbriefen und Schreiben an die Krankenkassen durch die Firma systemform MediaCard. Die Daten hierfür werden elektronisch von Hallstadt nach Prien übermittelt. Monatlich etwa 100.000 Datensätze werden hier verarbeitet. Schwerpunkt der Prüfung in Prien waren Aspekte der Gebäudesicherung, der Zugangs- und Zugriffskontrolle sowie das Trennungsgebot.

4.6.7.4.1 Gebäudesicherheit und Zutrittskontrolle

Im Zusammenhang mit einer Gebäudeerweiterung bzw. dem Umbau der Geschäftsräume in den Jahren 2007 und 2008 wurden die Sicherheitsstandards wesentlich erhöht. Der Neu- bzw. Anbau wurde in der sog. "Widerstandsklasse 4" errichtet. Wände, Fenster und Türen entsprechen besonderen Sicherheitsbestimmungen. Das Gebäude ist zudem im Innen- und Außenbereich videoüberwacht, mit Bewegungsmeldern versehen und mit Lichtstrahlern (Außenbereich) ausgestattet, die sich im Alarmfall einschalten. Hinzu kommt ein "doppelter Zaun", der die Annäherung an das Gebäude erschwert. Der Haupteingang sowie der Empfangsbereich sind ebenfalls per Kamera überwacht. Hinzu kommen die Zugänge zum Produktionsbereich sowie den Übergängen zu dem Bereich des Schwesterunternehmens "systemform Datenbelege". Der Zutritt zum Sicherheitsbereich erfolgt durch ein kartengesteuertes Zutrittssystem sowie eine Sicherheitsschleuse. Ein solches Sicherheitssystem ist auch für die Anlieferung von Material sowie den Versand der Briefe realisiert.

Besucher müssen sich legitimieren, in ein Besucherbuch eintragen und werden in Begleitung durch das Haus geführt.

4.6.7.4.2 Zugriff auf die DMP-Daten

Die Arbeitsvorbereitung erstellt die Druckaufträge, die inkl. der Kuvertierung in einem besonderen Teil des Gebäudes und von den hierfür vorgesehenen Mitarbeitern abgearbeitet werden. Um die einzelnen Verarbeitungsschritte zu dokumentieren, wird für jeden Auftrag ein Arbeitsblatt angelegt. Sind die Produktionsschritte beendet, geht das Blatt an die Arbeitsvorbereitung zurück. Im Anschluss werden die aus Hallstadt übermittelten Datenbestände gelöscht. Eingang und Löschung der Daten werden protokolliert. Für diesen Verarbeitungsschritt existiert allerdings keine klare, festgelegte Regelung. Derzeit werden die Daten 14 Tage nach dem Postversand gelöscht. Den zeitlichen Puffer hat man für evtl. Rückfragen oder Unzulänglichkeiten der Postzustellung gewählt, um ggf. Briefe erneut zu versenden. Von Seiten der Auftraggeber gibt es hierzu keine expliziten Anweisungen. Dieser Punkt muss aufgegriffen und zumindest von der Erforderlichkeit der Datenspeicherung abhängig gemacht werden.

4.6.7.4.3 Papiervernichtung

Soweit personenbezogene Daten vernichtet werden müssen, bedient sich systemform eines externen, zertifizierten Dienstleisters. Auf die Anforderungen zur Sicherstellung einer datenschutzgerechten Vernichtung hinsichtlich der einzuhaltenden Sicherheitsstufe bei der Zerkleinerung haben die Datenschutzbeauftragten hingewiesen.

4.6.7.5 Fazit

Die datenschutzkonforme Verarbeitung von DMP-Daten ist grundsätzlich sichergestellt. Allerdings muss einschränkend bemerkt werden, dass sich die Prüfung vornehmlich auf administrative und organisatorische Aspekte sowie (in Prien) die Gebäudesicherheit bezog.

4.6.8 Auskunftsanspruch gegenüber dem Gesundheitsamt

Ein Betroffener hat sich in meiner Dienststelle darüber beschwert, dass ein Gesundheitsamt für die von ihm beantragte Auskunft bzw. Akteneinsicht Gebühren in Höhe von 13 Euro je angefangener Viertelstunde forderte. Nach meiner Intervention über die Datenschutzbeauftragte der Kreisverwaltung konnte für den Beschwerdeführer die kostenfreie Auskunftserteilung bzw. Akteneinsicht gewährleistet werden.

4.6.8.1 Gebühren für Auskunft und Einsicht?

Das Recht auf Auskunft und Akteneinsicht nach § 18 HDSG gilt auch für personenbezogene Daten, die im Gesundheitsamt gespeichert werden. Die Erhebung und Speicherung personenbezogener Daten durch die Gesundheitsverwaltung ist umfassend.

Schuleingangsuntersuchungen, amtsärztliche Untersuchungen oder sozialpsychiatrische Stellungnahmen: nur wenige andere staatliche Stellen erheben und verarbeiten derart umfangreich personenbezogene Daten. So ist es leicht verständlich, dass Personen, die außerhalb der ohnehin gesetzlich vorgeschriebenen Kontakte mit dem Gesundheitsamt in Berührung kommen, sich für die Inhalte der zu ihnen geführten Akten interessieren.

Die Bitte um Akteneinsicht wurde jedoch für den Petenten zunächst zu einem Spießrutenlauf: das Gesundheitsamt forderte für die Einsichtnahme eine Gebühr von 13 Euro je angefangener Viertelstunde. Dies akzeptierte der Antragsteller nicht und wandte sich mit seinem Problem an meine Dienststelle.

4.6.8.2 Rechtliche Grundlagen für Auskunft und Akteneinsicht

Die Rechtsgrundlage für das Tätigwerden der Gesundheitsämter bildet das Hessische Gesetz über den öffentlichen Gesundheitsdienst (HGöGD, GVBl. I S. 659 vom 28. September 2007). Nach § 18 Abs. 4 HGöGD gelten die datenschutzrechtlichen Regelungen des HDSG. Hinsichtlich der Auskunft und der Einsicht ist dann § 18 HDSG einschlägig.

§ 18 Abs. 3 HDSG

"Daten verarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben dem Betroffenen auf Antrag gebührenfrei Auskunft zu erteilen.

§ 18 Abs. 5 HDSG

Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen.

Der Betroffene hat also nach § 18 Abs. 3 HDSG das Recht, gebührenfrei Auskunft über die zu seiner Person gespeicherten Daten zu erhalten. Die Auskunftspflicht der speichernden Stelle erstreckt sich dabei sowohl auf die Herkunft der Daten als auch die Empfänger unmittelbarer Daten.
Hinsichtlich der beim Gesundheitsamt geführten Akten ist Abs. 5 HDSG einschlägig, wonach dem Betroffenen ein Einsichtsrecht zusteht. Dabei ist die Behörde verpflichtet, alle Akten vorzulegen, die zu seiner Person geführt werden. Im Zusammenhang mit der Akteneinsicht ist auch die Fertigung von Kopien zulässig. Hierfür hat der Einsichtnehmer allerdings die übliche Kostenerstattung zu tragen.

4.6.8.3 Unkomplizierte Lösung des Problems

Im konkreten Fall konnte dem Beschwerdeführer schnell geholfen werden. Die Einschaltung der Datenschutzbeauftragten des Landkreises und deren Kontakt zum Gesundheitsamt führte dazu, dass man dort schnell den Irrtum erkannte, dem die Gebührenforderung zugrunde lag. Das Gesundheitsamt revidierte seine Auskunft und vereinbarte einen Termin, den der Beschwerdeführer im weiteren Verlauf auch wahrnahm.

4.7 Sozialwesen

4.7.1 Zusammenarbeit von SGB-II-(Hartz-IV-)Behörden mit Gesundheitsämtern

Die Gewährung oder Verlängerung von Sozialleistungen setzt Mitwirkungspflichten der Betroffenen voraus, wie sie die §§ 60 ff. SGB I vorsehen. Allerdings müssen die bei der Datenverarbeitung mitwirkenden öffentlichen Stellen den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit Rechnung tragen.

Ein Empfänger von Arbeitslosengeld II hatte sich über den Inhalt eines Gutachtens beschwert, welches vom Gesundheitsamt eines Landkreises im Auftrag einer SGB-II-Stelle (ARGE) erstellt und übermittelt wurde und in dem Fragen zur Arbeitsfähigkeit des Betroffenen beantwortet werden sollten. Der zuständige Arzt nutzte für die Erstellung des Gutachtens nicht das hierfür vorgesehene Formular der ARGE, sondern schrieb seine Feststellungen in einem formlosen Papier nieder. Dabei traf er u.a. auch Aussagen zur Person des Petenten bzw. seinem familiären Umfeld, welche für die eigentliche Fragestellung nicht von Bedeutung waren. So enthielt das sozialmedizinische Gutachten Angaben zur landsmannschaftlichen Herkunft der Eltern, den Geschwistern sowie Hobbys des Betroffenen. In der Weitergabe dieser Daten an die Arbeitsverwaltung sah der Beschwerdeführer eine Missachtung seines Rechts auf informationelle Selbstbestimmung und stellte die Frage nach der Erforderlichkeit für die Bewertung seiner Arbeitsfähigkeit.

Die Einschaltung des Gesundheitsamtes durch die ARGE war rechtmäßig. Denn zur Prüfung der Arbeitsfähigkeit kann der Sozialleistungsträger vom Leistungsempfänger verlangen, sich ärztlichen und psychologischen Untersuchungen zu unterziehen, um eine sachgerechte Entscheidung zu treffen (§ 62 SGB I).

§ 62 SGB I

Wer Sozialleistungen beantragt oder erhält, soll sich auf Verlangen des zuständigen Leistungsträgers ärztlichen und psychologischen Untersuchungsmaßnahmen unterziehen, soweit diese für die Entscheidung über die Leistung erforderlich sind.

Der Formularvordruck, der regelmäßig durch die Behörde zur Feststellung der Arbeitsfähigkeit genutzt wird, und damit die Datenerhebung als solche, waren nicht zu beanstanden. Problematisch war im konkreten Beschwerdefall die Erstellung eines "formlosen" Gutachtens durch den Amtsarzt, welches inhaltlich über das hinausging, was die ARGE für eine sachgerechte Entscheidung benötigte. Angaben über die landsmannschaftliche Herkunft der Eltern oder das familiäre Umfeld bzw. Angaben zur Kindheit sind Informationen, die die Arbeitsverwaltung nicht benötigt, um die Arbeitsfähigkeit des Betroffenen einschätzen zu können. Dem steht nicht entgegen, dass besagte SGB-II-Stelle ihr Interesse betonte, möglichst konkrete Angaben zu erhalten, unter welchen Umständen der Leistungsempfänger einsetzbar ist, um die Betroffenen möglichst schnell und dauerhaft wieder in den Prozess der Erwerbstätigkeit eingliedern zu können. Dies impliziert konkrete Angaben z.B. über Stärken und Schwächen des Betroffenen hinsichtlich möglicher Arbeitsgebiete. Diese könnten unter der Rubrik "Sozialmedizinische Empfehlungen" in dem Formular eingetragen werden, so dass die Verwendung eines "formlosen" Gutachtens grundsätzlich obsolet ist.

Sowohl die Arbeitsverwaltung als auch das Gesundheitsamt haben meine Position, die ich in einem gemeinsamen Gespräch zum Ausdruck gebracht habe, akzeptiert.

4.7.2 Auskunftsanspruch von Berufsgenossenschaften

Berufsgenossenschaften haben gegenüber Unternehmen Auskunftsansprüche, um mögliche Regressansprüche geltend machen zu können.

Eine Tierklinik hat angefragt, ob sie der für sie zuständigen Berufsgenossenschaft (einem Träger der gesetzlichen Unfallversicherung) Auskunft über Tierhalter geben müsse. Hintergrund des Auskunftsverlangens war, dass zwei Mitarbeiter der Tierklinik durch zur Behandlung in der Tierklinik sich befindende Tiere verletzt worden waren. Diese Verletzungen wurden der Berufsgenossenschaft zwecks unfallversicherungsrechtlicher Abwicklung gemeldet. Daraufhin erbat die Berufsgenossenschaft von der Tierklinik Auskunft über Name und Anschrift der entsprechenden Tierhalter. Die Tierklinik befürchtete allerdings, mit einer solchen Auskunft ihre Kunden zu verärgern, und bat mich deshalb um datenschutzrechtliche Bewertung.

Ausgangspunkt der rechtlichen Würdigung ist § 116 SGB X, der Ansprüche des sozialrechtlichen Leistungsträgers gegen Schadensersatzpflichtige betrifft. Bei dieser Vorschrift geht es darum, dass die Versicherung bei Dritten Regress nehmen kann, die sich etwa nach Bürgerlichem Recht gegenüber den Versicherten schadensersatzpflichtig gemacht haben. Im konkreten Fall kommt insbesondere die Tierhalterhaftung nach §§ 833 BGB infrage.

§ 833 BGB

Wird durch ein Tier ein Mensch getötet oder die Körper oder die Gesundheit eines Menschen verletzt …, so ist derjenige, welcher das Tier hält, verpflichtet, dem Verletzten den daraus entstehenden Schaden zu ersetzen.

Einen derartigen Schadensersatzanspruch der verletzten Mitarbeiter der Tierklinik nach § 833 BGB könnte der Unfallversicherungsträger auf der Grundlage von § 116 SGB X gegenüber den Tierhaltern geltend machen. Rechtlich handelt es sich bei § 116 SGB X um einen sog. gesetzlichen Forderungsübergang.

§ 116 Abs. 1 SGB X

Ein auf anderen gesetzlichen Vorschriften beruhender Anspruch auf Ersatz eines Schadens geht auf den Versicherungsträger über, soweit dieser aufgrund des Schadensereignisses Sozialleistungen zu erbringen hat, die der Behebung eines Schadens der gleichen Art dienen und sich auf denselben Zeitraum wie der vom Schädiger zu leistende Schadensersatz beziehen.

Damit die Versicherungsträger § 116 SGB X realisieren können, sieht § 192 SGB VII für den Bereich der gesetzlichen Unfallversicherung dementsprechende Mitteilungs- und Auskunftspflichten der Unternehmen vor. Die Unternehmen werden nämlich durch diese Vorschrift ausdrücklich angehalten, die Unfallversicherungsträger bei der Erfüllung ihrer gesetzlichen Aufgaben zu unterstützen (Abs. 3).

§ 192 Abs. 3 SGB VII

Die Unternehmen haben ferner auf Verlangen des zuständigen Unfallversicherungsträgers die Auskünfte zu geben, die zur Erfüllung der gesetzlichen Aufgaben des Unfallversicherungsträgers (§ 199) erforderlich sind.

Die gesetzlichen Aufgaben der Unfallversicherung sind in § 199 SGB VII explizit beschrieben; hierzu gehört gerade auch das Geltendmachen von Erstattungs- und Ersatzansprüchen.

§ 199 SGB VII Abs. 1. S. 2

Ihre (der Unfallversicherungsträger) Aufgaben sind:
…
4. Die Durchführung von Erstattungs- und Ersatzansprüchen

Wie es auch sonst für das Datenschutzrecht, insbesondere für das Sozialdatenschutzrecht prägend ist (vgl. § 67a SGB X), dürfen Unfallversicherungsträger Daten dann erheben, wenn dies für ihre Aufgabenerfüllung notwendig ist, § 199 SGB VII; etwa um im vorliegenden Fall den Anspruch gemäß §§ 116 SGB X, 833 BGB durchzusetzen.

§ 199 Abs. 1 Satz 1 SGB VII

Die Unfallversicherungsträger dürfen Sozialdaten erheben, soweit dies zur Erfüllung ihrer gesetzlich vorgeschriebenen oder zugelassenen Aufgaben erforderlich ist.

Vor diesem rechtlichen Hintergrund habe ich der Tierklinik erläutert, dass das Auskunftsverlangen der Berufsgenossenschaft betreffend die Tierhalter datenschutzrechtlich nicht zu monieren ist.

4.7.3 Datenverarbeitung bei der Anmeldung in Kindertageseinrichtungen

In Kommunen kommt es häufig vor, dass Eltern ihre Kinder gleichzeitig in mehreren Kindertageseinrichtungen anmelden. Dadurch wird fehlerhaft ein höherer Bedarf an Plätzen in Kindertageseinrichtungen signalisiert, als es tatsächlich der Fall ist.
Um diesem Problem der Mehrfachanmeldungen von Kindern in Kindertageseinrichtungen zu begegnen, ist es datenschutzrechtlich zulässig, dass Kindertageseinrichtungen die Anmeldungen miteinander abgleichen, um den realen Bedarf bestimmen zu können.

Aufgrund einer Eingabe eines Elternvereins habe ich für die Stadt Frankfurt ein Verfahren begleitet, das die Organisation der Aufnahme von Kindern in Kindertageseinrichtungen unterstützt, insbesondere das Problem der Mehrfachanmeldungen behandelt.

Um Mehrfachmeldungen abgleichen zu können, werden von den Kindertageseinrichtungen in Frankfurt jeweils stadtteilbezogen einmal jährlich die Namen und Geburtstage der angemeldeten Kinder miteinander abgeglichen. Dieser Abgleich findet auf sogenannten Planungsforen statt, zu denen die Leitungen der Kindertageseinrichtungen Namenslisten der angemeldeten Kinder mitbringen.

Durch die damit verbundene Transparenz betreffend die Anmeldungen soll unterstützt werden, dass der in §§ 22 ff. SGB VIII (Kinder- und Jugendhilfe) normierte Auftrag, Kinder in Tageseinrichtungen zu fördern, möglichst bei allen in Tageseinrichtungen angemeldeten Kindern realisiert werden kann.

§ 24 SGB VIII regelt den Anspruch auf Förderung in Tageseinrichtungen im Einzelnen. Anhand von fachlichen Kriterien (z.B. Wohnungsnähe, Arbeitsplatznähe) wird entschieden, welches Kind in welche Kindertageseinrichtung aufgenommen wird.

Die für die Ausführung des SGB VIII notwendige Datenverarbeitung wird durch die speziellen kinder- und jugendhilferechtlichen Vorschriften, §§ 61 ff. SGB VIII, gedeckt. Der spezielle Sozialdatenschutz nach dem SGB VIII gilt nämlich nicht nur für die Träger der öffentlichen Jugendhilfe (hier: die Stadt Frankfurt), sondern auch dann, wenn Träger der öffentlichen Jugendhilfe Einrichtungen von Trägern der freien Jugendhilfe in Anspruch nehmen (§ 61 Abs. 3 SGB VIII). In diesem Fall soll für die freie Jugendhilfe der gleiche Datenschutz wie für die öffentliche Jugendhilfe maßgebend sein.

§ 61 Abs. 3 SGB VIII

Werden Einrichtungen und Dienste der Träger der freien Jugendhilfe in Anspruch genommen, so ist sicherzustellen, dass der Schutz der personenbezogenen Daten bei der Erhebung und Verwendung in entsprechender Weise gewährleistet ist.

Allerdings stellte sich die Frage, ob die Eltern der angemeldeten Kinder einem auf die Mehrfachanmeldungen zielendem Abgleich widersprechen können.

Ein spezielles Widerspruchsrecht der Eltern sehen die §§ 61 ff. SGB VIII nicht vor, so dass auf das generelle Sozialdatenschutzrecht, auf das § 61 Abs. 1 SGB VIII verweist, rekurriert werden muss.

§ 76 SGB X räumt ein Widerspruchsrecht indes nur ein, soweit es um die Übermittlung besonders schutzwürdiger Sozialdaten geht. Bei Namen und Geburtstag eines zu einer Tageseinrichtung angemeldeten Kindes ist das allerdings nicht der Fall.

Auch das in (§ 84 Abs. 1a SGB X i.V.m.) § 20 Abs. 5 BDSG verankerte Recht zum Widerspruch ist mit Blick auf den Abgleich der Mehrfachanmeldungen nicht betroffen, da bei diesem Abgleich die Daten, anders als besagte Regelung voraussetzt, weder automatisiert noch in nicht automatisierten Dateien weiterverarbeitet werden. Vielmehr findet nach dem Abgleich eine Speicherung nicht statt. Darauf wird in dem Anmeldeformular auch ausdrücklich hingewiesen.

§ 20 Abs. 5 BDSG

Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an der Erhebung, Verarbeitung oder Nutzung überwiegt…

Neben den Widerspruchsrechten, die das Sozialdatenschutzrecht kennt, gibt es ein Widerspruchsrecht gemäß § 7 Abs. 5 HDSG. Diese Vorschrift umfasst auch nicht automatisierte Datenverarbeitung. Sie kann jedoch auch nicht zum Zuge kommen, weil es bei besagtem Abgleich der Mehrfachanmeldungen nicht um Datenverarbeitung auf der Grundlage des HDSG, sondern eben um eine auf das SGB VIII gestützte Datenverarbeitung geht.

Obwohl sich nach alledem ein gesetzliches Widerspruchsrecht mit Blick auf den Abgleich von Mehrfachanmeldungen nicht ergibt, hat der Datenschutzbeauftragte der Stadt Frankfurt mit meiner Unterstützung vorgeschlagen, zur Stärkung des informationellen Selbstbestimmungsrechts Eltern aus persönlichen Gründen in begründeten Einzelfällen ein Widerspruchsrecht gegen den Abgleich einzuräumen und die Eltern im Anmeldeformular darauf hinzuweisen. Diesem Vorschlag ist die Stadt Frankfurt erfreulicherweise gefolgt und hat das Anmeldeformular dementsprechend gestaltet. Ende 2010 werde ich mich bei der Stadt Frankfurt erkundigen, ob und inwiefern das eingeräumte Widerspruchsrecht praktische Bedeutung erlangt hat.

Der Elternverein, dessen Eingabe meine Beteiligung ausgelöst hat und den ich informiert habe, hat das Widerspruchsrecht und dessen Evaluation ausdrücklich begrüßt.

4.8 Personalwesen

4.8.1 Heimliche Personalbeurteilung durch externes Unternehmen

Es bedeutet einen groben Datenschutzverstoß, wenn der Dienstherr ein Privatunternehmen ohne Kenntnis der betroffenen Bediensteten beauftragt, deren dienstliches, insbesondere das Führungsverhalten zu eruieren und zu beurteilen.

Die Eingeberin, Kanzlerin einer Fachhochschule, trug mir folgenden Sachverhalt vor:
Im Auftrag des Präsidenten der Fachhochschule erhob die "Fairness-Stiftung gemeinnützige GmbH" mit Sitz in Frankfurt am Main die Eingeberin betreffende personenbezogene Daten, ohne deren Wissen durch Befragungen in deren dienstlichem Umfeld. Konkret ging es darum, dass das dienstliche Verhalten, insbesondere das Führungsverhalten der Kanzlerin durch die Stiftung eruiert und beurteilt wurde. Diese "Expertise" wurde dann an das Wissenschaftsministerium weitergeleitet, um die Versetzung der Kanzlerin auf eine Stelle außerhalb der Fachhochschule durchzusetzen. Der Versetzungsbescheid führte zu einer verwaltungsprozessualen Auseinandersetzung.

Für die Vorgehensweise der Fachhochschule und die damit verbundene Tätigkeit der Fairnessstiftung ist eine Rechtsgrundlage nicht ersichtlich; die damit verbundene Datenverarbeitung lässt sich weder auf den Datenschutz bei Dienst- und Arbeitsverhältnissen regelnden § 34 HDSG noch auf die ebenfalls das Dienstverhältnis betreffenden personalaktenrechtlichen Vorschriften der §§ 107 ff. HBG stützen.

Auch wenn man ergänzend die allgemeine Vorschrift zur Verarbeitung personenbezogener Daten im Auftrag heranzieht, § 4 HDSG, bleibt die Rechtswidrigkeit der Auftragsvergabe bestehen. Danach hätte die Hochschule die Stiftung auf die Beachtung des HDSG vertraglich festlegen, die Stiftung sich der Kontrolle des HDSB unterwerfen, und die Hochschule hätte den HDSB vorab unterrichten müssen (vgl. § 4 Abs. 3 HDSG). Dies alles war nicht geschehen, so dass schon deshalb die Datenerhebung auch nicht durch § 4 HDSG gerechtfertigt sein konnte.

Diese Rechtslage teilte ich dem Präsidenten der Fachhochschule mit und bat ihn um Stellungnahme in der Angelegenheit. Zudem wies ich zusätzlich auf meine Absicht hin, sein Vorgehen förmlich nach § 27 HDSG zu beanstanden.

Die Stellungnahme des Präsidenten lieferte keine Anhaltspunkte, die geeignet waren, die datenschutzrechtliche Unzulässigkeit des Vorgehens infrage zu stellen. Dies teilte ich dem Präsidenten mit. Da seine Stellungnahme mit der Zusage geendet hatte, zukünftig datenschutzrechtlich sorgsamer zu sein und mich in Zweifelsfällen einzubinden, hielt ich es für vertretbar, seiner Bitte zu entsprechen, von einer förmlichen Beanstandung abzusehen. Über das Ergebnis meiner Prüfung habe ich die Kanzlerin der Fachhochschule informiert.

4.8.2 Prüfung von Beihilfevorgängen durch die Innenrevision

Es ist datenschutzrechtlich unzulässig, wenn eine Kommune in die Bearbeitung von Beihilfevorgängen stets die Innenrevision einbezieht.

Bei der Überprüfung der Datenverarbeitung der Stadt Limburg bin ich darauf gestoßen, dass die Innenrevision in die Bearbeitung sämtlicher Beihilfevorgänge einbezogen wird. Die Stadt Limburg hat ausgeführt, dass dies seit jeher bei ihr ständige Praxis ist.

Diese Vorgehensweise ist datenschutzrechtlich nicht zulässig.

In den personalaktenrechtlichen Vorschriften des Hessischen Beamtengesetzes, die auch die Beihilfe betreffen (§§ 107a, 107g Abs. 2f), werden die Befugnisse der Innenrevision im Hinblick auf Personalakten nicht geregelt. Allerdings zeigt § 13 Abs. 4 HDSG, dass die Ausübung von Kontroll- und Aufsichtsbefugnissen, zu denen auch Revisionstätigkeit gehört, datenschutzrechtlich zulässig 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.

Diese Regelung spricht selbst schon vom "erforderlichen Umfang", und gerade bei dem sensiblen Thema Personalakte ist die Frage der Erforderlichkeit der Datenverwendung genau zu prüfen. Ganz dementsprechend bestimmt denn auch § 107

Abs. 1 Satz 5 HBG, dass von einer Vorlage von Personalakten abzusehen ist, wenn eine Auskunft ausreicht. Das bisher Ausgeführte zum Thema Personalakte/Innenrevision habe ich auch schon im meinem 36. Tätigkeitsbericht näher dargestellt (Ziff. 5.10.1). In diesem Beitrag hatte ich auch darauf hingewiesen, dass auf Bundesebene vorgesehen ist, und die Länder dürften dem erfahrungsgemäß folgen, diese Rechtsstellung der Innenrevision bei Personalakten explizit gesetzlich zu formulieren. Dies ist mittlerweile im Bundesbeamtengesetz geschehen; die Rechtslage hat der Bundesgesetzgeber in § 107 Abs. 2, S. 2 BBG ausdrücklich klargestellt. Danach haben Zugang zur Personalakte auch die mit der Innenrevision beauftragten Beschäftigten. Aber das hat nicht die Regel, sondern die Ausnahme zu sein.

§ 107 Abs. 2 BBG

Auf Verlangen ist Beauftragten für den Datenschutz nach § 4f des Bundesdatenschutzgesetzes Zugang zur Personalakte zu gewähren. Zugang zur Personalakte haben ferner die mit Angelegenheiten der Innenrevision beauftragten Beschäftigten, soweit sie die zur Durchführung ihrer Aufgaben erforderlichen Erkenntnisse nur auf diesem Weg und nicht durch Auskunft aus der Personalakte gewinnen können. Jede Einsichtnahme nach S. 2 ist aktenkundig zu machen.

Mit dieser Vorschrift soll verdeutlicht werden, dass die Innenrevision, die typischerweise nicht mit der Bearbeitung von Personalangelegenheiten betraut ist, ausnahmsweise Zugang zu Personalakten erhalten kann. Dies kann bspw. der Fall sein, wenn es anlassbezogen oder auch stichprobenhaft um die Überprüfung der Aktenführung durch die Personalsachbearbeiter geht (vgl. etwa Battis, BBG, § 107 Rdnr. 3).

Dürfen schon Personakten nicht uneingeschränkt der Innenrevision zugänglich gemacht werden, so muss dies erst recht für Beihilfeakten gelten. Die darin enthaltenen Daten zur Gesundheit erfordern wegen ihrer Sensitivität ein höheres Schutzniveau. Dies zeigt sich denn auch daran, dass Beihilfeakten im Personalaktenrecht speziellen Regelungen unterliegen (§§ 107a, 107g Abs. 2 HBG).

Vor diesem rechtlichen Hintergrund habe ich die Stadt Limburg auf die Unzulässigkeit hingewiesen, die Innenrevision durchgängig in die Beihilfebearbeitung einzubeziehen. Die Stadt Limburg hat daraufhin zugesagt, diese Praxis zu beenden.

4.8.3 Löschung von Daten in SAP R/3 HR

Das für die Personaladministration in der hessischen Landesverwaltung eingesetzte System SAP R/3 HR kann wichtige Datenschutzanforderungen nicht erfüllen: Die Löschung von Daten ist nicht vorgesehen. Dieses System hätte deshalb zum Einsatz in der hessischen Landesverwaltung nicht ausgewählt werden dürfen. Die Löschfunktion ist unverzüglich nachzubessern, um weitere Verstöße gegen die gesetzlich geregelten Löschfristen zu vermeiden.

Obwohl die Löschfristen für die Urlaubs- und Krankheitsdaten im SAP R/3 HR-System bereits überschritten sind, ist eine Löschung dieser Daten noch nicht erfolgt. Die Frist für die vorgeschriebene Löschung der Datensätze von aus dem Dienst ausgeschiedenen Bediensteten läuft in Kürze ab. Die Möglichkeit zur Löschung dieser Datensätze ist zwar inzwischen im SAP R/3 HR-System programmtechnisch hinterlegt, bisher aber noch nicht getestet worden und somit noch nicht einsatzbereit.

Schon in meinem 36. Tätigkeitsbericht (Ziff. 5.10.3.2) habe ich mich zur Problematik Löschung von Daten im SAP-System geäußert.

Die Tatsache, dass die Löschung von kompletten Personalstammdatensätzen zunächst im SAP-Standard nicht vorgesehen war, wurde durch die Landesregierung in ihrer Stellungnahme zum 36. Tätigkeitsbericht ausdrücklich bestätigt. Bereits im Dezember 2005 hat die hessische Landesverwaltung die SAP AG aufgefordert, die Löschfunktionen zu realisieren. Die Landesregierung teilte mit, dass entsprechende Funktionalitäten und Standard-Löschreports mit dem Releasewechsel zu SAP ERP 6.0 ab Ende Juni 2007 zur Verfügung stehen sollten, die allerdings noch zu testen seien. Außerdem hatte die Landesverwaltung noch inhaltliche und organisatorische Festlegungen zu treffen, und der Entwicklungsbereich der SAP AG musste einbezogen werden.

Im Hessischen Competence-Center wurde ein Projekt "Löschen von Personaldaten" gestartet, in dessen Arbeit ich ständig eingebunden war. An Workshops zum Thema "Löschen von Personaldaten im SAP-System im Rahmen von Fristen und Datenschutzvorschriften" der SAP AG, in denen die entsprechenden Probleme besprochen und einer Lösung zugeführt werden sollten, habe ich teilgenommen.

Die durchgeführten Tests und die Diskussion um die notwendigen inhaltlichen Festlegungen zur Löschung von Daten und der zu treffenden organisatorischen Maßnahmen haben bis heute leider nicht zum Erfolg geführt.
Die Entwicklung eines "Löschreports" für die Urlaubs- und Krankheitsdaten ist zwar schon weit vorangeschritten und zwischenzeitlich wurden Tests durchgeführt, allerdings sind immer noch nicht alle Fragen im Zusammenhang mit der notwendigen Überprüfung der Ergebnisse vor einem "Echteinsatz" des entsprechenden SAP-Tools, das weiterhin an die hessischen Anforderungen angepasst werden muss, geklärt.

Ich stelle fest, dass die Fristen für die Löschung von Urlaubs- und Krankheitsdaten im SAP R/3 HR-System des Landes Hessen und die einschlägigen Vorschriften zur Löschung von Daten (§ 107f HBG, §§ 19 Abs. 3 und § 34 Abs. 4 HDSG) nicht eingehalten werden und die vorgeschriebenen Löschungen von Krankheits- und Urlaubsdaten nicht erfolgt sind.

§ 107f HBG

(1) Personalakten sind nach ihrem Abschluss von der personalaktenführenden Behörde fünf Jahre aufzubewahren. Personalakten sind abgeschlossen,
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,
wenn der Beamte ohne versorgungsberechtigte Hinterbliebene verstorben ist mit Ablauf des Todesjahres,
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 aufgrund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

§ 34 Abs. 4 HDSG

Im Falle des § 19 Abs. 3 Satz 1 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.

Auch zukünftig werde ich die weitere Entwicklungsarbeit unter datenschutzrechtlichen Gesichtspunkten, sowohl im hessischen Projekt "Löschung von Personaldaten" als auch die Workshops "Löschen von Personaldaten im SAP-System im Rahmen von Fristen und Datenschutzvorschriften" der SAP AG begleiten. Ich erwarte allerdings, dass zügig an einer zeitnahen Lösung gearbeitet wird.

4.8.4 Download-Berechtigungen und Protokollierungen im SAP R/3 HR-System

Die Anzahl der vergebenen Download-Berechtigungen im SAP R/3 HR-System ist weiterhin extrem hoch. Mit einem Download können Personaldaten außerhalb des SAP-Systems gespeichert und unkontrolliert weiterverarbeitet werden.

Unter Ziff. 5.10.3.1 meines 36. Tätigkeitsberichts habe ich über die Praxis bei der Vergabe von Download-Berechtigungen im SAP R/3 HR-System berichtet.

Zum damaligen Zeitpunkt waren von 5.374 HR-Benutzern 2.718 mit einer Download-Berechtigung ausgestattet. Die Berechtigungen werden jeweils für die Teilsysteme von SAP (z.B. Rechnungswesen und Personalwesen) getrennt geprüft und vergeben. Die Vergabe einer Download-Berechtigung im Personalwesen (SAP R/3 HR-System) darf nur dann erfolgen, wenn die Aufgabe des oder der Berechtigten die Arbeit mit solchen Downloads erfordert. Diese Berechtigungen müssen restriktiv vergeben werden, da sie zur Folge haben, dass Personaldaten außerhalb des SAP-Systems unkontrolliert weiterverarbeitet werden können.

Das SAP-System wird im Landesintranet unter Einsatz eines Windows Terminal Servers (WTS) genutzt. Der WTS ermöglicht als zentrale Zugangsstelle den Zugriff auf die verschiedenen SAP-Teilsysteme. Zum Arbeiten mit SAP R/3 melden sich die zugangsberechtigten Bediensteten des Landes Hessen im Landesintranet über diesen WTS-Server an und erhalten Zugriff auf die jeweiligen SAP-Systeme. Den Bediensteten, die auf mehrere SAP-Teilsysteme zugriffsberechtigt sind, werden automatisch die weitestgehenden Zugriffsrechte für jedes System vergeben, da die Rechtevergabe auf WTS-Ebene und nicht auf der Ebene der Teilsysteme erfolgt.

Von den 2.718 Anwendern waren lediglich 1.679 Nutzer im HR-System berechtigt, Downloads durchzuführen. Dies bedeutete, dass 1.039 Anwender, die sowohl auf dem SAP-Rechnungswesen-System als auch auf dem SAP-HR-System zugangsberechtigt waren, Daten aus dem SAP-HR-System downloaden und somit personenbezogene Daten auf ihrer Festplatte speichern, mit anderen Daten zusammenzuführen, weiterverarbeiten oder weiterleiten konnten, obwohl ihre Aufgabe im Personalwesen dies nicht erforderte.

Im Zugriffsberechtigungsrahmenkonzept des Landes Hessen ist ausdrücklich geregelt, dass die Vergabe von Download-Berechtigungen restriktiv zu erfolgen hat, um eine unkontrollierte Verarbeitung von vertraulichen Daten des Landes Hessen auf lokalen Arbeitsplatzrechnern einzuschränken.

In ihrer Stellungnahme zu meinem 36. Tätigkeitsbericht vertrat die Landesregierung die Auffassung, eine Überprüfung dieser Vergabepraxis habe ergeben, dass die Vergabe der Download-Berechtigungen restriktiv erfolgt sei.
Diese Auffassung wird von mir bei dieser sehr hohen Anzahl von Usern, die downloadberechtigt sind, nach wie vor nicht geteilt.

Eine nochmalige Prüfung der im HR-System vergebenen Berechtigungen für das Downloaden von personenbezogenen Daten hat ergeben, dass zum heutigen Zeitpunkt von 5.511 HR-Anwendern für 2.194 Nutzer Downloadkonten auf WTS existieren. Lediglich 1.696 Anwender sind aus SAP-HR heraus berechtigt. Es ist festzustellen, dass auch weiterhin 498 Nutzer, die sowohl auf das Rechnungswesen-System als auch auf das HR-System zugreifen dürfen, aus WTS heraus Berechtigungen zum Download auf beide Systeme haben. Dies, obwohl sie diese Rechte nur für das Rechnungswesen-System haben dürften. Es kann auch bis heute nicht verhindert werden, dass für Mitarbeiter, die über WTS sowohl einen Zugang zum Rechnungswesen-System als auch zum HR-System haben, automatisch die weitestgehenden Zugriffsrechte für beide Systeme eingerichtet werden. Die Landesregierung hat in ihrer Stellungnahme zum 36. Tätigkeitsbericht das Problem eingeräumt und angekündigt, Lösungsansätze zu erarbeiten. Diese sind bis jetzt weder gefunden noch umgesetzt worden.

Somit können auch heute noch 498 Anwender personenbezogene Daten aus dem HR-System herunterladen, obwohl die zuständigen Legitimationsberechtigten ihnen dieses Recht für das HR-System aufgrund ihrer Aufgabenstellung nicht einräumen durften und nicht eingeräumt haben.

Die Problematik der unberechtigten Downloadmöglichkeiten wird noch dadurch verschärft, dass eine Protokollierung der Downloads nicht erfolgt. Einstellungen für eine gezielte Protokollierung auf SAP-Ebene bzw. WTS-/Betriebssystemebene für den Download und das Kopieren von Informationen aus dem HR-System existieren nicht.

Bei beiden beschriebenen Sachverhalten muss ein Verstoß gegen § 10 Abs. 2 Ziff. 3, 4 und 5 HDSG festgestellt werden.

§ 10 Abs. 2 Ziff. 3, 4 und 5 HDSG

Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. Außerdem sind Maßnahmen schriftlich anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, dass
…
die zur Benutzung eines Datenverarbeitungsverfahrens Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle),
es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind (Verantwortlichkeitskontrolle)
…

4.8.5 HEPIS-Neu - Einrichtung einer zentralen Stelle für Auswertungen aus SAP R/3 HR

Führungsberichte können bisher aus dem SAP R/3 HR-System nicht erstellt werden. Künftig soll eine zentrale Auswertestelle im Innenministerium solche Führungsberichte erstellen.

In meinem 36. Tätigkeitsbericht habe ich unter Ziff. 5.10.3.5 über die Absicht der Landesregierung berichtet, ein Business-Warehouse-HR zu implementieren, mit dem Führungsberichte und Berichte als Grundlage für strategische Entscheidungen erstellt werden sollten.

Meine Auffassung, dass den Mitarbeiterinnen und Mitarbeitern, die im Rahmen des Vorprojekts "Business-Warehouse HR/HEPIS-Neu", entsprechende Auswertemöglichkeiten entwickeln sollten, durch die Landesverwaltung zunächst konkrete und detaillierte Vorgaben gegeben werden müssten, teilte die Landesregierung nicht. Ich halte dies aber nach wie vor für notwendig, um aussagekräftige und zielgerichtete Auswertungen erstellen zu können.

In ihrer Stellungnahme stellte die Landesregierung fest, dass Anforderungen und Zielgruppen eines Gesamt-Personal-Berichtswesens für das operative HR-System und das zu entwickelnde Business-Warehouse definiert worden seien.

Dies konnte ich auch in der Folgezeit bei weiterer Mitarbeit im Vorprojekt leider nicht feststellen. In den unzähligen Sitzungen, an denen ich teilnahm, habe ich immer wieder die Frage nach den konkreten Vorgaben gestellt. Ich hielt und halte es für unmöglich, ein Business-Warehouse zu entwickeln, ohne dass im Vorhinein die notwendigen Auswertungen und deren Inhalte festgelegt und definiert werden. Nur so kann im Vorfeld konkret über die einzelnen Daten entschieden werden, die zunächst für die weiteren Verarbeitungsschritte aus anderen Systemen in das Business-Warehouse übertragen werden müssen, damit dort die entsprechenden Auswertungen erstellt werden können. Die Datenbasis ist die Grundlage jeder Auswertung.

Am 4. Mai 2009 wurde die zuständige Fachabteilung darüber informiert, dass auf Weisung des Hessischen Ministers des Innern und für Sport die Arbeiten an dem Projekt "HEPIS-Neu" bis auf Weiteres ausgesetzt werden.

Nach meinem jetzigen Kenntnisstand ist stattdessen beabsichtigt, dass eine "zentrale Auswertestelle" im Innenministerium eingerichtet werden soll, die zukünftig für die Erstellung von Führungsberichten und Berichten als Grundlage für strategische Entscheidungen zuständig sein soll. Mir wurde zugesagt, dass ich bei der Entwicklung der dort zu erstellenden Berichte rechtzeitig und umfassend eingebunden werde. Ich habe selbstverständlich meine Mitarbeit zugesagt. Auch eine "zentrale Auswertestelle", die im Innenministerium angesiedelt sein soll, hat die einschlägigen Vorschriften des § 120 HBG, des § 107 Abs. 3 HBG, des § 107g Abs. 1 und 2 HBG und des HDSG, insbesondere § 34 Abs. 1 HDSG zu beachten.

§ *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.*

§ *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 die zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

§ *107g Abs. 1 und 2 HBG*

(1) Personalaktendaten dürfen in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet und genutzt werden. Ihre Übermittlung ist nur nach Maßgabe des § 107d zulässig. Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist.

(2) Personalaktendaten im Sinne des § 107a dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden.

§ *34 HDSG*

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

5. Kommunen

5.1 Forderungsmanagement durch Kommunen

Die Beauftragung eines privaten Inkassounternehmens mit dem Forderungseinzug von Forderungen der öffentlichen Hand ist datenschutzrechtlich dann unproblematisch, wenn es sich um eine reine Hilfeleistung auf Anweisung der öffentlichen Stelle im Vorfeld der eigentlichen Vollstreckung handelt und das Inkassobüro keine genaue Kenntnis über das konkrete Schuldverhältnis erlangt.

Bereits in meinem 34. Tätigkeitsbericht (Ziff. 6.1) hatte ich mich mit der Frage beschäftigt, ob die Einbeziehung privater Dritter beim Einzug von Forderungen durch öffentliche Stellen (insbesondere Kommunen) datenschutzrechtlich zulässig ist. Inzwischen wurde diese Thematik auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgegriffen und äußerst kontrovers diskutiert. Einige Landesbeauftragte vertraten die Auffassung, dass diese Einbeziehung letztlich nur mit einer Aufgabenübertragung an das Inkassobüro möglich sei, es dafür aber keine gesetzliche Grundlage gebe und dies deshalb rechtlich unzulässig sei.

Für eine Übertragung der Aufgabe sehe auch ich keine rechtliche Grundlage. Zumal die eigentliche Vollstreckungsaufgabe nach dem Verwaltungsvollstreckungsgesetz eine hoheitliche Aufgabe ist und schon deshalb nicht auf einen Privaten übertragen werden kann.

Allerdings halte ich die Einschaltung eines privaten Inkassobüros dann für rechtlich unproblematisch, wenn das Büro als Verwaltungshelfer im Wege der Auftragsdatenverarbeitung nach § 4 HDSG bei der Vollstreckungsarbeit Hilfsdienste leistet. Die Vollstreckungsaufgabe bleibt in diesem Fall in der Hand der öffentlichen Stelle, das Inkassobüro erbringt lediglich Unterstützungsleistungen.

Diesen Weg ist die Landeshauptstadt Wiesbaden gegangen. Sie hat ein privates Inkassobüro damit beauftragt, sie bei der Beitreibung von Forderungen zu unterstützen. Dabei wurden dem Inkassobüro folgende Aufgaben zugewiesen:

- Führung der gesamten Korrespondenz mit den Schuldnern einschließlich aktiver und passiver Telefonkontakte,
- Überprüfung der Bonität des Schuldners,
- Adressermittlungen,
- Arbeitgeberermittlungen,
- Vermittlung von Ratenzahlungsvereinbarungen als Bote des Auftraggebers und deren Überwachung,
- Vermittlung von Vergleichen als Bote des Auftraggebers,
- Sachstandsmitteilungen,
- Abführen einzelner Beträge und Abrechnung gegenüber dem Auftraggeber.

Wie diese einzelnen Aufgaben durchgeführt werden sollen, wird von der Landeshauptstadt im Detail vorgegeben. Das heißt es gibt genaue Handlungsanweisungen durch den Auftraggeber an den Auftragnehmer. Insoweit hat der Auftragnehmer keinen eigenen Handlungsspielraum.

Der Auftraggeber teilt dem Auftragnehmer auch nicht mit, um welche Forderungen es sich handelt, sondern der Auftragnehmer weiß lediglich, dass der Schuldner XY der Landeshauptstadt einen Betrag in einer bestimmten Höhe schuldet. So erfährt das Inkassobüro grundsätzlich nicht, ob es sich bei der geschuldeten Zahlung z.B. um eine Steuerschuld handelt. Der Firma werden die folgenden Daten mitgeteilt:

- Name,
- Anschrift,
- Geburtsdatum,
- Höhe der offenen Forderung,
- Datum der Fälligkeit.

Besonderer Wert wurde bei der Vereinbarung zwischen der Landeshauptstadt Wiesbaden und dem privaten Inkassobüro auch auf die Festlegung besonderer technischer und organisatorischer Datenschutzmaßnahmen gelegt, damit die Daten auch im Bestand des Inkassobüros vor den Zugriffen anderer Abteilungen wirksam geschützt sind.

Ich habe unter diesen Rahmenbedingungen die Hilfeleistung durch ein privates Unternehmen beim Forderungseinzug datenschutzrechtlich nicht beanstandet.

5.2 Elektronisches Personenstandsregisterverfahren bei der ekom21

Die ekom21 hat zur Umsetzung der Vorgaben des Gesetzes zur Reform des Personenstandsrechts vom Februar 2007 ein elektronisches Personenstandsregisterverfahren entwickelt, das sie als Dienstleister den Kommunen anbietet.

Grundlage für das elektronische Personenstandsregister ist - wie im 36. Tätigkeitsbericht (Ziff. 4.3) und 37. Tätigkeitsbericht (Ziff. 9.2) schon ausgeführt - das Gesetz zur Reform des Personenstandsrechts vom 19. Februar 2007 (BGBl. I S. 122), das zum 1. Januar 2009 in Kraft getreten ist.

Pünktlich zum 1. Januar 2009 hat die Stadt Frankfurt am Main als erste Stadt in Deutschland das elektronische Personenstandsregister eingeführt. Dem sind mittlerweile ca. 300 Standesämter in Hessen gefolgt. Alle diese Standesämter nutzen das von der ekom21 angebotene Verfahren ePR21 (elektronisches Personenstandsregister). Mit diesem Verfahren bietet die ekom21 als erster Dienstleister in Deutschland eine Lösung für die Umsetzung des Personenstandsreformgesetzes an. Das Verfahren fußt auch auf den Vorarbeiten, die in der AG-Hessen, bestehend aus Standesamtsleitern, Vertretern des Hessischen Innenministeriums, des Standesamtsverlags, der ekom21 und meiner Dienststelle erarbeitet wurden. Das Register umfasst das Geburtenregister, das Eheregister, das Lebenspartnerschaftsregister und das Sterberegister.

Bei der Realisierung des Verfahrens hat die ekom21 einen Schwerpunkt auf die langfristige Verfügbarkeit der im ePR gespeicherten Daten gelegt. So wird das elektronische Personenstandsregister gespiegelt, d.h. ein vollständiges Abbild wird parallel vorgehalten. Zusätzlich gibt es das vom Gesetz vorgesehene Sicherungsregister, das auch ein Abbild des führenden Registers ePR darstellt. Auch das Sicherungsregister wird nochmals gespiegelt geführt. Das bedeutet, dass die Daten physikalisch vierfach vorhanden sind, wobei die Register und ihre gespiegelten Abbilder jeweils rechtlich als ein System zu betrachten sind.

Technische Basis dieser Lösung ist ein etabliertes Archivierungssystem, das wiederum bei der Speicherung WORM-Medien (einmal beschriebene Speichermedien) nutzt. In einem Datensicherheitskonzept ist niedergelegt, wie unberechtigte Zugriffe verhindert werden sollen. Eine Vorabkontrolle wurde durchgeführt und das Muster eines Verfahrensverzeichnisses, das die Kunden in die Verfahrensbeschreibung des Fachverfahrens integrieren können, liegt vor.

Die ekom21 hat mir über wesentliche Verfahrensschritte berichtet. Ich beabsichtige 2010 das Verfahren zu überprüfen.

5.3 Öffentliche Hinweispflicht der Meldebehörden über Widerspruchsrechte ihrer Einwohner vor Wahlen

Meldebehörden haben nicht nur einmal jährlich ihre Einwohner darauf hinzuweisen, dass diese der Weitergabe ihrer Adressdaten an Parteien, Trägern von Wahlvorschlägen oder Wählergruppen widersprechen können. Sie müssen auch beachten, dass der Hinweis bei anstehenden Wahlen oder Abstimmungen spätestens acht Monate vorher erfolgt.

Im Zusammenhang mit Wahlen kommt es immer wieder zu Eingaben von Bürgern, die sich über unerwünschte Wahlwerbung beschweren und bei mir nachfragen, wie die Absender an ihre Anschrift gekommen sind.

In den meisten Fällen stellte sich aufgrund meiner Überprüfung heraus, dass die Daten aus zulässigen Melderegisteranfragen gemäß § 35 Abs. 1 und 2 HMG stammten.

Auffallend war jedoch die häufige Unkenntnis der Betroffenen über die Möglichkeit, im Vorfeld von Wahlen gegen die Datenübermittlung rechtzeitig Widerspruch gemäß § 35 Abs. 5 HMG zu erheben. Zum einen liegt dies daran, dass die Betroffenen etwaige Hinweise überlesen oder die örtliche Bekanntmachungsform nicht kennen, zum anderen aber auch daran, dass die Meldebehörden ihrer Hinweispflicht nicht oder nicht rechtzeitig nachkommen.

Auch die Gesetzesänderung aus dem Jahr 2005, wonach der Hinweis auf das Widerspruchsrecht anlässlich von Wahlen spätestens acht Monate vor der Wahl zu erfolgen hat (§ 35 Abs. 5 S. 2 HMG), wird noch nicht überall beachtet. So war z.B. der öffentliche Hinweis einer Kommune im Juni 2009 für die Bundestagswahl im September 2009 zu spät, obwohl der Pflicht, bei der Anmeldung und einmal jährlich zu informieren, nachgekommen wurde.

Obgleich durch derartige Versäumnisse die Gültigkeit einer Wahl nicht beeinträchtigt wird (s. z.B. Urteil des OVG Saarland vom 4. April 2008, 3 A 8/07), liegt dennoch ein datenschutzrechtlicher Verstoß vor.

In meiner kommunalen Beratung weise ich auf die Einhaltung dieser Pflichten hin. Es wäre aber unterstützend, wenn auch von Seiten des HMDIS entsprechende Informationen an die Kommunen erfolgen könnten.

5.4 Auskunft über eine erteilte erweiterte Melderegisterauskunft

Wird über einen Betroffenen eine erweiterte Melderegisterauskunft aufgrund eines berechtigten Interesses erteilt, so ist die Meldebehörde verpflichtet, den Betroffenen hierüber unverzüglich zu unterrichten. Hat der Anfragende hingegen ein rechtliches Interesse an der erweiterten Melderegisterauskunft geltend gemacht, so darf die Meldebehörde den Betroffenen weder darüber unterrichten noch ihm auf Anfrage eine Auskunft hierüber erteilen. Möchte der Betroffene eine Prüfung der Rechtmäßigkeit der Erteilung der Auskunft, muss er den Hessischen Datenschutzbeauftragten einschalten. Auch ein Rechtsnachfolger kann berechtigter Antragsteller eines Auskunftsersuchens sein.

Ein Bürger bat mich um rechtliche Prüfung der Auslegung und Anwendung des Hessischen Meldegesetzes. Der Beschwerdeführer hatte als Rechtsnachfolger seiner kurz zuvor verstorbenen Mutter von der Gemeindeverwaltung des Wohnortes Auskunft darüber verlangt, wer über Daten seiner Mutter eine erweiterte Melderegisterauskunft erhalten hatte, womit das berechtigte Interesse begründet wurde und welchen Inhalt die Auskunft hatte. Als Rechtsnachfolger war er berechtigt, entsprechende Auskünfte einzuholen, da die informationelle Selbstbestimmung und damit der Datenschutz Verstorbener über den Tod hinaus wirken. Bei der Ausübung von Betroffenenrechten eines Verstorbenen ist ein Rechtsnachfolger kein Dritter. Die Gemeinde verweigerte die Auskunft mit dem Hinweis, dass § 34 Abs. 2 Satz 2 HMG eine Unterrichtung des Betroffenen verbietet, wenn der Datenempfänger ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, glaubhaft gemacht hat. Dies sei hier der Fall gewesen. Damit sei auch eine Auskunft unzulässig.

§ 34 Abs. 2 HMG

Soweit jemand ein berechtigtes Interesse glaubhaft macht, darf ihm zusätzlich zu den in Abs. 1 Satz 1 genannten Daten einer einzelnen bestimmten Person eine erweiterte Melderegisterauskunft erteilt werden über

1. *Tag und Ort der Geburt,*
2. *frühere Vor- und Familiennamen,*
3. *Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine eingetragene Lebenspartnerschaft führend oder nicht,*
4. *Staatsangehörigkeiten,*
5. *frühere Anschriften,*
6. *Tag des Ein- und Auszugs,*
7. *Vor- und Familienname sowie Anschrift der Ehegattin oder des Ehegatten oder der Lebenspartnerin oder des Lebenspartners,*
8. *gesetzliche Vertreterin/gesetzlicher Vertreter oder Betreuerin oder Betreuer und*
9. *Sterbetag und -ort.*

Die Meldebehörde hat Betroffene über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten; dies gilt nicht, wenn der Datenempfänger ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, glaubhaft gemacht hat.

Der Beschwerdeführer bat mich um Überprüfung, ob die Weigerung rechtens sei und es eine Möglichkeit gäbe, die Informationen trotzdem zu erhalten, da diese für die Ordnung des Nachlasses von Bedeutung sein könnten.
Aufgrund meiner Nachfrage übersandte mir die Gemeinde die kompletten Unterlagen zur erteilten erweiterten Melderegisterauskunft. Die Anfrage war ordnungsgemäß dokumentiert und ihre Bearbeitung datenschutzrechtlich nicht zu beanstanden.
Auskunftsansprüche der Betroffenen sind in § 9 HMG spezialgesetzlich geregelt, die Vorschriften des Hessischen Datenschutzgesetzes finden daher keine Anwendung (§ 3 Abs. 3 HDSG)

§ 9 Abs. 1, 6, 7 HMG

(1) Die Meldebehörde hat Betroffenen auf Antrag Auskunft zu erteilen über
die zur Person gespeicherten Daten und Hinweise, auch soweit sie sich auf deren Herkunft beziehen,
die Empfänger oder Kategorien von Empfängern von regelmäßigen Datenübermittlungen sowie die Arten der zu übermittelnden Daten,
die Zwecke und die Rechtsgrundlagen der Speicherung und von regelmäßigen Datenübermittlungen.
…
(6) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind Betroffene darauf hinzuweisen, dass sie sich an den Hessischen Datenschutzbeauftragten wenden können.

(7) Wird Betroffenen keine Auskunft erteilt, so ist sie auf Verlangen dem Hessischen Datenschutzbeauftragten zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Hessischen Datenschutzbeauftragten an Betroffene darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

§ 9 Abs. 1 Nr. 3 HMG regelt den Auskunftsanspruch auf Antrag eines Betroffenen über Empfänger sowie Art der übermittelten Daten, soweit es sich um regelmäßige Datenübermittlungen handelt. Für Datenübermittlungen im Einzelfall sieht das HMG keinen Auskunftsanspruch vor.

Lediglich soweit der Empfänger die Daten aus einem berechtigten Interesse heraus begehrt, aber kein rechtliches Interesse darstellen kann, ist bei den erweiterten Melderegisterauskünften in § 34 Abs. 2 HMG eine antragslose Unterrichtungspflicht der Meldebehörde vorgesehen.

Ein berechtigtes Interesse ist anzunehmen, wenn ein von der Rechtsordnung erlaubtes Interesse, insbesondere auch ein wirtschaftliches Interesse glaubhaft gemacht wird. Ein rechtliches Interesse besteht in der Regel erst dann, wenn Interessen im Rahmen eines konkreten bestehenden Schuldverhältnisses dargelegt werden können, z.B. zur Vollstreckung einer Forderung. Hier soll verhindert werden, dass sich z.B. ein Schuldner auf Vollstreckungsmaßnahmen einstellen und sie damit vereiteln kann.

Das Ergebnis war für den Betroffenen unbefriedigend, weil er weder nach § 34 Abs. 2 HMG über die erteilte Auskunft unterrichtet werden muss noch ihm nach § 9 Abs. 1 Nr. 3 ein Auskunftsanspruch für eine einmalige Auskunft zusteht.

In die rechtliche Prüfung des Auskunftsanspruchs habe ich das hessische Innenministerium eingebunden. Dieses hält durch das Ersatzrecht des § 9 Abs. 7 HMG die Rechte des Betroffenen für ausreichend berücksichtigt.

Ich halte die generelle Einschränkung des Auskunftsanspruchs auf regelmäßige Datenübermittlungen ohne Abwägung der Belange des Betroffenen im Melderecht für unangemessen und habe deshalb im Rahmen der anstehenden Gesetzgebung für ein neues Bundesmeldegesetz eine entsprechende Änderung gefordert.

5.5 Ordnungsgemäße Verwendung der Zuzugstransaktion bei PAMELA

Nach dem Hessischen Melderecht ist der Zugriff auf Einwohnermeldedaten anderer Kommunen nur zulässig, wenn der Betroffene tatsächlich in der anfragenden Kommune zugezogen ist.

In meinem 33. Tätigkeitsbericht (Ziff. 6.4) und in meinem 34. Tätigkeitsbericht (Ziff. 9.4) hatte ich darüber berichtet, dass einige hessische Kommunen den für die Durchführung eines Zuzugs nach § 37a Abs. 3 HMG rechtmäßigen automatisierten Zugriff auf Einwohnermeldedaten anderer Kommunen nutzen, um die dort gespeicherten Daten zu anderen Zwecken als einem Zuzug zu erhalten. Die Mitarbeiter simulieren in der entsprechenden Transaktion einen Zuzug und brechen den Vorgang vor einer endgültigen Speicherung aber nach Erhalt der gewünschten Informationen wieder ab. Durch eine Auswertung von Datenbankprotokollen lässt sich dieses Vorgehen nachweisen. In der Vergangenheit habe ich betroffene Kommunen jeweils über die Unzulässigkeit dieser Vorgehensweise informiert.

Wie in meinem 33. und 34. Tätigkeitsbericht angekündigt, habe ich auch weiterhin die Einhaltung der Zweckvorgabe der Zuzugstransaktion überprüft. Entgegen dem Ergebnis des Jahres 2005 ergab auch die neueste Auswertung der Datenbankprotokolle, dass einige Kommunen häufig Zuzugstransaktionen abbrechen. Auffällig ist hierbei, dass in einigen Landkreisen fast alle Kommunen sich dieser unzulässigen Methode bedienen, während es vor allem im nordhessischen Raum Landkreise

gibt, in denen nicht eine Kommune auffällig ist. Erfreulich ist in diesem Zusammenhang nur, dass nur zwei der in den vergangenen Jahren von mir angeschriebenen Kommunen weiterhin durch überdurchschnittliche Abbrüche bei Zuzugstransaktionen aufgefallen sind.

Ich habe wieder einige der Kommunen mit erhöhten Zahlen von Zuzugsabbrüchen angeschrieben und um Stellungnahme unter gleichzeitigem Hinweis auf die ausdrückliche Zweckbindung des § 37a Abs. 3 HMG gebeten. Den mir bereits vorliegenden Stellungnahmen ist das fehlende Unrechtsbewusstsein für Zugriffe auf fremde Datenbestände deutlich zu entnehmen. Eine Kommune hat hierfür sogar den Begriff "Pseudozuzug" geschaffen. Angebliche Amtshilfe und Zeitersparnis setzen für diese Einwohnermeldeämter offensichtlich die Vorgaben der Rechtsgrundlage außer Kraft.

Der im Jahr 2004 von der Kundenbetreuung des Fachbereichs Einwohnerwesen der Kommunalen Gebietsrechenzentren erteilte Hinweis an alle am Verfahren Einwohnerwesen teilnehmenden Kommunen, dass der Abruf von Daten eines Einwohners einer anderen Kommune nur im Rahmen einer tatsächlichen Anmeldung zulässig ist, konnte offensichtlich nicht überall langfristig überzeugen.

Ich werde daher weiterhin entsprechende Prüfungen der Datenbankprotokolle veranlassen und die betroffenen Kommunen direkt informieren.

5.6 Auskunft über Mitglieder eines Naturschutzbeirates

Mitglieder eines Beirates oder einer anderen öffentlichen Institution unterliegen in dieser Funktion nicht dem Datenschutz. Allerdings muss die Weitergabe personenbezogener Daten auf die Informationen beschränkt bleiben, die im direkten Zusammenhang mit dem öffentlichen Amt stehen.

Eine Bürgerinitiative bat das Umweltamt einer Stadt als Untere Naturschutzbehörde um Auskunft, welche Personen dem nach § 52 HENatG zu berufenden Naturschutzbeirat angehören. Die Bürgerinitiative wollte damit überprüfen, ob die im Naturschutzgesetz gemachten Vorgaben für die Zusammensetzung des Naturschutzbeirates eingehalten wurden.

§ 52 HENatG

(1) Bei der obersten Naturschutzbehörde und den unteren Naturschutzbehörden werden unabhängige und sachverständige Naturschutzbeiräte gebildet.

(2) Die Naturschutzbeiräte beraten die Naturschutzbehörden in grundsätzlichen Angelegenheiten des Naturschutzes. Der Beirat ist von der Naturschutzbehörde über grundsätzliche Angelegenheiten des Naturschutzes rechtzeitig zu unterrichten, dies gilt insbesondere für:
1. die Vorbereitung von Rechtsverordnungen;
2. Planungen und Planfeststellungen nach anderen Rechtsvorschriften von überörtlicher Bedeutung, bei denen die Naturschutzbehörde mitwirkt;
3. für das gesamte Kreis- oder Stadtgebiet bedeutsame Vorgänge, bei denen die untere Naturschutzbehörde eine Entscheidungs- oder Mitwirkungsbefugnis hat.
4. Durch die Beteiligung der Naturschutzbeiräte sollen Verwaltungs- und Entscheidungsverfahren nicht über das nötige Maß hinaus verzögert werden.

(3) Die Mitglieder des Beirats bei der obersten Naturschutzbehörde werden durch die für Naturschutz und Landschaftspflege zuständige Ministerin oder den hierfür zuständigen Minister, die Mitglieder der Beiräte bei den unteren Naturschutzbehörden werden vom Kreisausschuss, in den Städten vom Magistrat berufen. Die Zahl der zu berufenden Mitglieder der Beiräte wird von der zuständigen Ministerin oder dem zuständigen Minister oder den anderen nach Satz 1 zuständigen Stellen unter Berücksichtigung fachlicher oder regionaler Belange festgelegt; hierbei darf die Zahl zwölf nicht überschritten werden. Mindestens die Hälfte der Beiratsmitglieder wird auf Vorschlag der anerkannten Naturschutzverbände berufen. Die Mitglieder der Beiräte sollen orts- und sachkundige Personen sein. Bedienstete derjenigen Behörden, bei denen der Beirat eingerichtet wird, können nicht berufen werden. Die Amtsdauer beträgt vier Jahre. Die Beiräte wählen aus ihrer Mitte den Vorsitzenden.
Mitglieder eines Beirates oder einer anderen öffentlichen Institution unterliegen in dieser Funktion nicht dem Datenschutz. Das bedeutet, dass über ihre Funktion innerhalb des Beirates bzw. über den Anlass ihrer Berufung auf Anfrage eine Auskunft erteilt werden muss. Da nach den Vorschriften des Naturschutzgesetzes mindestens die Hälfte der Mitglieder des Naturschutzbeirates auf Vorschlag anerkannter Naturschutzverbände berufen werden müssen, gehört auch die Tatsache, welcher Naturschutzverband die einzelnen Mitglieder benannt hat zu den Informationen, die im Zusammenhang mit dem öffentlichen Amt nicht dem Datenschutz unterliegen.

Nach Klärung der Rechtslage erhielt die Bürgerinitiative die gewünschten Informationen.

5.7 Datenschutz bei der Feuerwehr

5.7.1 "Florix-Hessen"

Das HMDIS ist auch für den Brand- und Katastrophenschutz zuständig. In dieser Funktion hat es den Feuerwehren das Programm "Florix-Hessen" zur Verfügung gestellt, das im Unterschied zu dem bisherigen Einzelplatzverfahren für den Brand- und Katastrophenschutz wichtige übergreifende Arbeitsabläufe unterstützt.

Um die Arbeit der Feuerwehren zu unterstützen, gab es in Hessen seit vielen Jahren das Einzelplatzprogramm "Florix". Da es nach Einschätzung des Innenministeriums nicht mehr den Anforderungen genügte und mögliche Vorteile einer IT-Unterstützung nicht zum Tragen kamen, wurde 2007 mit Überlegungen zur Weiterentwicklung begonnen, die mir vorgestellt wurden. Im Jahr 2009 wurde das darauf aufbauende Verfahren "Florix-Hessen", eine Web-Lösung, eingeführt. Das HMDIS hat Muster für Verfahrensverzeichnisse und eine Reihe von weiteren Dokumenten bereitgestellt. Im Zuge der Einführung zeigten sich einige Probleme, die inzwischen behoben sind bzw. deren Behebung in Kürze ansteht.

5.7.1.1 Das Verfahren "Florix-Hessen"

"Florix-Hessen" dient der zentralen Verwaltung von Daten der Feuerwehren als gemeindliche Einrichtungen und der jeweiligen Aufsichtsbehörden. Es umfasst eine Personalverwaltung der Feuerwehrangehörigen, Einsatzberichterstattung und Fakturierung sowie Materialverwaltung.

Dazu werden die Daten auf kommunaler Ebene erfasst, ausgewertet und abgefragt, wobei auch feuerwehrinterne Stellen, welche nicht am Verwaltungssitz der Kommune ansässig sind, zugreifen können.
Die Landkreise können die zur dortigen Wahrnehmung von Aufgaben notwendigen Daten abfragen sowie Statistiken erstellen.

Ferner unterstützt "Florix-Hessen" die Verwaltung von Lehrgängen der Feuerwehren, z.B. bei der Anmeldung von Teilnehmern. Dabei werden von den Feuerwehren mögliche Teilnehmer dem Landkreis benannt, der das eigentliche Anmeldeverfahren steuert.

"Florix-Hessen" unterstützt auch die Regierungspräsidien und das HMDIS als Aufsichtsbehörden. Sie können statistische Auswertungen vornehmen und im Materialbereich Daten abfragen, die im Rahmen der Gefahrenabwehrplanung und Brandschutzförderung Informationen über die relevanten Materialbestände der Feuerwehren liefern. Um die gewünschten Auswertungen vornehmen zu können, entschied man sich für eine zentrale Lösung.

Neben den genannten Modulen, die für die eigentliche Arbeit der Feuerwehren vorgesehen sind, gibt es für Feuerwehrvereine noch eine Funktion zur Verwaltung von Vereinsdaten. Feuerwehrvereine sind Vereine im Sinne des BGB. Sie haben sich zum Ziel gesetzt, die Arbeit der Feuerwehr zu unterstützen. Mitglieder müssen nicht selbst Angehörige der Feuerwehr sein und auch nicht jeder Feuerwehrmann ist Mitglied im Verein. Insofern ist das Vereinsmodul kein fachlicher Bestandteil von Florix und sowohl hinsichtlich der Datenspeicherung als auch der Zugriffsrechte für jeden Verein gekapselt.

5.7.1.2 In "Florix-Hessen" gespeicherte personenbezogene Daten

Personenbezogene Daten werden über Feuerwehrangehörige und Vereinsangehörige sowie im Zusammenhang mit Einsatzberichten gespeichert. Rechtsgrundlagen für die Speicherung der Daten der Feuerwehrangehörigen und der Einsatzberichte sind § 55 Abs. 2, 5 und 6 HBKG und § 34 Abs. 1 HDSG.

§ 55 Abs. 2, 5 und 6 HBKG

(2) Die Feuerwehren, die Katastrophenschutzbehörden und die Aufsichtsbehörden sowie die Landesfeuerwehrschule dürfen für Einsätze sowie für die Ausbildung und Fortbildung notwendige personenbezogene Daten von Feuerwehrangehörigen und Helferinnen oder Helfern im Katastrophenschutz im erforderlichen Umfang verarbeiten. Hierzu zählen nur folgende Daten:

1. Name,
2. Vornamen,
3. Geburtsdatum,
4. Anschrift,
5. Beruf,
6. Angaben über die körperliche Tauglichkeit und Eigenschaften,
7. Datum des Eintritts in die Feuerwehr oder der Verpflichtung in der Einheit und Einrichtung des Katastrophenschutzes,
8. Name der Feuerwehr oder Bezeichnung der Einheit oder Einrichtung des Katastrophenschutzes,
9. Dienstgrad, Beförderungen,
10. Funktion in der Feuerwehr oder in der Einheit und Einrichtung des Katastrophenschutzes,
11. Ausbildungslehrgänge und Fortbildungslehrgänge einschließlich der Beurteilungsergebnisse,
12. besondere Kenntnisse und Fähigkeiten,
13. Telefonnummern und Telefaxnummern sowie Angaben über die Erreichbarkeit,
14. Beschäftigungsstelle und Bankverbindungen.

…

(5) Für die Erstellung einer landesweiten Statistik für den Brandschutz oder den Katastrophenschutz dürfen die Feuerwehren und die Katastrophenschutzbehörden sowie die zuständigen Aufsichtsbehörden nur folgende Daten im erforderlichen Umfang verarbeiten:

1. Anzahl der geschädigten oder betroffenen Personen,
2. Ort des Ereignisses,
3. Datum und Uhrzeit des Ereignisses,
4. Art des Ereignisses.

(6) Die zuständigen Gefahrenabwehrbehörden, sonstige für die Gefahrenabwehr zuständige Behörden und die Polizeidienststellen dürfen den Feuerwehren und Katastrophenschutzbehörden die zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlichen betrieblichen Daten übermitteln. Die Behörden übermitteln diese Daten auf Anforderung, soweit ihnen diese im Rahmen ihrer Aufgabenerfüllung bekannt geworden sind. Sie übermitteln die Daten im Einzelfall auch ohne Anforderung, wenn dies zur Erfüllung der Aufgaben nach diesem Gesetz erforderlich ist.

§ 34 Abs. 1 HDSG

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

Für die Speicherung der Daten von Vereinsangehörigen muss eine Einwilligung eingeholt werden.
Außerdem können Kontaktadressen von Stellen und Personen gespeichert werden, mit denen die jeweils erfassende Dienststelle regelmäßig Kontakte unterhält.

Beispiele für Daten von Feuerwehrangehörigen sind

- Name, Geburtsdatum, Adresse, Erreichbarkeiten, Beruf
- Abteilungszugehörigkeit, Dienstgrad, Zutrittsberechtigungen (Schlüsselvergabe u.Ä.), Dienstausweise, dienstliche Ehrungen, Abzeichen - z.B. Wettbewerbe
- Zugzugehörigkeit, Funktionen in der Feuerwehr, überörtliche Funktionen
- arbeitsmedizinische Tauglichkeiten und Untersuchungen (ohne Untersuchungsergebnis, nur Tauglichkeitsfeststellung), vorhandene Impfungen, Fahrerlaubnis, erhaltene persönliche Ausstattung, Erreichbarkeiten, Beurlaubungen
- Arbeitgeber, Angehörige (als Verständigungsadressen im Einsatzfall bzw. bei Unfällen), Bankverbindung (für Kostenerstattungen u.Ä.)
- Lehrgänge - einschließlich Anmeldung.

Bei einer Einsatzdokumentation fallen als Daten Zeitpunkt, Art und Ort des Schadensereignisses, ausgerückte und eingesetzte Mittel und Personal, ins Einsatzgeschehen involvierte Personen, Lage und Maßnahmen der Feuerwehr sowie statistische Felder zur Einsatzart, Ort und Umfang und Gebührenbescheid an.

5.7.1.3 Zugriffsberechtigte

Feuerwehrmodul

Die jeweilige Feuerwehr muss für sich festlegen, wer welche Zugriffsrechte auf die eigenen Daten hat.

Neben den Feuerwehren haben Bedienstete der Brandschutzdienststelle der Landkreise im Rahmen ihrer Aufsichtsfunktionen sowie für die Lehrgangsabwicklung Zugriff. Gleiches gilt für Beschäftigte der Brandschutzdezernate bzw. des Brandschutzreferates bei den Regierungspräsidien und dem HMDIS im Rahmen ihrer Aufsichtsfunktionen. Für die Lehrgangsabwicklung haben Bedienstete der Landesfeuerwehrschule Zugriff auf die Daten der Lehrgangsteilnehmer.

In den Gesprächen mit dem HMDIS wurden die Zugriffsrechte für die Landkreise, Regierungspräsidien und das HMDIS genauer spezifiziert. Danach soll wie folgt verfahren werden:
Der generelle Zugriff auf Daten einer Person ist nicht gerechtfertigt. Der Zugriff besteht nur für Daten, die benötigt werden. Dafür gibt es zwei Konstellationen:

- Im Rahmen und für die Zeit der Bearbeitung eines Workflows zu einer Person, z.B. Anmeldung zu Lehrgängen oder Beantragung von Ehrungen,
- aufgrund der Dienststellung einer Person in einem öffentlichen Amt.

Der Workflow für die Lehrgangsanmeldung und die Beantragung von Ehrungen über die Verwaltungsebenen hinweg existiert noch nicht und muss noch erarbeitet werden.

Als öffentliche Ämter gelten:

- Leiterin oder Leiter der Feuerwehr und Stellvertreterin oder Stellvertreter,
- Kreisbrandinspektorin oder Kreisbrandinspektor und Stellvertreterin oder Stellvertreter,
- Kreisbrandmeisterin oder Kreisbrandmeister und Stellvertreterin oder Stellvertreter,
- Stadtbrandinspektor oder Stadtbrandinspektorin und Stellvertreterin oder Stellvertreter,
- Gemeindebrandinspektor oder Gemeindebrandinspektorin und Stellvertreterin oder Stellvertreter,
- Wehrführer oder Wehrführerin und Stellvertreterin oder Stellvertreter,
- Kreis-/Stadt-/Gemeindefeuerwehrwarte/innen,
- örtliche Jugendfeuerwehrwarte/innen.

Für diesen Personenkreis kann zu dienstlichen Zwecken nur auf folgende Daten in "Florix-Hessen" zugegriffen werden: Titel, Name, Einsatzabteilung, Geburtsdatum, Geschlecht, Anschrift, Tel./Erreichbarkeiten, Dienstgrad und Dienststellung sowie auf die zugehörige "Historie".

Gegen die Zugriffsberechtigung auf die "Einsatzberichte" durch Aufsichtsbehörden bestanden wegen etwaiger persönlicher Daten betroffener Personen, z.B. Verletzte oder Unfallverursacher, datenschutzrechtliche Bedenken. Nach eingehender Diskussion wurde ein solcher Zugriff auch nicht als notwendig erachtet.

Da eine Reihe von Daten für mehrere Daten verarbeitende Stellen im Zugriff sind, handelt es sich bei "Florix-Hessen" um ein gemeinsames Verfahren nach § 15 HDSG.

Vereinsmodul

Auf die Daten der Feuerwehrvereine haben nur vom Vorstand des Vereins zugelassene Personen Zugriffsrechte. Es gibt keine Rechte für leitende Mitglieder der Feuerwehr oder Beschäftigte der Aufsichtsbehörden.

5.7.1.4 Umsetzung

"Florix-Hessen" wurde im Auftrag des HMDIS durch die Fa. Dräger entwickelt. Dräger ist auch Auftragnehmer beim Betrieb des Verfahrens und bedient sich eines kommerziellen Rechenzentrums.

Das Verfahren ist webbasiert und es wird über das Internet auf die Daten zugegriffen. Damit dieser Ansatz datenschutzrechtlich akzeptabel ist, wurden eine Reihe von Sicherheitsmaßnahmen ergriffen. Es verbietet sich, diese im Detail zu erläutern. Jedoch können einige Grundzüge skizziert werden.

- Die Datenbestände der einzelnen Feuerwehren sind gegeneinander abgeschottet. Die Feuerwehr kann für die eigenen Daten Administratorrechte und andere Zugriffsrechte an Angehörige der Feuerwehr vergeben.
- Die Datenübertragung erfolgt verschlüsselt. Es kommt das https-Protokoll zum Einsatz.
- Um auf die Daten zugreifen zu können, benötigt ein Benutzer nicht nur eine Benutzerkennung und ein Passwort, sondern auch ein passendes (Software-)Zertifikat. Aus dem Zertifikat ergibt sich, zu welcher Stelle und damit auch zu welcher Anwenderebene das Gerät gehört, von dem aus zugegriffen wird. Anwenderebenen sind die Gemeinde (und damit Feuerwehr), der Kreis oder die Landesbehörde. Es wird beispielsweise geprüft, ob das Zertifikat zur gleichen Feuerwehr wie die Benutzerkennung gehört. Ist das nicht der Fall, wird der Zugriff verweigert.

Das HMDIS hat den Feuerwehren Muster für ein Verfahrensverzeichnis nach § 6 HDSG zur Verfügung gestellt und Muster für eine Reihe von Informationen oder Erklärungen.

5.7.1.5 Probleme

Trotz der Vorbereitungen haben sich Probleme ergeben. Auf zwei möchte ich eingehen.

5.7.1.5.1 Freiwilligkeit der Verarbeitung von Vereinsdaten

Aus einigen Eingaben musste ich entnehmen, dass nicht in allen Kommunen die Unterschiede der Rechtsgrundlagen zur Speicherung von Daten der Feuerwehrangehörigen und der Feuerwehrvereine beachtet wurden.

Es kam vor, dass keine Einwilligung bei den Vereinsangehörigen zur Datenspeicherung eingeholt wurde. Mit der Begründung, die Daten müssten gespeichert werden, wurden vorhandene Daten kopiert oder Daten erfasst.

5.7.1.5.2 Nutzung privater PC

Ein weiteres Problem ergab sich daraus, dass in vielen Feuerwehren Bürger ehrenamtlich tätig sind und von zu Hause die Daten in "Florix-Hessen" pflegen müssen. Es steht kein Geld zur Verfügung, um überall dienstliche Geräte zur Verfügung zu stellen. Das HMDIS hat daher private PCs zugelassen. Der Nutzer erhält lediglich eine Informationsschrift, was er zu beachten hat.

Diese Lösung ist nicht befriedigend. Man kann unterstellen, dass der Bürger nicht wissentlich gegen Regelungen verstößt; anderenfalls könnte er auch in den Räumen der Feuerwehr unberechtigt Daten kopieren. Durch die Nutzung privater Rechner könnten aber die Zertifikate (s. Ziff. 5.7.1.3) in fremde Hände gelangen, was die Sicherheit des Verfahrens schwächt, oder Daten als Kopie auf dem Rechner verbleiben und Unberechtigte diese zur Kenntnis nehmen.

Bei der Suche nach Lösungen haben das HMDIS und ich zwei Möglichkeiten ins Auge gefasst, die beide auf USB-Sticks basieren.

Als Interimslösung steht ein USB-Stick zur Verfügung, auf dem ein portabler Browser installiert ist. Nur in diesem Browser wird das Zertifikat gespeichert. Es kann nicht vom USB-Stick kopiert werden. Gleichzeitig kann festgelegt werden, auf wie vielen Rechnern mit diesem Stick gearbeitet werden kann. Wenn der Browser gestartet wird, kann nur die Startseite von Florix aufgerufen werden. Nach Beenden des Programms werden die temporären Dateien gelöscht.
Mit dieser Lösung ist nicht ausgeschlossen, dass Schadprogramme durch entsprechende Routinen das Zertifikat oder Daten kopieren.

Als zukünftige Lösung wird deshalb über einen bootfähigen USB-Stick nachgedacht, der eine vergleichbare Funktionalität hat und zusätzlich Gefahren durch Schadprogramme weitgehend reduziert.

5.7.2 Verarbeitung von Gesundheitsdaten

Medizinische Daten, die während eines Übungskurses auf einer Atemschutzübungsanlage zur Gesundheitsüberwachung erhoben wurden, dürfen von der Feuerwehr nicht über die Übung hinaus gespeichert werden, da sie für die weitere Aufgabenerfüllung der Feuerwehr nicht erforderlich sind.

Mehrere Angehörige der Feuerwehr eines Landkreises haben sich an meine Dienststelle gewandt und die Erhebung und Speicherung von Gesundheitsdaten durch die Kreisbranddirektion beanstandet. Bei einem Streckendurchgang auf der Atemschutzübungsanlage seien Herzfrequenz sowie Blutdruckmessungen nach dem Muster vorher/nachher bei den Teilnehmern des Durchgangs aufgezeichnet worden. Die Feuerwehrangehörigen sahen für eine derartige Datenverarbeitung keine Rechtsgrundlage und bezweifelten auch die Erforderlichkeit dieser Maßnahme, da die Personen, die mit dieser Überwachung der Gesundheitsdaten befasst gewesen seien, keine medizinischen Kenntnisse aufweisen würden. Zudem wurde die weitere Speicherung dieser Daten beim Kreis als unzulässig erachtet.

Eine Rücksprache bei der Brandschutzabteilung im Hessischen Ministerium des Innern und für Sport zeigte, dass in den einzelnen Kreisen in Hessen der Ablauf der Übungskurse auf den Atemschutzübungsanlagen sehr unterschiedlich gehandhabt wird. Teilweise wurde so verfahren, wie oben beschrieben. Teilweise wurden während der Übungen keine Gesundheitsdaten erhoben.

Der betroffene Kreis hat die Datenerhebung und weitere Speicherung) auf § 55 Abs. 2 Nr. 6 Hessisches Brand- und Katastrophenschutzgesetz (HBKG) gestützt. Danach dürfen Angaben über die körperliche Tauglichkeit und Eigenschaften der Wehrangehörigen von den Feuerwehren, Katastrophenschutzbehörden und den Aufsichtsbehörden für Einsätze oder die Ausbildung und Fortbildung im notwendigen Umfang verarbeitet werden.

§ 55 Abs. 2 HBKG

Die Feuerwehren, die Katastrophenschutzbehörden und die Aufsichtsbehörden sowie die Landesfeuerwehrschule dürfen für Einsätze sowie für die Ausbildung und Fortbildung notwendige personenbezogene Daten von Feuerwehrangehörigen und Helferinnen oder Helfern im Katastrophenschutz im erforderlichen Umfang verarbeiten. Hierzu zählen nur folgende Daten:

1. *Name,*
2. *Vornamen,*
3. *Geburtsdatum,*
4. *Anschrift,*
5. *Beruf,*
6. *Angaben über die körperliche Tauglichkeit und Eigenschaften,*
7. *Datum des Eintritts in die Feuerwehr oder der Verpflichtung in der Einheit und Einrichtung des Katastrophenschutzes,*
8. *Name der Feuerwehr oder Bezeichnung der Einheit oder Einrichtung des Katastrophenschutzes,*
9. *Dienstgrad, Beförderungen,*
10. *Funktion in der Feuerwehr oder in der Einheit und Einrichtung des Katastrophenschutzes,*
11. *Ausbildungslehrgänge und Fortbildungslehrgänge einschließlich der Beurteilungsergebnisse,*
12. *besondere Kenntnisse und Fähigkeiten,*
13. *Telefonnummern und Telefaxnummern sowie Angaben über die Erreichbarkeit,*
14. *Beschäftigungsstelle und Bankverbindungen.*

Von Seiten der Wehrangehörigen wurde argumentiert, dass die körperliche Tauglichkeit und Eigenschaft durch regelmäßige Lehrgänge und arbeitsmedizinische Untersuchungen nachgewiesen werde, die zusätzliche Verarbeitung von Gesundheitsdaten anlässlich der Übungsläufe in der Atemschutzübungsanlage sei nicht erforderlich.
Insbesondere die Frage nach der Erforderlichkeit dieser Datenverarbeitung habe ich in einem Gespräch mit Vertretern der Brandschutzabteilung des hessischen Innenministeriums erörtert. Zweifel an der Erforderlichkeit waren schon insofern angebracht, als die Vorgehensweise - wie oben dargelegt - von Kreis zu Kreis unterschiedlich, die Aufgabenstellung aber überall einheitlich ist. Letztlich teilte mir das Innenministerium mit, dass die Überwachung und Messung des gesundheitlichen Zustandes (Messung des Blutdrucks/Pulsüberwachung) während der Durchführung der Atemschutzübung aus seiner Sicht erforderlich ist, um bei Auftreten von gesundheitlichen Problemen (z.B. deutliche Überhöhung des Pulsschlags) eingreifen zu können und den Abbruch der Übung anzuordnen. Dies sei zum Schutz der Teilnehmer geboten. Diese Argumentation schien aus meiner Sicht überzeugend, zumal von Seiten der Kreisbrandinspektion vorgetragen worden ist, dass es bei derartigen Übungen schon zu Todesfällen gekommen sei. Ich habe deshalb aus datenschutzrechtlicher Sicht nichts gegen die Erhebung dieser Daten während der Übung einzuwenden.

Davon zu unterscheiden ist die weitere Speicherung dieser Daten. Hier wurde auch von den Vertretern des Ministeriums vorgetragen, dass die Speicherung der bei der Übung erhobenen Daten für die weitere Aufgabenerfüllung nicht erforderlich ist. Damit ist sie datenschutzrechtlich auch nicht zulässig. Ich habe deshalb gegenüber dem zuständigen Kreisbrandinspektor die Löschung der bereits gespeicherten Daten verlangt. Diese wurde mir umgehend bestätigt. Bei künftigen Übungen darf während des Streckendurchlaufs der Gesundheitszustand kontrolliert werden, eine weitere Dokumentation darf allerdings nicht stattfinden.

Insgesamt strebt das Innenministerium aufgrund der stattgefundenen Erörterung der Problematik eine einheitliche Lösung für ganz Hessen an.

6. Sonstige Selbstverwaltungskörperschaften

6.1 Rundfunk

6.1.1 Ergebnisse der Prüfung der GEZ

Gemeinsam mit den Landesdatenschutzbeauftragten von Brandenburg und Berlin habe ich bei der Gebühreneinzugszentrale (GEZ) ein weiteres Mal die Einhaltung der Datenschutzvorschriften stichprobenartig überprüft. Geprüft wurden u.a. Datenübermittlungen der GEZ an Dritte, der Zugriff der Rundfunkgebührenbeauftragten auf Teilnehmerkonten, die Betriebsstättendatenbank und der elektronische Anmeldungs- und Änderungsdienst.

Die GEZ ist eine öffentlich-rechtliche nichtrechtsfähige Verwaltungsgemeinschaft mit Sitz in Köln, die aufgrund einer Verwaltungsvereinbarung der in der ARD zusammengeschlossenen Landesrundfunkanstalten, des ZDF und des Deutschlandradios errichtet worden ist. Sie fungiert als gemeinsames Rechen- und Servicezentrum der Rundfunkanstalten beim Einzug der Rundfunkgebühren. Ihre Aufgaben in diesem Zusammenhang sind vielfältig: Sie nimmt An- und Abmeldungen der Rundfunkteilnehmer entgegen, verwaltet den Teilnehmerbestand, nimmt die Gebühren an und betreibt das Gebühreninkasso, bearbeitet Anträge auf Befreiung von der Rundfunkgebührenpflicht und führt sog. Mailing-Aktionen durch, um Rundfunkteilnehmer, die ihre Geräte nicht angemeldet haben, zur Anmeldung zu bewegen. Die GEZ verarbeitet die Daten im Auftrag der einzelnen Landesrundfunkanstalten. Mit 43 Mio Teilnehmerkonten zählt sie zu den größten Verarbeitern personenbezogener Daten in Deutschland.

6.1.1.1 Datenübermittlungen der GEZ an Dritte

6.1.1.1.1 Auskünfte an Polizei- und Staatsanwaltschaften

An die GEZ gerichtete Auskunftsersuchen der Polizei und der Staatsanwaltschaften betreffen entweder Ermittlungsverfahren gegen Rundfunkteilnehmer, Dritte oder Bedienstete der GEZ. Die GEZ erteilt Auskünfte aus Teilnehmerkonten nur, wenn das Ersuchen schriftlich eingegangen ist, ein staatsanwaltschaftliches Aktenzeichen oder eine polizeiliche Tagebuchnummer und eine Unterschrift enthält. Auskunftsersuchen erfolgten nach Angaben der GEZ bislang ausschließlich im Rahmen der Strafverfolgung, nicht jedoch für Zwecke der Gefahrenabwehr. Auskünfte werden nicht zum Teilnehmerkonto gespeichert, es wird dort auch kein Hinweis auf das Auskunftsersuchen aufgenommen. Bei den Ermittlungen gegen Rundfunkteilnehmer oder Dritte geht es in den meisten Fällen um Vermögensdelikte, wie z.B. Betrug oder Insolvenzstraftaten. Häufig wird lediglich nachgefragt, ob eine bestimmte Person unter einer bestimmten Adresse als Rundfunkteilnehmer gemeldet ist oder war. Vor allem bei Konkursstraftaten wird darüber hinaus oft um Auskunft gebeten, ob noch offene Forderungen der GEZ bestehen (wenn ja, in welcher Höhe) und ob noch Zahlungen in einem bestimmten Zeitraum stattgefunden haben. Eher selten dient das Auskunftsersuchen der Aufenthaltsermittlung einer bestimmten Person.

Die Datenverarbeitung im Zusammenhang mit staatsanwaltschaftlichen und polizeilichen Ermittlungsverfahren begegnete keinen datenschutzrechtlichen Bedenken. Staatsanwaltschaft und Polizei können gestützt auf §§ 161 Abs. 1, 163 Abs. 1 StPO Auskünfte von der GEZ verlangen. Die Datenspeicherung getrennt vom Teilnehmerkonto ist datenschutzrechtlich geboten, da in der Regel kein Zusammenhang zum Teilnehmerkonto besteht. Eine Speicherung im Teilnehmerkonto ist nicht erforderlich und würde dem Grundsatz der Zweckbindung widersprechen. Lediglich über die Speicherdauer gab es zunächst unterschiedliche Ansichten. Die GEZ wollte die Daten über Ermittlungsverfahren nach den handelsrechtlichen Aufbewahrungsbestimmungen des § 257 HGB aufbewahren, was eine zehnjährige Aufbewahrungsdauer bedeutet hätte. Die Landesrundfunkanstalten und die GEZ ließen sich jedoch davon überzeugen, dass es sich bei den Akten über Auskunftsersuchen nicht um Unterlagen i.S.v. § 257 Abs. 1 HGB handelt. Die Unterlagen werden nunmehr vier Wochen nach Bearbeitung gelöscht.

§ 161 Abs. 1 StPO

Zu dem in § 160 Abs. 1 und 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen, und in diesem Falle befugt, von allen Behörden Auskunft zu verlangen.

§ 161 Abs. 1 StPO

Die Behörden und Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Zu diesem Zweck sind sie befugt, alle Behörden um Auskunft zu ersuchen, bei Gefahr im Verzug auch, die Auskunft zu verlangen, sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

§ 257 Abs. 1, 2 und 4 HBG

(1) Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:

1. Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
2. die empfangenen Handelsbriefe,
3. Wiedergaben der abgesandten Handelsbriefe,
4. Belege für Buchungen in den von ihm nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege).

(2) Handelsbriefe sind nur Schriftstücke, die ein Handelsgeschäft betreffen.
…
(4) Die in Absatz 1 Nr. 1 und 4 aufgeführten Unterlagen sind zehn Jahre, die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre aufzubewahren.

6.1.1.1.2 Auskunftsersuchen von Finanzämtern, kommunalen Behörden und Sozialleistungsträgern

Anfragen von Finanzämtern oder kommunalen Behörden beantwortet die GEZ nicht. Die Anfragen erfolgen in der Regel ins Blaue und zielen auf eine Übermittlung von Bankverbindungen und Anschriften. Auch Anfragen von Sozialleistungsträgern, zunehmend von ARGE nach SGB II, beantwortet die die GEZ nicht. Nach Angaben der GEZ geben sich die anfragenden Behörden in der Regel damit zufrieden, dass sie keine Auskunft erhalten.

Bei ihrer restriktiven Auskunftspraxis orientiert sich die GEZ an der strickten Zweckbindung, die § 3 Abs. 3 Satz 1 RGebStV für Gebührendaten vorschreibt. Angesichts des Umstands, dass sich die Finanzbehörden anscheinend mit der Auskunftsverweigerung abfinden, brauchte nicht geklärt zu werden, ob insbesondere die in § 93 Abs. 1 Satz 2 AO geregelte Auskunftspflicht die Zweckbindung des § 3 Abs. 3 Satz 1 RGebStV aufhebt.

§ 3 Abs. 3 Satz 1 RGebStV

Die Landesrundfunkanstalt darf die in Abs. 2 genannten Daten nur für die ihr im Rahmen des Rundfunkgebühreneinzugs obliegenden Aufgaben verarbeiten und nutzen.

6.1.1.1.3 Datenübermittlungen an die Firma Creditreform

Die GEZ bzw. die Landesrundfunkanstalten schalten bei der Einziehung offener Rundfunkgebührenforderungen die Fa. Creditreform ein. Dies erfolgt nach Angaben der GEZ am Ende des förmlichen Mahn- und Vollstreckungsverfahrens. Creditreform wird demnach erst tätig, wenn eine offene Forderung trotz eines durchgeführten Vollstreckungsverfahrens nach dem Verwaltungsvollstreckungsrecht nicht eingetrieben werden konnte.

Die Forderungen werden nicht an Creditreform abgetreten. Creditreform führt keine Zwangsmaßnahmen durch, sondern wird nach der Verfahrenskonzeption der Landesrundfunkanstalten nur als Verwaltungshelfer tätig. Creditreform schreibt die Gebührenschuldner in der Regel zweimal an. Beide Schreiben sind mit der GEZ abgestimmt. Im ersten Schreiben wird der Schuldner über die Beauftragung informiert und gebeten, die Forderung zu begleichen. Creditreform bezeichnet sich in diesem Schreiben als Vermittler und beschreibt die Zahlungsaufforderung als Chance, weitere Unannehmlichkeiten und Kosten zu vermeiden. Das zweite Schreiben weist den Schuldner auf die bestehende Vollstreckbarkeit des Bescheids hin und bietet ihm die Möglichkeit an, bei Zahlungsschwierigkeiten Vollstreckungsschutz zu beantragen. Es wird darauf hingewiesen, dass Creditreform mit der Landesrundfunkanstalt in Verhandlung über den Vollstreckungsschutz stehe. Nach Auskunft der GEZ ist das Verfahren sehr erfolgreich.

Ob und in welchem Umfang die Beauftragung von Creditreform zulässig ist, ist zunächst eine verwaltungsrechtliche Frage. Die Vollstreckung öffentlich-rechtlicher Forderungen ist eine hoheitliche Aufgabe, für die das Verwaltungsvollstreckungsrecht maßgeblich ist. § 7 Abs. 6 Satz 1 RGebStV ordnet die Anwendung der Vorschriften über den Verwaltungszwang ausdrücklich an. Damit steht fest, dass Creditreform nicht mit Aufgaben der Vollstreckung betraut werden könnte, da dies nur im Wege der Beleihung möglich wäre, die hier nicht gegeben ist. Creditreform kann daher lediglich als Verwaltungshelfer tätig werden. Folgerichtig sieht das von der GEZ und den Landesrundfunkanstalten festgelegte Verfahren dies auch so vor. Datenschutzrechtlich folgt daraus, dass Creditreform nur im Wege der Auftragsdatenverarbeitung gemäß § 4 HDSG für den Hessischen Rundfunk tätig werden kann. Auch das entspricht der Konzeption der Landesrundfunkanstalten.

Zu monieren war, dass der HR seiner Pflicht, den HDSB gemäß § 4 Abs. 3 Satz 2 HDSG vorab über die Beauftragung zu informieren, nicht erfüllt hatte. Darüber hinaus enthielt der Vertrag mit Creditreform keine Klausel, wonach sich der Auftragnehmer meiner Kontrolle unterwirft. Der HR hat eine entsprechende Vertragsänderung zugesagt. Von mir zur Sicherung, dass die gesetzlichen Grenzen der Auftragsdatenverarbeitung eingehalten werden, konkret angeregte inhaltliche Präzisierungen des Vertrages im Hinblick auf das Zahlungsverfahren hält der HR allerdings für entbehrlich. Verwaltungshilfe und Datenverarbeitung im Auftrag sind dadurch gekennzeichnet, dass lediglich untergeordnete Hilfstätigkeiten übertragen werden können. Der Auftragnehmer darf keinen eigenen Entscheidungsspielraum erhalten, sondern muss streng weisungsgebunden handeln. Dem widersprechen Vertragsregelungen, die Creditreform das Recht einräumen, über Zahlungsmodalitäten und das Mahnverfahren (Anzahl und Inhalt der Mahnschreiben) zu entscheiden.

§ 7 Abs. 6 Satz 1 RGebStV

Bescheide über rückständige Rundfunkgebühren werden im Verwaltungszwangsverfahren vollstreckt.

6.1.1.2 Zugriff der Rundfunkgebührenbeauftragten auf Teilnehmerkonten

Kein Einvernehmen konnte mit dem Hessischen Rundfunk darüber erzielt werden, in welchem Umfang Rundfunkgebührenbeauftragte einen Online-Zugriff auf die bei der GEZ geführten Teilnehmerkonten erhalten dürfen. Der Hessische Rundfunk beschäftigt ca. 100 Gebührenbeauftragte. Sie haben die Aufgabe, Personen zu ermitteln, die Rundfunkgeräte zum Empfang bereithalten, diese jedoch nicht bei der GEZ angemeldet haben. Die Rundfunkgebührenbeauftragten stehen in keinem Arbeitsverhältnis zu den Rundfunkanstalten, sondern sind als freie Mitarbeiter tätig. Die Datenverarbeitung erledigen sie zum größten Teil in ihrem häuslichen Bereich oder vor Ort bei den besuchten Personen. Dazu hat ihnen die GEZ einen Online-Zugang zu sämtlichen 43 Mio. Teilnehmerkonten eingerichtet, der sowohl mit stationären als auch mobilen Geräten genutzt werden kann.

Den bundesweiten Zugriff der Gebührenbeauftragten auf die Teilnehmerkonten rechtfertigt der HR in erster Linie mit der Außenwirkung des Beauftragten-Dienstes, dessen Kompetenz und Souveränität. Sachverhalte müssten sofort und einvernehmlich beim Teilnehmer geklärt werden. Dies liege sowohl im Interesse des einzelnen Rundfunkteilnehmers als auch der Gemeinschaft der Gebührenzahler, denn dadurch ließen sich unklare Gebührensituationen vermeiden, die zu fehlerhaften Gebührenbescheiden und zu erheblichen Prozess- und Prozesskostenrisiken für die Landesrundfunkanstalten und damit die Gesamtheit der Gebührenzahler führen könnten.

Dem ist entgegenzuhalten, dass Gebührenbeauftragten durchaus eine datenschutzrechtlich angemessene Rolle bei Zugriffen auf die Teilnehmerkonten zugewiesen werden kann. So können z.B. beim WDR Unterbeauftragte das Abrufverfahren nicht nutzen. Einer eventuellen Qualitäts- und Effizienzsteigerung im Beauftragten-Dienst durch den bundesweiten Datenzugriff stehen erhebliche Datenschutzrisiken gegenüber. Selbst durch eine Protokollierung der Datenzugriffe lässt sich eine missbräuchliche Verwendung der Daten nicht ausschließen. Es gibt keinen vergleichbaren Verwaltungsbereich, in dem "externen" Mitarbeitern derartige Rechte und Möglichkeiten eingeräumt werden. Die Zugriffsmöglichkeit muss deshalb wieder auf den geographischen Zuständigkeitsbereich der Gebührenbeauftragten beschränkt werden.

6.1.1.3 Betriebsstättendatenbank

Die GEZ vermutet bei den nicht privaten (NP-)Teilnehmern, (d.h. gewerblichen Teilnehmern) einen hohen Prozentsatz nicht gemeldeter Rundfunkteilnehmer. Sie geht davon aus, dass weniger als 50% der Teilnehmer gemeldet sind und die Zahl der angemeldeten Geräte noch deutlich unter diesem Wert liegt. Vor diesem Hintergrund arbeitet die GEZ seit längerem an der Errichtung einer NP-Datenbank, die als Arbeitsmittel zur Erhöhung der Anmeldequote der GEZ, den Landesrundfunkanstalten und den Rundfunkgebührenbeauftragten zur Verfügung stehen soll. Die Datenbank soll genutzt werden für Mailingaktionen, Telefonmarketing, den Beauftragtendienst sowie für Regional- und Eventmarketing. In der NP-Datenbank werden u.a. folgende Merkmale gespeichert:

- Name,
- Postleitzahl, Ort, Straße, Hausnummer,
- Branchencode (allgemein und Schober-intern),
- Werbecode,
- Rechtsform,
- Betriebsgröße,
- Firmenart,
- Telefonnummer,
- Anzahl der Beschäftigten,
- Anzahl der Betten (bei Hotellerie und Gastronomie),
- Anzahl der Fahrzeuge,
- Gründungsdatum,
- Vorname, Name eines Ansprechpartners,
- E-Mail-Adresse,
- Homepage,
- Anzahl der PCs.

Die in der NP-Datenbank gespeicherten Angaben werden von einem externen Anbieter quartalsweise bezogen.

Soweit Datensätze über Freiberufler, Einzelunternehmer, Kleingewerbetreibende usw. gespeichert werden, handelt es sich um Daten natürlicher Personen, so dass für diesen Teil der Datenbank die datenschutzrechtlichen Vorschriften gelten. Die Daten über juristische Personen unterliegen nicht den gesetzlichen Datenschutzbestimmungen.

Die Datenerhebung bei einem externen Anbieter überschreitet in einigen Fällen das gesetzlich zulässige Maß. § 8 Abs. 4 RGebStV erlaubt grundsätzlich die Erhebung personenbezogener Daten bei Dritten ohne Kenntnis des Betroffenen. Unerheblich ist, ob es sich um Daten von Teilnehmern handelt oder nicht. Es genügt, dass die Daten zur Feststellung, ob ein Teilnehmerverhältnis besteht, erhoben, verarbeitet oder genutzt werden. Die NP-Datenbank erfüllt diese Voraussetzung. Auch die Anforderung, dass die Datenbestände geeignet sein müssen, Rückschlüsse auf die Gebührenpflicht zuzulassen (§ 8

Abs. 4 Satz 2 Nr. 1 RGebStV), ist erfüllt. § 8 Abs. 4 Satz 2 Nr. 2 RGebStV erlaubt allerdings nur die Erhebung der dort enumerativ aufgeführten Daten. Die Regelung gestattet weder die Erhebung der Mitarbeiterzahl, der Bettenzahl, der Betriebsgröße noch der Anzahl der Kfz.

Die GEZ und die Landesrundfunkanstalten sind dagegen der Ansicht, dass die Erhebung auch dieser Daten zulässig sei. Sie berufen sich darauf, dass es sich um Daten aus allgemein zugänglichen Quellen handele. Für derartige Daten gilt das Hessische Datenschutzgesetz nicht (§ 3 Abs. 4 HDSG). Beide übersehen jedoch, dass die Norm in diesem Falle nicht anwendbar ist. § 8 Abs. 4 RGebStV ist eine bereichsspezifische Vorschrift zur Erhebung personenbezogener Daten bei nichtöffentlichen Stellen ohne Kenntnis des Betroffenen. Sie regelt abschließend die Datenerhebung der GEZ und der Landesrundfunkanstalten und unterscheidet nicht zwischen Daten aus allgemein zugänglichen Quellen und solchen, die diese Eigenschaft nicht haben. Als bereichsspezifische Regelung geht § 8 Abs. 4 RGebStV den Bestimmungen des HDSG vor (§ 3 Abs. 3 HDSG), so dass ein Rückgriff auf § 3 Abs. 4 HDSG nicht möglich ist.

Darüber hinaus handelt es sich bei den von der GEZ angemieteten Daten nicht um allgemein zugängliche Daten i.S.v. § 3 Abs. 4 HDSG. Allgemein zugänglich sind Daten, wenn sie sowohl in ihrer Zielsetzung als auch in ihrer Publikationsform einem unbegrenzten Personenkreis ohne rechtliche oder tatsächliche Hürden ohne Weiteres zugänglich sind. Bei der Veräußerung von Privatanschriften durch privatwirtschaftliche Adresshändler erhält gerade nicht ein unbegrenzter Personenkreis Zugang zu diesen Informationen. Vielmehr entscheidet der Adresshändler als Privatrechtssubjekt im Rahmen seiner Privatautonomie ganz individuell darüber, welchem Personenkreis er seine Informationen zur Verfügung stellt. Private Adresshändler sind nicht verpflichtet, ihre Informationen jedermann zugänglich zu machen. Anders verhält es sich bei Daten in veröffentlichten Medien, Adressbüchern, Telefonbüchern oder öffentlichen Registern wie dem Handelsregister, die jeder ohne Weiteres erhalten kann. Zudem mietet die GEZ nicht nur schlichte Adressdaten an, die in der Tat häufig in öffentlich zugänglichen Registern enthalten sind. Sie erhält von den Adresshändlern selektierte und strukturierte Datenbestände, die in dieser Form nicht ohne Weiteres allgemein zugänglichen Quellen entnommen werden können.

Eine Erhebung und Speicherung von Daten, die über den in § 8 Abs. 4 Satz 2 N. 2 RGebStV festgelegten Datensatz hinausgehen, ist daher unzulässig.

§ 8 Abs. 4 RGebStV

Die zuständige Landesrundfunkanstalt oder die von ihr beauftragte Stelle nach Absatz 2 kann zur Feststellung, ob ein den Vorschriften dieses Staatsvertrages genügendes Rundfunkteilnehmerverhältnis besteht, und zur Verwaltung von Rundfunkteilnehmerverhältnissen personenbezogene Daten bei nichtöffentlichen Stellen ohne Kenntnis des Betroffenen erheben, verarbeiten oder nutzen. Voraussetzung dafür ist, dass
die Datenbestände dazu geeignet sind, Rückschlüsse auf die Gebührenpflicht zuzulassen, insbesondere durch Abgleich mit dem Bestand der nach § 3 angemeldeten Rundfunkteilnehmer und
sich die Daten auf Angaben zu
a) Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe,
b) Berufs-, Branchen- oder Geschäftsbezeichnungen,
c) Vor- und Familiennamen,
d) Titel,
e) Anschriften und
f) Geburtsdatum
beschränken und kein erkennbarer Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat.

Es dürfen keine Daten, die Rückschlüsse auf tatsächliche oder persönliche Verhältnisse liefern könnten, an die übermittelnde Stelle rückübermittelt werden. Die Daten sind spätestens zwölf Monate nach ihrer Erhebung zu löschen. Sie sind unverzüglich zu löschen bei Feststellung des Nichtbestehens oder des Bestehens eines Rundfunkteilnehmerverhältnisses, das den Voraussetzungen dieses Staatsvertrages entspricht. Das Verfahren der regelmäßigen Datenübermittlung durch die Meldebehörden nach den Meldegesetzen oder Meldedatenvermittlungsverordnungen der Länder bleibt unberührt.

§ 3 Abs. 3 und Abs. 4 HDSG

(3) Soweit besondere Rechtsvorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten vorhanden sind, gehen sie den Vorschriften dieses Gesetzes vor.

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

6.1.1.4 Online An- und Änderungsmeldungen

Die GEZ stellt auf ihrer Internetseite (http://www.gez.de) Anmelde- und Änderungsformulare zur Verfügung. Auf meine Anregung hin hat sie das Verfahren des elektronischen Anmeldungs- und Änderungsdienstes durch eine an das sog. doppelte Opt-In-Verfahren angelehnte Prozedur vor Missbrauch durch Dritte stärker geschützt. Das Verfahren der doppelten Einwilligung (doppeltes Opt-In-Verfahren) wird im E-Mail-Marketing und bei der Bestellung von Newslettern zur Vermeidung von Verstößen gegen das Verbot unverlangter E-Mail-Werbung (§ 7 Abs. 2 Nr. 3 UWG) eingesetzt. Bei einer Anmeldung oder Änderungsmeldung per Webformular schickt die GEZ nun an die im Formular angegebene E-Mail-Adresse eine Bestä-

tigungsmail mit einem Aktivierungslink. Erst nachdem der Empfänger der Bestätigungsmail den Link angeklickt hat, wird die Anmeldung bzw. Änderung an die GEZ gesendet und verarbeitet. Die GEZ kann so die Eingaben im Webformular verifizieren und missbräuchliche Anmeldungen und Änderungen weitgehend verhindern.

7. Entwicklungen und Empfehlungen im Bereich der Technik

7.1 Datenschutzgerechter Einsatz von Voice over IP in der Landesverwaltung; Projekt HessenVoice

In das Projekt HessenVoice wurde ich schon frühzeitig eingebunden. Ziel ist es, für die hessische Landesverwaltung datenschutzgerecht eine zukunftssichere, zentrale Telekommunikationsstruktur mit der Technik "Voice over IP" aufzubauen. Diese erlaubt es, das Hessische Verwaltungsnetz (HessenNetz) neben der Datenkommunikation auch für die Sprachübertragung zu nutzen. Erste Teilprojekte wurden in den fünf Standorten erfolgreich realisiert. Bei einem zukünftig angedachten flächendeckenden Einsatz müssen aber weiterhin Datenschutzaspekte berücksichtigt werden, die eine Verschlüsselung erfordern können.

7.1.1 Sachstand

Bereits in meinem 34. Tätigkeitsbericht habe ich mich mit der Thematik der Sprachübertragung in Internetprotokoll basierten Netzen (Voice over IP, VoIP) beschäftigt.
Zum damaligen Zeitpunkt im Jahr 2005 wurde in der Landesverwaltung als Basis für die Einführung von VoIP eine Bestandsdatenerfassung zu den vorhandenen Telekommunikationsanlagen durchgeführt. Die Ergebnisse dieser Erhebung sind die Planungsgrundlagen für das heutige Projekt. Es ist langfristig vorgesehen, sukzessive die althergebrachten Telekommunikations-Anlagen abzulösen. Mit dem Projekt HessenVoice wird das Ziel verfolgt, den Dienststellen der Landesverwaltung über eine zentrale Telekommunikationsinfrastruktur Telefoniedienste bereitzustellen, diese zu standardisieren und zentral durch die HZD zu betreiben. HessenVoice nutzt hierfür die Technik Voice over IP (VoIP). Diese Technologie erlaubt es, das nach außen aufwendig abgeschottete, sichere Hessische Verwaltungsnetz neben der Datenkommunikation unter Wahrung der gebotenen Trennung auch für die Sprachübermittlung zu nutzen.

Nach ersten Pilotprojekten in den Finanzämtern Kassel, Nidda und Frankfurt werden zwei große Teilprojekte bis Ende 2009 realisiert.

7.1.1.1 Justiz- und Verwaltungszentrum

Im November 2009 wird in Wiesbaden von sechs Justiz-Dienststellen das neu erstellte Gebäude Justiz- und Verwaltungszentrum (JuVZ) bezogen. Die in diesem Gebäude vom Land Hessen für den Anteil Justizzentrum bereitgestellte Lösung basiert auf den im Projekt HessenVoice angebotenen Voice-Services.

Mit der VoIP-Technologie wurden im JuVZ die 840 Telefone über LAN angeschlossen und Kommunikationslösungen zur Verfügung gestellt, die über zentral für die Hessische Verwaltung implementierte Komponenten gewährleistet werden. Die betroffenen Dienststellen Arbeitsgericht, Verwaltungsgericht, Landgericht, Amtsgericht, Staatsanwaltschaften und Sozialgericht bleiben in der Verwaltung und Vor-Ort-Betreuung autark, jedoch werden Leistungen wie Amtszugang, Anschluss an das HessenNetz und Vermittlungsplatzfunktion gemeinsam genutzt. Beim JuVZ Wiesbaden kommt die neue Rufnummer 0611-32-61xxxx zum Einsatz. Die Rufnummer 32-xxxxxx ist als künftige Rufnummer aller Dienststellen der Hessischen Landesverwaltung in Wiesbaden vorgesehen.

7.1.1.2 Oberfinanzdirektion Frankfurt

Im Dezember 2009 zieht die Oberfinanzdirektion (OFD) Frankfurt am Main mit Sitz in der Adickesallee in den Gebäudekomplex OFD Main Triangel um. Dort bezieht die OFD das Forum und Etagen im Hochhaus des Gebäudekomplexes. 500 Anschlüsse werden hier in gleicher Weise wie im Justiz- und Verwaltungszentrum mit VoIP-Technologie realisiert.

7.1.2 Datenschutzrechtliche Bewertung

7.1.2.1 Allgemeines

Der HDSB wurde schon frühzeitig - im Jahr 2008 - in das Projekt HessenVoice einbezogen, um datenschutzrechtliche Belange sowohl in rechtlicher wie in technischer Sicht von Anfang an zu berücksichtigen. Dabei wurden im Berichtszeitraum im Wesentlichen Details der Vorabkontrolle zur Vorbereitung des Verfahrens nach § 34 Abs. 5 HDSG diskutiert.

Die gegenwärtige datenschutzrechtliche Bewertung stützt sich auf die vorgelegte Vorabkontrolle (Version 04.02 vom 18. November 2009), den Entwurf eines Verfahrensverzeichnisses (Stand 27. August 2009), den Entwurf des Revisionskonzeptes sowie die Ergebnisse der Gespräche mit Herrn Staatssekretär Westerfeld und den Mitarbeitern der Abteilung VII des HMDIS.

7.1.2.2 Vorabkontrolle und Verfahrensverzeichnis

Die Vorabkontrolle ist umfassend und beinhaltet folgende Punkte:

- die Festlegung der Daten verarbeitenden Stellen,
- den Vorschlag von Regelungen zur Privattelefonie,

- die Zweckbestimmung des Verfahrens,
- die Art der gespeicherten Daten und den Kreis der Betroffenen,
- die Rechte der Betroffenen,
- die Systemkonfiguration und Arbeitsabläufe,
- eine Risikobetrachtung: Beschreibung der Gefährdungen durch die neue Technologie und Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit.

Nach einer Beurteilung der vorgelegten Vorabkontrolle und des Standes der ergänzenden Konzeptpapiere wird die als Ergebnis der Vorabkontrolle zunächst getroffene Wertung, dass die mit VoIP verbundenen datenschutzrechtlichen Gefahren durch die geplanten Konzepte angemessen abgefangen werden, von mir mitgetragen.

Neben vielen Detailfragen wie zur Netzstruktur, der Administration, der Verkehrslenkung oder einer unter Umständen notwendigen Speicherung von Verkehrsdaten zu Abrechnungszwecken wurde insbesondere geprüft, ob eine Verschlüsselung der Signalisierungs- bzw. der Sprachdaten bei den ersten Teilprojekten zwingend notwendig ist.

Für die zunächst selbständigen Projekte mit ihren begrenzten Netzstrukturen kann unter strengen Voraussetzungen auf eine Verschlüsselung verzichtet werden. Inwieweit es jedoch bei der Komplexität der zu erwartenden Gesamtstruktur gelingen kann, für HessenVoice unter Verzicht auf die Verschlüsselungsoptionen einen dauerhaft sicheren Betrieb zu gewährleisten, muss zukünftig geprüft werden. Um eine ausreichende Sicherheit jetzt zu erreichen, muss

- die konsequente Trennung der verschiedenen Datenströme technisch und organisatorisch vollständig gewährleistet werden,
- die Manipulation aller aktiven Netzkomponenten, insbesondere der Switche für die VoIP-Endgeräte, unter allen Umständen ausgeschlossen sein und
- es dürfen nur zugelassene Endgeräte in definierten Konfigurationen an das Netzwerk angeschlossen werden.

7.1.2.3 Notwendige Konzepte

Der grundsätzliche Aufbau und die Zielsetzung des Revisionskonzeptes wurden mit mir abgestimmt. Der Entwurf stellt derzeit alle Möglichkeiten des Zugriffs und der Aktivitäten im Betrieb dar. Alle für die Revision relevanten Parameter sind wie die Revisionsprozesse insgesamt noch festzulegen. Den im vorangegangen Absatz genannten Kernforderungen für einen sicheren Betrieb ist bei der Ausgestaltung des Betriebs- bzw. Administrationskonzeptes in geeigneter Weise Rechnung zu tragen. Bis zum Start des Echtbetriebes der nächsten Teilprojekte müssen die relevanten Teile der Konzepte fertiggestellt sein.

7.1.2.4 Gespräche

In den Gesprächen wurden die Ergebnisse der Pilotprojekte erläutert und bewertet.

Der wesentliche offene Punkt bleibt, ob die Verschlüsselung der Gesprächs- und Signalisierungsdaten ggf. auch selektiv eingesetzt werden muss, um dem Schutzbedarf der Daten hinreichend Rechnung zu tragen. Ich halte die Option weiterhin für erforderlich. Sofern sie als Stand der Technik zur Verfügung steht und mit verhältnismäßigem Aufwand realisiert werden kann, ist sie einzusetzen. Dies entspricht auch der Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. Oktober 2005 in Lübeck: "Telefonieren mit Internettechnologie (Voice over IP - VoIP)"; s. 34. Tätigkeitsbericht, Ziff. 10.9.

Bei der Einführung von HessenVoice wird vorerst im "Justizzentrum Wiesbaden" und in der "OFD" auf eine Verschlüsselung der entsprechenden Datenströme verzichtet. Bei allen anstehenden Beschaffungen bzw. Ausschreibungen von neuen Systemen muss aber darauf geachtet werden, dass der Einsatz der Verschlüsselungsoption zu einem späteren Zeitpunkt problemlos möglich ist.

7.1.3 Ausblick

Wenn die Realisierung in der beschriebenen Form erfolgt, und auch die Beteiligung des HDSB und damit die Berücksichtigung von Datenschutzgesichtspunkten weiterhin sichergestellt wird, kann das Projekt unter datenschutzrechtlichen Aspekten befürwortet werden.

7.2 Einsatz von USB-Sticks

USB-Sticks sind als Speichermedien weit verbreitet, um Daten zu transportieren. Sie werden zunehmend auch benutzt, um Programme und ganze Systemumgebungen mit sich zu führen und auf fremden Computern eine eigene, bekannte Arbeitsumgebung einstellen zu können. Diese Möglichkeit bietet eine Reihe sinnvoller Einsatzzwecke, die aber mit Anforderungen an die technische Ausgestaltung verbunden sind.

7.2.1 Der USB-Stick als PC-Ersatz

In der hessischen Landesverwaltung aber auch in Kommunen ergibt sich immer wieder der Wunsch oder die Notwendigkeit von Telearbeitsplätzen. Wünschenswert ist es, dass dazu Dienstgeräte zur Verfügung gestellt werden. Da oft zu wenig Geld zur Verfügung steht, wird über Lösungen nachgedacht, die kostengünstiger sind. In vielen Fällen wären private Rechner vorhanden, aber deren Nutzung weist aus Datenschutz- und Datensicherheitsgründen große Risiken auf. Als neuer Ansatz

wird über bootfähige USB-Sticks oder Boot-CDs nachgedacht, die mit vertretbaren Kosten einen Privat-PC für die Dauer der Arbeit zu einer Art dienstlichen Rechner machen. Diesen Gedankengang möchte ich an mehreren Beispielen erläutern.

7.2.1.1 Die Idee

Damit außerhalb der Dienststelle dienstliche Daten problemlos verarbeitet werden können, müssen einige Rahmenbedingungen erfüllt werden.

- Der Rechner muss während der Verarbeitung der Daten allein dem Bediensteten zur Verfügung stehen.
- Dritte dürfen keinen Zugriff auf gespeicherte Daten erhalten.
- Die Daten müssen bei einer Datenübertragung oder während des Transports vor einer unbefugten Kenntnisnahme geschützt sein.

Falls der Bedienstete einen Dienstrechner erhält, können diese Bedingungen durch technische und organisatorische Maßnahmen erfüllt werden. Es muss eine Anweisung geben, dass nur der Mitarbeiter den Dienstrechner benutzen darf. Wenn ein passendes Betriebssystem gewählt ist, kann eine sichere Anmeldung erreicht werden. Zusammen mit einer Festplattenverschlüsselung ist eine unbefugte Kenntnisnahme der gespeicherten Daten weitgehend ausgeschlossen. Bei einem Dienstrechner werden auch die zugelassenen Programme installiert. Damit ist die Gefahr durch Schadprogramme kontrollierbar. Außerdem kann eine Softwareumgebung vorgegeben werden, die eine sichere, verschlüsselte Datenübertragung gewährleistet.

Wenn ein privater PC genutzt wird, sind die Anforderungen nur schwer oder gar nicht umzusetzen. Hinsichtlich der Forderung, dass der Rechner dem Bediensteten während der Verarbeitung allein zur Verfügung steht, gibt es keinen Unterschied zu einem Dienstrechner. Im Regelfall kann aber unterstellt werden, dass später auch andere Personen damit arbeiten. Diese könnten auf gespeicherte Daten zugreifen. Man muss davon ausgehen, dass viele andere Programme installiert sind; diese könnten beabsichtigt oder ungewollt beispielsweise Schadprogramme wie Viren oder Trojaner sein. Damit akzeptable Bedingungen vorhanden sind, müsste der Mitarbeiter den eigenen PC so administrieren, dass Unbefugte weitgehend weder direkt noch indirekt auf die Daten zugreifen können. Dieser Zustand ist schon bei einer professionellen Administration schwer herstellbar. Umso seltener trifft es bei privaten PCs zu.

Der Gedanke ist nun, den Rechner durch Programme von einem Speichermedium zu starten ("booten"), die der Arbeitgeber zur Verfügung stellt. Es sollen zwar der Hauptspeicher, die Tastatur, der Bildschirm und die Maus genutzt werden, aber auf der Festplatte vorhandene Programme wie das Betriebssystem sollen außen vor bleiben und der Plattenspeicher soll ebenfalls möglichst nicht angesprochen werden. Damit könnte ein privater PC für die Dauer der Arbeit bezüglich der Programme und Daten zu einem rein dienstlichen Rechner werden.

Während bei älteren Rechnern neben der Festplatte als Bootmedium Disketten oder CDs ausgewählt werden können, kann es bei neueren Rechnern auch ein USB-Stick sein. Wegen ihrer geringen Speicherkapazität sind Disketten aber praktisch nicht mehr in Gebrauch. CDs und DVDs sind als Bootmedium geeignet. Jedoch gibt es Probleme, wenn nachträglich Daten geändert oder gespeichert werden sollen. Hier hat ein USB-Stick Vorteile.

7.2.1.2 Der Telearbeitsplatz

Eine hessische Kommune hat für Telearbeitsplätze eine Grundstruktur auf Basis eines Terminalservers in Kombination mit einem bootfähigen USB-Stick gewählt. Dabei werden vom Telearbeitsplatz Tastatureingaben und die Mausbewegung an den Server übertragen, während zum Telearbeitsplatz Bildschirminhalte gesendet werden. Es findet keine Übertragung von Dateien statt. Nachdem sich der Mitarbeiter am Terminalserver angemeldet hat, kann er mit seinen Fachanwendungen wie im Büro arbeiten.

Für die Telearbeit bei dieser Kommune sollen lokal keine Dateien gespeichert werden, so dass die Funktion "Dateien auf den PC herunterladen" auf dem Terminalserver ausgeschaltet ist.

Es bleiben noch folgende Anforderungen umzusetzen:

- Die Daten müssen sicher übertragen werden.
- Der Benutzer muss sicher identifiziert werden.

Die sichere Übertragung wird durch folgende Maßnahmen erreicht: Auf einem USB-Stick wird ein Betriebssystem und weitere Software installiert. Die Software stellt sicher, dass nur mit einem bestimmten Server unter einer fest vorgegebenen Internetadresse (IP-Adresse) verschlüsselt kommuniziert werden kann. Außerdem wird zwischen dem Server und dem PC mittels eines Challenge-Response-Verfahrens ein VPN (virtual private network) aufgebaut, das in diesem Fall eine verschlüsselte Datenübertragung beinhaltet. Das Verfahren basiert auf Zertifikaten. Es arbeitet mit einem geheimen und dem öffentlichen Schlüssel, der im Zertifikat hinterlegt ist. Jeder USB-Stick wird mit einem eigenen, eindeutigen Zertifikat ausgeliefert. Falls der USB-Stick verlorengeht, kann das zugehörige Zertifikat gesperrt werden. Nach der Sperrung ist es nicht mehr möglich, sich mit diesem Stick am Terminalserver anzumelden. Die Daten können somit im VPN sicher übertragen werden.

Nachdem der VPN-Tunnel aufgebaut ist, meldet sich der Mitarbeiter mit seiner Benutzerkennung und einem Passwort am Terminalserver an. Anschließend kann er wie gewohnt arbeiten. Durch diese Anmeldung und die vorgeschaltete Prüfung der Zertifikate ist der Benutzer sicher identifiziert.

Da die Softwareumgebung vom USB-Stick gebootet wird, können auf dem PC bereits vorhandene Schadprogramme weder das Zertifikat kopieren noch Passwörter mitschneiden. Da auch keine Dateien auf dem PC verbleiben, sind die Sicherheitsrisiken so weit reduziert, dass auch ein Privat-PC für die Telearbeit genutzt werden kann.

7.2.1.3 Erstellen sonderpädagogischer Gutachten am Privat-PC

Rund 60.000 Lehrer dürfen nach der neuen Rechtsverordnung (s.a. Kapitel 4.5.1) in Hessen personenbezogene Daten auf ihren privaten Rechnern verarbeiten. Die Verantwortung für die Verarbeitung der Daten verbleibt aber bei der Schule. Der Datensatz ist in Anlage 6 abschließend beschrieben (Der vollständige Datensatz ist unter den Materialien meiner neu erschienenen Broschüre "Datenschutz in Schulen" abgedruckt; sie ist im Internet unter http://www.datenschutz.hessen.de/downloads/173 abrufbar). Hierbei handelt es sich zum einen um Daten mit normalem Schutzbedarf (Anlage 6, Ziff. 1 bis 13) wie z.B. Name, Geburtsname, Vorname etc.; zum anderen um Daten mit hohem Schutzbedarf (Anlage 6, Ziff. 14) wie medizinische und psychologische Informationen, die in den sog. sonderpädagogischen Gutachten benötigt werden.

Im häuslichen Umfeld des Lehrers sind je nach Schutzbedarf unterschiedliche Verfahrensweisen erforderlich.

Für die Verarbeitung der Schüler- und Elterndaten mit normalem Schutzbedarf habe ich mich mit dem HKM auf folgende Vorgehensweise verständigt:
Die Lehrer speichern die Daten auf einen normalen USB-Stick, der einen verschlüsselten Container beinhaltet. Auf der Homepage der staatlichen Schulämter wird eine Software zum Verschlüsseln mit Installationshilfe angeboten. Einzelheiten zu den Rahmendingungen sind auf meiner Homepage unter der Rubrik Fachthemen Schule im Artikel "Verarbeitung von Lehrer- und Schülerdaten auf den privaten Datenverarbeitungseinrichtungen der Lehrer" beschrieben.

Für die sonderpädagogischen Gutachten reicht diese Vorgehensweise wegen der Sensitivität der Daten und der hohen Fallzahlen nicht aus. Denn Hessen ist in der Betreuung und Förderung von Schülern nach Aussage des HKM deutschlandweit führend. So wurden allein im letzten Jahr rund 20.000 Schüler betreut, die Zahl ist steigend.

Die Erstellung eines solchen Gutachtens erstreckt sich über einen längeren Zeitraum. Hier dürfen Informationen zur Anamnese des Schülers in seiner Familie, zur Vorgeschichte, zum Lernverhalten, zur sprachlichen und körperlichen Entwicklung, zum emotionalen und sozialen Verhalten und Weiteres verarbeitet werden. Leider stehen dienstliche Geräte aus Kostengründen in dem erforderlichen Umfang für die Lehrer nicht zur Verfügung. Um den Lehrern aber dennoch ein datenschutzrechtlich zulässiges Arbeiten zu Hause mit moderner Technik zu ermöglichen und gleichzeitig dem hohen Schutzbedarf der gespeicherten Informationen Rechnung zu tragen, habe ich mich mit der Thematik eines bootfähigen USB-Sticks beschäftigt.

Eine Lösung könnte idealerweise wie folgt aussehen:
Der USB-Stick ist mit einem bootfähigen Betriebssystem und einem verschlüsselten Container zur Speicherung der Gutachten während der Bearbeitung ausgestattet.

Der Zugriff auf den entschlüsselten Container ist nur nach dem Bootvorgang und einer Anmeldung an dem jetzt zur Verfügung stehenden System möglich. Das Gutachten kann nur vom zuständigen Lehrer auf diesem Wege angelegt und bearbeitet werden.

Nach der Fertigstellung, die über einen längeren Zeitraum erfolgen kann, ist das Gutachten nur in der Schule an einem dafür vorgesehenen Arbeitsplatz auszudrucken und danach zu löschen. Aus diesem Grund muss der USB-Stick über einen weiteren, direkt (ohne vom Stick zu booten) zugänglichen Speicherbereich verfügen. Das Gutachten, dass während der Bearbeitung entschlüsselt im Container liegt, muss nun jeweils schulspezifisch mit einem weiteren Schlüssel, dem öffentlichen Schlüssel der Schule verschlüsselt werden und in den allgemein zugänglichen Bereich, den Transferbereich, kopiert werden. Für den Transport von zu Hause in die Schule befindet sich nun das Gutachten verschlüsselt in dem Transferbereich. Da der private Schlüssel der Schule nicht bekannt ist, kann niemand drittes, auch der Lehrer nicht, die Datei entschlüsseln. Im Schulsekretariat wird die verschlüsselte Datei aus dem allgemein zugänglichen Bereich des USB-Sticks auf den dafür vorgesehenen Verwaltungsrechner übertragen und mit dem passenden privaten Schlüssel der Schule entschlüsselt. Danach ist das Gutachten nur noch auszudrucken und alle Informationen sind, wie in der Rechtsverordnung beschrieben, sowohl auf dem Stick als auch auf dem Rechner zu löschen.

7.2.1.4 Feuerwehr

Wie unter Ziff. 5.7.1 beschrieben, wird für Feuerwehren, die "Florix-Hessen" nutzen, derzeit eine USB-Lösung mit einem portablen Browser angeboten. Diesen Ansatz betrachte ich als eine Übergangslösung. Sinnvollerweise sollten Dienst-PC beschafft werden. Kurz- und mittelfristig stehen hierfür aber wohl keine Mittel zur Verfügung, so dass ich auch in diesem Fall in einem entsprechend konfigurierten bootfähigen USB-Stick eine mögliche Alternative sehe.

7.2.2 Der USB-Stick als Speichermedium

In diesem Jahr hat mich die Landesärztekammer Hessen um eine Stellungnahme zu einem Produkt gebeten, das in einem Ärztenetz in Nordhessen eingesetzt werden sollte. Als Datenträger für medizinische Daten dient in diesem Fall ein USB-Stick, auf dem sich neben den verschlüsselt gespeicherten Daten auch Programme zur Verwaltung dieser Daten befinden.

Der reguläre Zugriff auf die Daten wurde durch die auf dem USB-Stick vorhandenen Programme gesteuert, die für Notfälle den Zugriff auf einen Teil der Daten ermöglichen.

In der Stellungnahme habe ich zahlreiche rechtliche und technische Aspekte thematisiert. Sie differenziert u.a. zwischen dem Einsatz eines USB-Sticks auf Reisen und für den vorübergehenden Transport von Befunden. Die dauerhafte Speicherung einer Krankenakte auf einem USB-Stick war nicht Gegenstand meiner Stellungnahme.

Meine Stellungnahme habe ich gegenüber der Landesärztekammer abgegeben. Dort können ggf. Details erfragt werden.

7.3 Public-Key-Infrastrukturen (PKI) für Bürger - technische Anforderungen an die Standards

Damit PKI-Funktionen sicher genutzt werden können, muss ihre jeweilige Verwendung in allen Anwendungen sachgerecht, transparent und eindeutig sein. Die PKI-Funktionen dürfen nicht inhaltlich vertauscht werden und es muss eine strikte Trennung der Funktionen gegeben sein. Der Hessische Datenschutzbeauftragte hatte sich in die Überarbeitung des Standards "COMMON-PKI" zur Version 2 eingeschaltet, um entsprechende Verbesserungen zu erreichen.

Es ist für eine sichere und transparente Nutzung unverzichtbar, sowohl die jeweils richtige, also die inhaltlich-logisch zutreffende der drei Funktionen Authentisierung, Signatur und Verschlüsselung zu verwenden als auch diese Funktionen sauber auseinanderzuhalten. Ersteres geschieht auf der Anwendungsebene, Letzteres erfordert eine entsprechende technische Unterstützung. Allgemein verbindliche Regelungen werden mit Hilfe von Normen und Standards getroffen, spezielle für konkrete Verfahren oder Anwendungen in Sicherheitsleitlinien, sogenannten Policies.

7.3.1 Regelungen in Normen und Standards

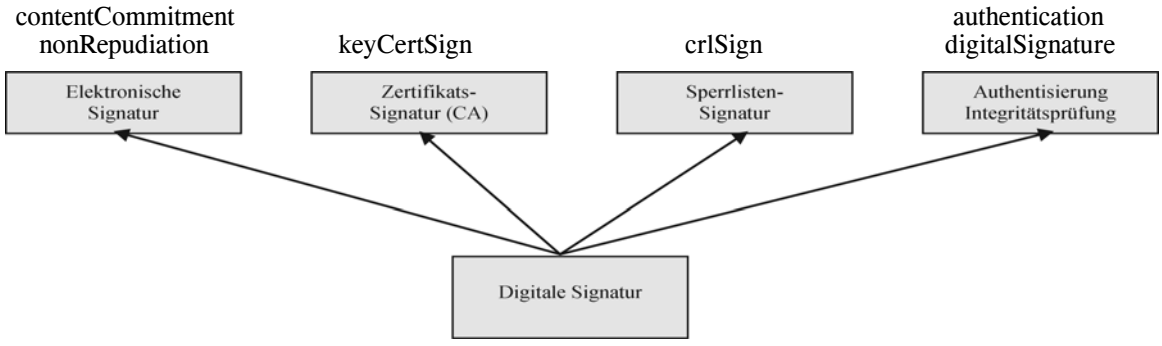
Im Bereich Public-Key-Infrastrukturen relevante Standards sind der US-amerikanische RFC 5280, die deutsche COMMON-PKI, die in Englisch geschrieben ist und eine europäische bzw. internationale Geltung und Akzeptanz anstrebt, sowie der Telekommunikations-Standard X.509 der internationalen Fernmeldeunion ITU.
Auf dieser "unteren", technischen Ebene finden wir für Authentisierung und elektronische Signatur eine identische technische Vorgehensweise, nämlich das Bilden eines Hashwertes und dessen anschließende Verschlüsselung mit dem privaten Authentisierungs- bzw. Signatur-Schlüssel. Das E-Government-Glossar des BSI E-Government-Handbuchs definiert:

Digitale Signatur

Sicherungsmechanismus für elektronische Daten, bei dem aus der Information mittels eines geheimen Schlüssels (und kryptografischer Verfahren) ein Wert erzeugt wird, der mithilfe eines zugehörigen öffentlichen Schlüssels verifiziert werden kann.
(Klammerzusatz von HDSB).

Diese Definition ist wichtig für das Problemverständnis auf der Anwendungsebene, wie die Abbildung zeigt:

Key Usage Feld im Zertifikat (Anwendung)



Technische Ebene

Die digitale Signatur auf der technischen Ebene wird für verschiedene Funktionen auf der Anwendungsebene genutzt und erhält hierfür im Key Usage Feld des Schlüssel-Zertifikates unterschiedliche Einträge:

- für die elektronische Signatur von Dokumenten "nonRepudiation" (RFC 5280, COMMON-PKI Version 1) bzw. "contentCommitment" (Common-PKI Version 2, X.509 V3),
- für die Signatur von Zertifikaten "keyCertSign",
- für die Signatur von Sperrlisten "crlSign",
- für die Authentisierung, Integritätsprüfung und ggf. andere Nicht-Signatur-Anwendungen "digitalSignature" (RFC 5280, COMMON-PKI, X.509 V3).

7.3.2 Beispiel Common-PKI Version 2

Unter den Aspekten des Daten- und des Verbraucherschutzes hat sich meine Mitarbeiterin an der Erarbeitung der COMMON-PKI Version 2 beteiligt, um hier eine strikte Funktionstrennung zu erreichen und irreführende Bezeichnungen zu ändern:

7.3.2.1 Bezeichnungen

7.3.2.1.1 Content Commitment statt Non Repudiation

Bei der elektronischen Signatur geht es - im Gegensatz zur Signatur von Zertifikaten oder Sperrlisten - immer um Dokumente:
- um die Authentifizierung des Unterzeichners bzw. der Unterzeichnerin des Dokuments und
- um die Integrität, also die Unverfälschtheit des Inhalts des Dokumentes, der wesentlich und keineswegs beliebig ist - im Gegensatz beispielsweise zu Zufallszahlen bei einem Authentisierungsverfahren - und deswegen auch vor dem Signieren zuverlässig angezeigt werden soll.

Nur die qualifizierte elektronische Signatur an einem Dokument erfüllt die höheren Anforderungen, die rechtlich mit dem Schriftformerfordernis bei Papierdokumenten gleichwertig sind. Aber auch bei fortgeschrittenen (AES) und einfachen elektronischen Signaturen geht es um den nicht mehr unbemerkt veränderbaren oder austauschbaren Inhalt, also um "content commitment", was eine stärkere und klarere Aussage ist als "non repudiation".

Dem Vorschlag, dieses Feld in der Common PKI entsprechend umzubenennen, wurde gefolgt, zumal X.509 V3 diese Umbenennung schon vorgenommen hatte.

7.3.2.1.2 Authentication statt Digital Signature

Die Funktion "Authentisierung und Integritätsprüfung" heißt in allen drei Standards "digitalSignature". Diese Bezeichnung ist unter zwei Aspekten missverständlich:

- Zum einen wegen der Verwechslung mit der technischen Ebene, die ja englisch auch "digital signature" heißt und somit leicht zu einer grundsätzlichen Verwechslung der Ebenen führt.
- Zum anderen, weil damit auf der Anwendungsebene über den Begriff "digitalSignature" leicht ein (inhaltlicher) Bezug zur elektronischen Signatur assoziiert wird, der bei der Authentisierung aber gerade nicht gegeben ist. Für die notwendige inhaltliche Trennung der beiden Funktionen ist diese irreführende Bezeichnung fatal.

Eine Lösung dieses Problems wäre die Umbenennung von "digitalSignature" in "authentication". Obwohl selbst in der Diskussion innerhalb der Expertenrunde der COMMON-PKI diese Verwechslungen mehrfach auftraten, wurde dieser Vorschlag meiner Mitarbeiterin nicht aufgegriffen, weil man nicht von der Bezeichnung in den anderen Standards abweichen wollte. Bisher hat weder X.509 V3 noch RFC 5280 eine klarstellende Änderung vorgenommen.

Die in diesem Zusammenhang aufgestellte Behauptung, es handle sich um einen rein technischen Standard, alles andere müsse man jeweils auf der Anwendungsebene regeln, kann nicht befriedigen: Es handelt sich zwar um einen technischen Standard, dieser legt aber auch die Begriffe auf der Anwendungsebene fest. Gerade deshalb ist es notwendig, dass die Begriffe für Experten und für Bürgerinnen und Bürger klar, eindeutig und unmissverständlich sind.

7.3.2.2 Funktionstrennung

Auf die Ausführungen des Datenschutzes zur Funktionstrennung hin wurden viele, teilsweise recht ausführliche Kommentierungen in den Standard eingefügt, die die Gefahren und sogar rechtliche Konsequenzen konkret benennen. So wird darauf hingewiesen, dass den Nutzenden die Zustimmung zum Inhalt (content commitment) zugerechnet wird, wenn sowohl "contentCommitment" als auch "digitalSignature" im KeyUsage Feld des Zertifikats gesetzt sind. Die Nutzenden sind also gut beraten, wenn sie eine Mischung der Funktionen für ihre eigenen Schlüssel sowohl im beruflichen als auch im privaten Umfeld strikt ablehnen, damit sie sich nicht in einem Verfahren authentifizieren, bei dem der Hashwert mit dem eines später vorgelegten, ihnen unbekannten Dokumentes übereinstimmt. Die Nutzenden werden nachträglich kaum beweisen können, dass sie nicht ein Dokument signiert (bzw. technisch: seinen Hashwert verschlüsselt), sondern sich lediglich authentisiert haben. Da das Zertifikat aber sowohl Signatur als auch Authentisierung zulässt, wird ihnen im Zweifelsfall der Inhalt des Dokuments zugerechnet. Das bedeutet, dass sie die gleichen Rechtsfolgen tragen müssen, die sich ergeben würden, wenn sie das ausgedruckte Dokument unterschrieben hätten.

Die neuen Kommentierungen bleiben alle auf der Stufe der Empfehlungen (RECOMMENDED, SHOULD) stehen. Da diese Empfehlungen nicht von allen Herstellern umgesetzt werden, ist so aber eine Lösung dieses Problems nicht erreichbar.

Es muss stattdessen absehbar zu einer Verpflichtung (MANDATORY, MUST bzw. FORBIDDEN, MUST NOT) kommen. Dabei ist ein zweistufiges Vorgehen möglich:

- zunächst kann man die Funktionstrennung für die Ausgabe neuer Zertifikate verbindlich machen und
- ca. drei bis fünf Jahre später auch für die Prüfung der Zertifikate.

Damit wäre ein sanfter Übergang geschaffen, der die Gültigkeit bisher ausgegebener Zertifikate während ihrer Laufzeit nicht infrage stellt und somit die Betreiber und Anwender von Public-Key-Infrastrukturen nicht unter Zeit- oder Kostendruck setzt.
Wichtig ist es allerdings, hier zeitnah aktiv zu werden, bevor ein medienwirksamer Fall der Funktionsvermischung dazu führt, dass die Bürgerinnen und Bürger aus berechtigter Sorge und Angst vor den für sie unkalkulierbaren Folgen die Nutzung beider Funktionen grundsätzlich verweigern.
Insofern ist zu hoffen, dass der Standard "COMMON-PKI Specifications for Interoperable Applications", die Interoperabilität der Anwendungen nicht langfristig oder gar dauerhaft über die Forderung nach Transparenz und Sicherheit für die Bürgerinnen und Bürger stellt.

7.3.3 Regelungen in Policies

Selbstverständlich kann man entsprechende Festlegungen auch in Policies treffen. Dies bleibt aber insofern immer eine Notlösung, als man damit keine übergreifende, also über die jeweils einzelne Anwendung hinausgehende Verbindlichkeit und Interoperabilität erreichen kann. Auch dann nicht, wenn für alle Anwendungen Policies zur Verfügung stünden. Vielmehr müssten Betroffene bei allen ihren Kommunikationsbeziehungen in die Zertifikate ihrer Partner schauen und die zugehörigen Policies aufmerksam lesen. Selbst dann wären die Verfahren immer noch weder sicher noch transparent und erst recht nicht benutzerfreundlich. Und auch mit umfangreichem Fachwissen und entsprechendem Aufwand wird ein Nutzender nicht zuverlässig feststellen können, ob eine strikte Funktionstrennung gegeben ist. Denn es gibt inzwischen Chipkarten, bei denen zu einem Schlüsselpaar jeweils bis zu drei verschiedene Zertifikate gespeichert werden können; also beispielsweise eines zur Authentisierung, eines für die elektronische Signatur und eines zur Verschlüsselung. Damit wäre das evtl. im Kontext mitgelieferte bzw. das geprüfte Zertifikat bezüglich der Funktion zwar eindeutig, eine Funktionstrennung aber dennoch nicht gegeben und ein Missbrauch zu Lasten selbst von IT-Spezialisten weiterhin möglich. Hier ist grundsätzlich zu fragen bzw. festzulegen, wie die PKI-Software mit diesen neuen Gegebenheiten umgeht und umgehen soll.

Transparenz und Sicherheit auf der Anwendungsebene können für die Betroffenen mit automatisiert prüfbaren Policies für Web-Anwendungen wenigstens teilweise erreicht werden. Dies ist eine Forderung der Datenschutzbeauftragten, beispielsweise im Rahmen der Entwicklung des Transport-Protokolls OSCI Transport 2, das im Bereich der öffentlichen Verwaltung eingesetzt werden soll. Damit könnten zukünftig sowohl Nutzende in ihrem Browser als auch Verfahren wie z.B. Web-Anwendungen festlegen, was sie von ihrem Kommunikationspartner bzw. (Web)Service verlangen. Abweichungen könnten dann angezeigt und die Verarbeitung nur mit Zustimmung der Nutzenden fortgesetzt werden.

7.3.4 Positive Ansätze

Die Forderung des Datenschutzes nach strikter Funktionstrennung wurde für OSCI-Transport 2 bereits in die "Funktionale[n] Anforderungen und Entwurfsziele" aufgenommen. Initiiert wurde dies von meiner Mitarbeiterin in einer gemeinsamen Arbeitsgruppe des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit den Entwicklern von OSCI Transport.

7.3.5 Weiterer Handlungsbedarf

Wichtig ist eine klare Regelung auf der Ebene der Normen und Standards. Die Verwendung eindeutiger, unmissverständlicher Begriffe und die saubere Trennung der Funktionen sind für die Transparenz und Sicherheit der Verfahren und die Nutzbarkeit der Authentisierungs- und der Signaturfunktion unabdingbare Voraussetzung.
Diese Anforderungen sollten auch bei den im Aktionsplan (s. Ziff. 7.4) genannten Maßnahmen vorrangig umgesetzt werden. Dies gilt insbesondere für den geplanten europäischen Signaturstandard.

7.4 Aktionsplan der EU-Kommission für elektronische Signaturen

Der "Aktionsplan für elektronische Signaturen und die elektronische Identifizierung zur Förderung grenzübergreifender öffentlicher Dienste im Binnenmarkt" führt neben der qualifizierten elektronischen Signatur als weiteren Begriff die "auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Signatur" neu ein. Diese soll offenbar EU-weit als Alternative zur qualifizierten Signatur verwendet werden. Da dieses Vorgehen problematisch ist, wird ein Vorschlag für eine sinnvolle Alternative aufgezeigt.

7.4.1 Ein neuer Signaturbegriff: AES-QC

In dem Aktionsplan für elektronische Signaturen und die elektronische Identifizierung zur Förderung grenzübergreifender öffentlicher Dienste im Binnenmarkt werden zwei Signaturbegriffe definiert und betrachtet:

1. Zum einen die qualifizierte elektronische Signatur (QES), die bisher schon im deutschen Signaturgesetz (SigG) definiert war. In der EU-Signaturrichtlinie (EU-SRL) ist dieser Begriff in Artikel 5 Abs. 1 zwar auch enthalten, er wurde aber nicht mit einer eigenen Bezeichnung versehen. Dies führt immer wieder zu der falschen Aussage, dass die EU-SRL keine qualifizierte elektronische Signatur kenne.

2. Zum anderen wird erstmals die "auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Signatur (AES-QC)" definiert und betrachtet. AES-QC sind fortgeschrittene elektronische Signaturen (AES, Advanced Electronic Signatures) mit einem qualifizierten Zertifikat (QC, Qualified Certificate). Sie sind wie QES, die ohne sichere Signaturerstellungseinheit (SSCD, Secure Signature Creation Device) erstellt wurden. Auch für sie gelten die von

den Mitgliedsstaaten zu gewährleistenden Haftungsregelungen des Artikels 6 der EU Signaturrichtlinie (EU-SRL) für den Zertifizierungsdiensteanbieter.
In Deutschland gibt es nur qualifizierte elektronische Signaturen mit qualifiziertem Zertifikat (QC), keine AES-QC.

7.4.2 Rechtlicher Unterschied

Nach deutschem Recht (§ 126a BGB, § 3a Abs. 2 VwVfG) kann nur die qualifizierte elektronische Signatur die manuelle Unterschrift und deren Rechtsverbindlichkeit ersetzen. Für den Bereich der EU ist in Artikel 5 Abs. 1 EU-SRL eine entsprechende Regelung getroffen und weiter festgelegt, dass die QES als Beweismittel in Gerichtsverfahren zugelassen sind.
Die AES-QC kann also, da sie nicht mit einer sicheren Signaturerstellungseinheit erstellt wird, weder nach deutschen noch nach europäischem Recht die Schriftform ersetzen.
Artikel 6 EU-SRL regelt die Haftung eines Zertifizierungsdiensteanbieters (ZDA), "der ein Zertifikat als qualifiziertes Zertifikat öffentlich ausstellt oder für ein derartiges Zertifikat öffentlich einsteht" dafür,

- dass zum Zeitpunkt seiner Ausstellung die Angaben im Zertifikat vollständig und richtig sind und der Signaturschlüssel-Inhaber/Unterzeichner im Besitz der zugehörigen Signaturerstellungsdaten war,
- für den Fall, dass der Widerruf des Zertifikats nicht registriert worden ist

es sei denn, der ZDA weist nach, dass er nicht fahrlässig gehandelt hat.

Der ZDA kann darüber hinaus Beschränkungen für die Verwendung des Zertifikates und Grenzen für den Wert von Transaktionen angeben, für die das Zertifikat verwendet werden kann. Sofern diese Einschränkungen für Dritte erkennbar sind, haftet der ZDA nur innerhalb dieser Einschränkungen.

Diese Haftungsregelung gilt gleichermaßen für AES-QC und QES. Streitigkeiten werden aber selten die korrekte Ausstellung oder die Registrierung eines Widerrufs des Zertifikats betreffen. In der Mehrzahl der Fälle wird die oder der Signierende nach der Ausstellung des Zertifikats bestreiten, das konkrete Dokument signiert zu haben. Dies geschieht unabhängig davon, ob die Signaturumgebung oder der Umgang der Signierenden mit ihren Signaturmitteln den Sicherheits-Anforderungen entspricht oder nicht.

In all diesen Fällen hilft die Haftungsregelung dem Empfangenden nicht. Er wird im Rechtsstreit kaum Gegenbeweise zu Aussagen des oder der Signierenden führen können. Einzig wenn das Dokument mit einer qualifizierten elektronischen Signatur nach deutschem Recht versehen ist, hilft den Empfangenden im Rechtsstreit die Beweislastumkehr. Der Absendende muss dann nachweisen, dass er das Dokument nicht signiert hat: Das wird ihm kaum gelingen.

7.4.3 Prüfbarkeit verschiedener Signatur-Qualitäten

Technisch ist außerdem festzustellen, dass es kein Verfahren gibt, mit dem geprüft und festgestellt werden kann, ob eine elektronische Signatur nur "einfach" ist oder ob sie die vier zusätzlichen Anforderungen an eine fortgeschrittene elektronische Signatur erfüllt. Nach Art. 2 Nr. 2 EU-SRL und § 2 Nr. 2 SigG ist eine elektronische Signatur nur fortgeschritten, wenn sie

a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist,
b) die Identifizierung des Signaturschlüssel-Inhabers ermöglicht,
c) mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Die mangelnde Prüfungsmöglichkeit, ob eine einfache oder fortgeschrittene Signatur gegeben ist, liegt wesentlich an der Unmöglichkeit, als Empfangender nachzuprüfen, ob die Signatur mit Mitteln erzeugt wird, die der Inhaber unter seiner alleinigen Kontrolle hat (s. o. Buchstabe c) der Anforderungen). Wenn nun eine sichere Signaturerstellungseinheit verwendet wird, ist zwar Buchstabe c) immer noch nicht bewiesen, er kann aber in diesem Fall mit einer ähnlichen Berechtigung bzw. Wahrscheinlichkeit wie bei der QES unterstellt werden, weil der private Signaturschlüssel aus der SSCD nicht gestohlen oder ausgelesen werden kann. Daher kann man - wenn man genau wie bei der QES unterstellt, dass evtl. weitere Einschränkungen und Voraussetzungen des Signatursoftware-Herstellers und des IT-Grundschutzes, insbesondere für das Passwort, beachtet werden - von einer fortgeschrittenen elektronischen Signatur (AES) ausgehen.

Die Verwendung einer sicheren Signaturerstellungseinheit kann außerdem von der Stelle, die das Zertifikat herausgibt, problemlos bestätigt werden. Hierfür gibt es technisch mindestens zwei verschiedene Möglichkeiten:

- Der Herausgeber kann die Bestätigung in die zugehörige Policy aufnehmen.
- Es ließe sich beispielsweise ein SSCD-Bit in das vom Herausgeber signierte Zertifikat einfügen.

Besonders unter diesen Qualitäts- und Nachprüfbarkeitsaspekten, aber auch unter dem Aspekt, dass die Haftungsregelungen den Empfangenden nicht die Sicherheit bringen, die sie benötigen, sind fortgeschrittene elektronische Signaturen, die mit einer sicheren Signaturerstellungseinheit erstellt werden, also AES-SSCD, den AES-QC eindeutig vorzuziehen.

Solche Signaturen können u.a. von der Verwaltungs-PKI des Bundes und den darunterliegenden Zertifizierungsinstanzen (CAs, Certification Authorities), auch der teilnehmenden Bundesländer, ausgegeben werden. Die Hessen-PKI nutzt diese Möglichkeit bereits. Diese Signaturen entsprechen der höchsten Qualitätsstufe (Stufe 3) der in Entwicklung befindlichen

neuen Policy der Verwaltungs-PKI des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dies wäre damit für Zertifikate, die ab 2010 nach dieser Policy herausgegeben werden sollen, auch automatisiert nachprüfbar.

	QES	AES-QC	V-PKI neue Policy Stufe 3	prüfbar?
AES	X	X	X	Nein
QC	X	X		Ja, QC-Bit
SSCD	X		X	Ja *

*= wenn Herausgeber Schlüssel-Speicherung auf SSCD bestätigt

Abbildung 1: Funktionsumfang und Prüfbarkeit der verschiedenen fortgeschrittenen Signaturarten

7.4.4 Prüfung von Signaturen an Dokumenten

Deutschland prüft qualifiziert signierte Dokumente gemäß § 2 Nr. 3a) SigG auf den Zeitpunkt der Erstellung und weicht damit - von der EU genehmigt - von der Empfehlung in Anhang IV der EU-SRL ab, um eine wichtige Analogie zur manuellen Unterschrift auf die elektronische Signatur zu übertragen: dass nämlich die Unterschrift ab dem Zeitpunkt der Unterzeichnung unbefristet gilt.

Sinnvoll ist dies für alle Dokumentsignaturen, unabhängig von ihrer Qualität, also gleichgültig ob sie qualifiziert, fortgeschritten oder einfach sind. Das ist derzeit bei der Prüfung fortgeschrittener und einfacher Signaturen auch in Deutschland nicht der Fall: Hier wird auf den Zeitpunkt der Prüfung geprüft, was spätestens beim Ablauf des Signaturzertifikates, wegen des Schalenmodells (s. 36. Tätigkeitsbericht, Ziff. 8.1.1.2) bei Ungültigkeit eines der ausstellenden Zertifikate evtl. auch schon früher, zum Prüfergebnis "ungültig" führt.

Für die Verwaltungs-PKI des Bundes, unter der auch die Hessen-PKI als eigene CA betrieben wird, ist eine entsprechende Änderung - Prüfung der Gültigkeit von Signaturen auf den Zeitpunkt der Erstellung - für die nächste Fassung der Policy, die 2010 in Kraft treten soll, vorgesehen. Hersteller von Komponenten zur Signaturprüfung sind gut beraten, ihre Verfahren so bald wie möglich auf diese Anforderung anzupassen. Sie ist keineswegs neu. In § 15 Abs. 2 Nr. 2 b der Signaturverordnung (SigV) ist die Formulierung schon immer enthalten:

§ 15 Absatz 2 Nr. 2 b SigV:

Signaturanwendungskomponenten … müssen gewährleisten, dass
1. …
2 bei der Prüfung einer qualifizierten elektronischen Signatur …
a) …
b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

7.4.5 Nationale Interessen koordinieren und einbringen

In Deutschland fehlt bisher eine offene nationale Diskussion zwischen allen Betroffenen und Interessierten. Auch eine Koordination und Vertretung der deutschen Interessen im Rahmen des Aktionsplanes erscheint dringend erforderlich. Dieser Plan wird auch Konsequenzen für die Ausgestaltung des Einheitlichen Ansprechpartners im Rahmen der EU-Dienstleistungsrichtlinie haben.

Für den geplanten europäischen Signaturstandard ist eine engagierte, qualifizierte und koordinierte Mitarbeit von deutscher Seite dringend erforderlich. Insbesondere vor dem Hintergrund, dass inzwischen auch andere europäische Staaten die Intention der abweichenden deutschen Regelungen nachvollziehen können und gutheißen.
Die Aktivitäten sollten den Inhalt der Ziffern 7.4.2 und 7.4.3 ebenso umfassen wie das zur Verwendung eindeutiger, unmissverständlicher Begriffe und der sauberen Trennung der Funktionen auf der Ebene von Normen und Standards unter Ziff. 7.3 Gesagte.

Der Hessische Datenschutzbeauftragte ist im Rahmen seiner Möglichkeiten gerne zur Unterstützung und Mitarbeit bereit. Die Koordination sollte von einer geeigneten Stelle des Bundes wie z.B. dem Beauftragten der Bundesregierung für Informationstechnik oder dem Bundeswirtschaftsministerium übernommen werden und alle entsprechenden betroffenen und interessierten Stellen beim Bund und in den Bundesländern einbeziehen.

7.5 Zertifizierungen

In Rahmen meiner Prüfung und Beratung werden mir immer wieder Zertifizierungen auf der Basis von Normen und Standards vorgelegt. Um Missverständnisse bei der Beurteilung der Aussage eines Zertifikates zu vermeiden ist es wichtig,

Gegenstand und Ziel der Zertifizierung zu berücksichtigen. Es ist ein großer Unterschied, ob das Management der IT-Sicherheit einer Institution oder eines abgegrenzten Teiles einer Institution zertifiziert wird, oder die in einer konkreten Hard- oder Software implementierten Sicherheitsmaßnahmen.

7.5.1 Zertifizierung des Managements der IT-Sicherheit

7.5.1.1 Gegenstand einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz

Gegenstand einer ISO 27001-Zertifizierung ist das Management der IT-Sicherheit.

Die internationale Norm ISO 27001 spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Die Norm wurde auch als DIN-Norm veröffentlicht. Sie spezifiziert Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen, welche an die Gegebenheiten der einzelnen Organisationen adaptiert werden sollen. Die ISO 27001 wurde entworfen, um die Auswahl geeigneter Sicherheitsmechanismen zum Schutze sämtlicher Unternehmenswerte (Assets) in der Wertschöpfungskette sicherzustellen.

Der Zusatz "auf der Basis von IT-Grundschutz" bedeutet, dass die erforderlichen Standard-Sicherheitsmaßnahmen, die gegen die verschiedenen Gefährdungen getroffen werden, aus den umfangreichen Grundschutzkatalogen des BSI zusammengestellt und umgesetzt werden.

7.5.1.2 Zertifizierungsverfahren und Bedeutung

Voraussetzung für die Vergabe dieses Zertifikates ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Zu dessen Aufgaben gehören eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Die Zertifizierungsstelle BSI stellt aufgrund des Audit-Reports fest, ob die notwendigen Sicherheitsmaßnahmen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es.

In den Grundschutzkatalogen gibt es fünf verschiedene Schichten: die Bausteingruppen "Übergeordnete Aspekte", "Infrastruktur", "IT-Systeme", "Netze" und "Anwendungen". Für die Prüfung wird aus jeder dieser fünf Schichten jeweils ein Baustein nach dem Zufallsprinzip ausgewählt. Darüber hinaus wählt der Auditor gezielt einige Bausteine aus und nimmt ggf. Stichproben aus der Ergänzenden Risikoanalyse.

Unter dem Begriff "Anwendung" werden beim IT-Grundschutz, und folglich auch bei der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz, nicht - wie sonst üblich - einzelne konkrete Anwendungsprogramme oder Verfahren verstanden und betrachtet, sondern die Schicht "Anwendungen" enthält Bausteine, die bestimmte Dienste oder Funktionen bereitstellen, wie z.B. Webserver, Datenbanken, Mobile Datenträger, Allgemeiner Verzeichnisdienst, Telearbeit oder Datenträgeraustausch. Für jede dieser "Anwendungen", wie im Übrigen auch für alle Bausteine der anderen Schichten, sind in den Grundschutzkatalogen die typischen Gefährdungslagen dargestellt und Maßnahmeempfehlungen gegeben, die für die Zertifizierung umgesetzt sein müssen.

Die Bedeutung des Verfahrens ergibt sich daraus, dass bei ISO 27001 die Geschäftsprozesse dominieren und nicht die IT-Sicherheit. Das Ergebnis der Zertifizierung ist die Bestätigung, dass das Management der Informationssicherheit den Anforderungen genügt im Sinne des sog. PDCA-Verfahrens, einem ständigen Kreislauf von Plan-Do-Check-Act (Plane - Setze um - Prüfe - Reagiere auf Abweichungen). Deshalb wird die Zertifizierung jährlich mit den inzwischen erfolgten Änderungen aktualisiert und nach Ablauf von drei Jahren wieder komplett neu durchgeführt.

Voraussetzung für eine solche Zertifizierung ist u.a., dass aktuelle Dokumentationen, Konzepte und Sicherheitsrichtlinien vorliegen, dass Änderungen regelmäßig eingearbeitet werden, dass Rollenkonzepte, Aufgabenverteilungen, Vertretungsregelungen und Notfallpläne umgesetzt sind und regelmäßig Schulungen der Mitarbeiter stattfinden. Besonders wichtig ist eine klare persönliche Verantwortung für die verbleibenden Restrisiken.

7.5.2 Zertifizierung der IT-Sicherheitseigenschaften von Software oder Systemen

7.5.2.1 Common Criteria und Schutzprofile

Die Common Criteria (CC, Gemeinsame Kriterien) sind eine mehrteilige Norm, die als Grundlage für die Prüfung und Bewertung der Sicherheitseigenschaften von Produkten und Systemen der Informationstechnik (IT) dient. Die aktuelle Version CC 3.1 ist bei der Internationalen Standardisierungsorganisation (ISO) zur Standardisierung eingereicht und löst die für Zertifizierungen nicht mehr aktuelle Version CC 2.3 ab, die als ISO/IEC 15408:2005 zum internationalen Standard wurde.

Die CC schaffen Vergleichbarkeit bezüglich der Ergebnisse unabhängiger Prüfungen und Bewertungen der Sicherheit des sog. Evaluationsgegenstandes (EVG). Sie dienen als Richtschnur für die Entwicklung von Produkten oder Systemen mit IT-Sicherheitsfunktionen sowie bei der Beschaffung von handelsüblichen Produkten oder Systemen mit solchen Funktionen.

Die CC eignen sich ferner zur Spezifikation von Sicherheitsvorgaben. Für grundsätzliche Anforderungen, die an die Sicherheit bestimmter Arten von Produkten gestellt werden und die in Ausschreibungen gefordert und von Herstellern umgesetzt werden sollen, können auch sog. Schutzprofile (PP, Protection Profiles) auf der Basis der CC erstellt werden.

Ein PP definiert eine implementierungsunabhängige Menge von IT-Sicherheitsanforderungen an eine Kategorie von EVG [Evaluationsgegenständen]. Solche EVG sollen weit verbreitete Bedürfnisse von Anwendern nach IT-Sicherheit befriedigen. Anwender können daher durch Erstellung eines PP oder Verweis auf ein solches ihre IT-Sicherheitsbedürfnisse ausdrücken, ohne Bezug auf einen konkreten EVG zu nehmen.
(Common Criteria Teil I, Anhang B)

Es gibt z.B. ein Schutzprofil zur Videoüberwachung, das auch datenschutzrechtliche Anforderungen berücksichtigt, sowie zwei Profile zur "Benutzerbestimmbaren Informationsflusskontrolle", deren Grundlagen von einer Arbeitsgruppe des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten erarbeitet wurden. Die Entwicklung dieser Profile wurde von Mitarbeiterinnen meines Hauses unterstützt und begleitet.

7.5.2.2 Gegenstand der Zertifizierung nach den CC

Die CC gelten für in Hardware, Firmware oder Software implementierte Sicherheitsmaßnahmen.
Die CC befassen sich mit dem Schutz von Informationen vor nicht autorisierter Preisgabe, Modifizierung oder Zugangsverlust. Sie können aber auch auf andere Aspekte von IT-Sicherheit angewendet werden, die nicht unter diese Schutzkategorien der Vertraulichkeit, Integrität oder Verfügbarkeit fallen. Die CC gelten aber nicht für die Bewertung inhaltlicher Qualitäten von kryptografischen Algorithmen. Wenn diese erforderlich ist, muss das Evaluationsschema eine solche Bewertung explizit vorsehen.

7.5.2.3 Zertifizierungsverfahren und Bedeutung

In Deutschland ist das BSI für die Zertifizierung nach den CC zuständig. Von ihm zugelassene Evaluatoren verwenden die in den CC enthaltenen Kriterien, um die Übereinstimmung eines EVG mit den Sicherheitsanforderungen zu beurteilen. Das BSI überprüft das von dem Evaluator erstellte Gutachten und zertifiziert ggf. den EVG.

Die Bedeutung der CC reicht weit über Deutschland hinaus: Es gibt derzeit weltweit 13 Länder, die mit einer eigenen Zertifizierungsstelle Produkte nach den CC zertifizieren, und zwölf weitere, die solche Zertifikate nutzen. Ferner gibt es ein Abkommen, mit dem diese 25 Länder ihre Zertifizierungen nach den CC gegenseitig anerkennen. Eine Zertifizierung nach den CC durch eines der Länder gilt damit auch in den anderen, ohne dass das Verfahren dort jeweils neu durchlaufen wird.

7.5.3 Beispiel ELSTER

Für die Abgabe von Steuer-Voranmeldungen und -Erklärungen wird am ELSTER-Online-Portal nach wie vor ein Authentisierungsverfahren anstelle einer qualifizierten elektronischen Signatur als Äquivalent zur eigenhändigen Unterschrift im manuellen Verfahren genutzt. Da das konkret eingesetzte Verfahren in einigen Punkten die Mechanismenstärke "maximal niedrig" hat, handelt es sich auch nicht um ein "starkes" Authentisierungsverfahren. Denn die Stärke eines Mechanismus richtet sich nach derjenigen der schwächsten Komponente (Minimum-Prinzip). Dies ist unmittelbar einleuchtend, weil Angreifer natürlich immer an den Schwachstellen angreifen.

Darüber hinaus authentisiert das Verfahren nicht die Steuerpflichtigen, die die Steuerklärung oder -voranmeldung abgeben müssen, sondern lediglich die Person, die die Erklärung mit ELSTER abschickt. Das kann eine beliebige andere Person sein.

Neuerdings argumentiert die Steuerverwaltung, dass "die ELSTER-Anwendungen (inkl. RA-Dienst), Systeme, Räume und Sicherheitsmanagementprozesse für ihre Clearingstellen nach ISO 27001 auf der Basis der Grundschutzkataloge zertifiziert" seien und "erklärtermaßen auch dem hohen bis sehr hohen Schutzbedarf" genügten.

Dies ist in mehrfacher Hinsicht irreführend:
Zunächst einmal bedeutet eine ISO 27001-Zertifizierung nicht, dass das Verfahren ELSTER als solches oder einzelne seiner Komponenten geprüft und zertifiziert wurden, sondern, wie unter Ziff. 7.5.1.1 dargelegt wurde, dass das IT-Sicherheitsmanagement mit seinen fünf Schichten, die als Bausteine auch Systeme und Räume umfassen, geprüft wurde.

Eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz besagt, dass das IT-Sicherheitsmanagement-Verfahren eingerichtet ist und dass der IT-Grundschutz - soweit das vom Auditor stichprobenartig geprüft wurde - umgesetzt ist. Selbst wenn darüber hinausgehende, zusätzlich erforderliche Risikoanalysen und deren Umsetzung in die Prüfung mit einbezogen wurden, wird weder attestiert, dass das IT-Sicherheitsmanagement noch dass die ELSTER-Anwendungssoftware oder Teile von ihr "erklärtermaßen auch dem hohen bis sehr hohen Schutzbedarf" genügen. Der Auditor hat bezüglich des Schutzbedarfs lediglich geprüft, ob die von ELSTER vorgelegte Definition der Schutzbedarfskategorien plausibel ist.

Eine Aussage darüber, ob oder dass die ELSTER-Anwendungssoftware oder Teile von ihr dem hohen bis sehr hohen Schutzbedarf genügen, kann ausschließlich mit einer Zertifizierung nach den CC getroffen werden. Auch die unterschiedlichen Meinungen zur Qualität des Verfahrens ließen sich mit einer Zertifizierung des Verfahrens und seiner Sicherheitseigenschaften nach den CC zuverlässig und eindeutig klären. Dabei würden die getroffenen Maßnahmen mit den Sicherheitsanforderungen verglichen, und insbesondere festgestellt, ob sie überhaupt zielführend sind.

Da die CC keine Bewertung der Qualität der kryptografischen Algorithmen und Parameter vornehmen, bietet sich als Alternative der Algorithmenkatalog gemäß der Signaturverordnung an. Dieser Katalog wird vom BSI jährlich nach Beratung

mit Experten fortgeschrieben. Die Anforderungen an die Algorithmen und Parameter entsprechen bei ELSTER nicht dem Algorithmenkatalog. Für die Steuerkontoabfrage ist das unter Datenschutzaspekten nicht akzeptabel. Für die anderen ELSTER-Anwendungen sind klare Übergangsfristen wünschenswert.

Für ein Webportal im Internet, das allen Bürgern zur Verfügung steht, ist eine Zertifizierung von ELSTER nach CC als vertrauensbildende Maßnahme sinnvoll und wünschenswert. Spätestens dann, wenn die Bürger zur Nutzung des Verfahrens verpflichtet werden sollen, ist sie meiner Meinung nach als Nachweis der Sicherheit des Verfahrens erforderlich.

7.6 Orientierungshilfen des Arbeitskreises Technik

Mit aktuellen Orientierungshilfen gibt der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (AK-Technik) immer wieder Handreichungen zu technischen Fragestellungen heraus. In diesem Jahr wurden drei Themen aufgegriffen.

Der AK-Technik bereitet aktuelle datenschutzrelevante technische Fragestellungen in Orientierungshilfen auf. Mit den Orientierungshilfen leistet er einen Beitrag zum datenschutzgerechten Einsatz von IT-Technik. Dieses Jahr wurde die Orientierungshilfe "Protokollierung" neugefasst und die Orientierungshilfen "Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb" sowie "Biometrische Authentisierung - Möglichkeiten und Grenzen" erstmalig veröffentlicht.

Die Orientierungshilfe "Protokollierung" aus dem Jahr 1995 wurde durch eine Neufassung ersetzt. Die generellen Gesichtspunkte aus der alten Orientierungshilfe sind noch gültig, aber der Bezug zur heute verfügbaren Technik war nicht mehr ohne Weiteres herstellbar. Es war auch nicht beschrieben, wie die Anforderungen bei der heute verfügbaren Technik umgesetzt werden können. Vor diesem Hintergrund wurde die Orientierungshilfe komplett überarbeitet. Sie geht nun auf den Zweck und die Anforderungen an eine Protokollierung ein, stellt Arten von Protokolldaten dar, behandelt die Qualität der Protokolldaten und erläutert Aspekte bei der Implementierung. Der Text ist in diesem Tätigkeitsbericht im Anhang unter Ziff. 10.1 zu finden.

Die neue Orientierungshilfe "Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb" geht besonders auf die Frage ein, ob und wann Echtdaten zu Testzwecken genutzt werden dürfen. Sie beschreibt die verschiedenen Ausprägungen eines Tests im Projektbetrieb und legt die Unterschiede zwischen Pilot- und Regelbetrieb dar. Die Orientierungshilfe finden Sie ebenfalls im Anhang unter Ziff. 10.2.

Die Anmeldung an einen Rechner, die sog. Authentisierung, geschieht meist noch dergestalt, dass ein Benutzer seine Kennung und sein Passwort eingibt. Da die Kennung und das Passwort auch durch andere Personen eingegeben werden können, wird oft als wesentlich bessere Technik die biometrische Authentisierung betrachtet. Hierbei wird der Benutzer an einem biometrischen Merkmal erkannt. In der Orientierungshilfe "Biometrische Authentisierung - Möglichkeiten und Grenzen" werden Grundlagen der Biometrie beschrieben, aber eben auch die Möglichkeiten und die - heutigen - Grenzen dieser Technik. Sie finden die Orientierungshilfe unter Ziff. 10.3.

8. Bilanz

8.1 Neuregelung der Aufbewahrungsfristen in den Gesundheitsämtern (36. Tätigkeitsbericht, Ziff. 5.8.4.3)

In meinem 36. Tätigkeitsbericht hatte ich u.a. auf unzureichende oder fehlende Aufbewahrungsbestimmungen für die Lagerung personenbezogener, medizinischer Unterlagen in den Gesundheitsämtern hingewiesen.

Ein Kontakt mit dem Gesundheitsamt ist praktisch für jeden Bürger unumgänglich: Schuleingangsuntersuchung, amtsärztliche Begutachtungen für öffentliche oder private Arbeitgeber bzw. Sozialbehörden oder die Sammlung von Leichenschauscheinen, um nur einige Bereiche zu benennen. Die beim Gesundheitsamt gespeicherten Daten sind vielfältiger Natur. Regelungen für die Aufbewahrung dieser Daten waren bislang jedoch allenfalls fragmentarisch oder fehlten ganz. So gab es für die Speicherung der Leichenschauscheine bislang keine bereichsspezifischen Regelungen. Meine im 36. Tätigkeitsbericht formulierte Kritik hat die Gesundheitsämter veranlasst, eine Arbeitsgruppe einzurichten, um mit meiner Beteiligung für die personenbezogenen medizinischen Unterlagen konkrete Speicherfristen festzulegen:

- So werden Leichenschauscheine künftig über einen Zeitraum von 30 Jahren aufbewahrt.
- Die Daten amtsärztlicher Untersuchungen werden für zehn Jahre im Aktenbestand belassen.
- Auch für Meldungen oder Belehrungen nach dem Infektionsschutzgesetz, die Dokumentation der Sprachheilbeauftragten und der Prüfungsunterlagen der Heilpraktikerprüfungen, um nur einige weitere Unterlagen zu nennen, wurden in der Regel zehnjährige Aufbewahrungsfristen festgelegt. Damit orientiert man sich nun vornehmlich an den Maßgaben aus der Ärztlichen Berufsordnung, die nach § 10 Abs. 3 eine Aufbewahrungsfrist für ärztliche Unterlagen von zehn Jahren vorsieht.

Die festgelegten Speicherfristen sollen in einem Erlass allgemeinverbindlich für den öffentlichen Gesundheitsdienst festgelegt werden.

Ausgeklammert sind die Daten des Sozialpsychiatrischen Dienstes. Diese Organisationseinheit innerhalb der Gesundheitsämter nimmt zum Teil Aufgaben der freiwilligen Beratung von psychisch in einer Notsituation befindlichen Hilfesuchenden wahr, wird andererseits aber auch auf Veranlassung anderer Behörden amtlich tätig. In diesem Zusammenhang bedarf es

weiterer Erörterungen, um sowohl datenschutzrechtlichen Belangen als auch erforderlichen Aufbewahrungsregelungen Rechnung zu tragen.

8.2 Optische Archivierung: Abschluss der Auftragsdatenverarbeitung durch den MDK Sachsen-Anhalt (36. Tätigkeitsbericht, Ziff. 5.8.5)

Im Jahr 2004 hatte der Medizinische Dienst der Krankenversicherung in Hessen ein umfangreiches und hinsichtlich seines Volumens in Hessen wohl einmaliges Auftragsdatenverarbeitungs-Projekt angestoßen. Dabei ging es um die Auflösung der Papierarchive der Versichertenakten in den Geschäftsstellen des MDK Hessen, deren Verlagerung und Zentralisierung beim MDK Sachsen-Anhalt in Magdeburg sowie Scan-Dienstleistungen (optische Archivierung) im Zusammenhang mit der Anforderung eingelagerter Unterlagen durch den MDK Hessen. Mehr als 800.000 Versichertenakten wurden nach Magdeburg verbracht und vom MDK Sachsen-Anhalt in einem ausgelagerten, zentralen Archiv aufbewahrt.

In Anbetracht der Bedeutung dieses Datenverarbeitungs-Projekts habe ich die datenschutzrechtlichen Aspekte der länderübergreifenden Zusammenarbeit intensiv begleitet. Dazu gehörte nicht nur eine umfangreiche rechtliche Beleuchtung der zwischen den beiden MDKs geschlossenen Verträge und das Hinwirken auf Korrekturen, da wo diese erforderlich waren. Auch war ein Mitarbeiter von mir mehrfach vor Ort in Magdeburg, um sich vom ordnungsgemäßen Verfahren der Auftragsdatenverarbeitung zu überzeugen. Über die Ergebnisse habe ich in meinem 33. Tätigkeitsbericht (Ziff. 5.8.2), im 34. Tätigkeitsbericht (Ziff. 5.8.7) und im 36. Tätigkeitsbericht (Ziff. 5.8.5) ausführlich berichtet.
Die im Rahmen der umfangreichen Prüfungstätigkeit festgestellten Mängel z.B. hinsichtlich der Verschlüsselung der Daten bei der Übermittlung von Magdeburg nach Oberursel zum dortigen zentralen Server des MDK Hessen oder dem Standort des für die Datenübertragung vorgesehen Servers in Magdeburg wurden schnell behoben. Gravierende, das Projekt in Frage stellende Defizite konnten nicht festgestellt werden.

Nach gut fünf Jahren seit dem Abschluss des Vertrages wurde das Archiv in Magdeburg im Januar 2009 aufgelöst. Dies ergab sich auch, weil z.B. Pflegegutachten, die einen wesentlichen Bestandteil des Archivgutes ausmachten, einer Aufbewahrungsfrist von fünf Jahren unterliegen und dann ohnehin zur Vernichtung anstanden. Dieser Prozess, einerseits Akten auf Anforderung zu scannen und nach Hessen zu übermitteln und anderseits stetig die Aufbewahrungsfristen der Akten zu überprüfen und ggf. zu vernichten, führte schließlich zum Abschluss des Datenverarbeitungsprojektes.

8.3 Prüfung der Datenübermittlungen zwischen Kliniken und MVZ (37. Tätigkeitsbericht, Ziff. 4.7.4)

Im 37. Tätigkeitsbericht hatte ich über verschiedene Rechtsfragen im Zusammenhang mit MVZ berichtet. Ich hatte zunächst die rechtlichen Voraussetzungen einer Übermittlung von Patientendaten zwischen Kliniken und MVZ dargelegt. Seitens der LÄK und der KV Hessen wurden keine Einwände gegen die dargelegten Rechtspositionen geäußert. Das Präsidium der LÄK hat 2009 beschlossen, diesen Beitrag auf der Internetseite der LÄK zu veröffentlichen, um die Ärzteschaft im Hinblick auf den Datenschutz noch weiter zu sensibilisieren. Mein Tätigkeitsbeitrag ist dort abrufbar unter http://www.laekh.de/front_content.php?idart=1781.

Ein weiteres Thema dieses Tätigkeitsbeitrags war die Ausgestaltung der Zugriffsmöglichkeiten auf Patientendaten innerhalb eines MVZ. Zu diesem Thema besteht weiterhin Diskussionsbedarf (s. Ziff. 4.6.4).

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

9.1 Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. Februar 2009

Stärkung der IT-Sicherheit - aber nicht zu Lasten des Datenschutzes

Das Bundeskabinett hat am 14. Januar 2009 den Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen (BRDrucks. 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Weiter sollen aber zugleich auch das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) geändert werden.

Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Entsprechende Ansätze gibt es nun auch in der Bundesverwaltung. So sieht der Gesetzentwurf vor, dem BSI sehr weitgehende Befugnisse einzuräumen. Kritisch sind insbesondere

1. die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten (§ 5),
2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und

3. die fehlende Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor zu (erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

Äußerst bedenklich ist darüber hinaus die Regelung, dass im Zweifelsfall allein das Bundesministerium des Innern entscheiden darf, ob Daten dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind und wie damit weiter zu verfahren ist (§ 5 Abs. 6). In solchen Zweifelsfällen sollten diese Daten gelöscht oder einem Richter zur Entscheidung vorgelegt werden.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau nur mit datenschutzgerechten Lösungen gewährleistet wird. Die Datenschutzbeauftragten fordern strengere Sicherheitsstandards und soweit möglich die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss revisionssicher ausgestaltet werden. Der vorgelegte Gesetzentwurf enthält keine solchen Regelungen.

Die Gesetzesänderung des Telemediengesetzes böte öffentlichen und privaten Anbietern von Telemedien die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer im Internet, da sie entsprechend der Gesetzesbegründung weit auslegbar ist. Der Gesetzgeber muss unmissverständlich klarstellen, dass die Erhebung und Auswertung personenbezogener Daten ultima ratio ist.

Sowohl die Betreiber der "Netze des Bundes" als auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu gewährleisten.

9.2 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2009

Defizite beim Datenschutz jetzt beseitigen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.

2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.

3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

9.3 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2008

Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Dateien bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16. Dezember 2008 (Az.: 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei "Gewalttäter Sport" bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitung statt findenden polizeilichen Datenverarbeitung rechtswidrig. Die Datenschutzbeauftragten von Bund und Ländern fordern das Bundesministerium des Innern und die Landesregierung auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

9.4 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2009

Eckpunkte für ein Gesetz zum Beschäftigtendatenschutzgesetz

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.

- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besondere Festlegungen im Hinblick auf Gesundheitsdaten (u.a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen etc.).

- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z.B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.

- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z.B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

- Der Einsatz von Überwachungssystemen, wie z.B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgagen.

- Es bedarf der Festlegung der Rechte der Beschäftigten, z.B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.

- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.

- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.

- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

9.5 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. März 2009

Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem "berechtigten Interesse abhängig", was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte des Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17. Dezember 2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder

appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

9.6 Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. April 2009

Datenschutz beim vorgesehenen Bürgerportal unzureichend

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-Drucks. 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.

- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss - entgegen der Stellungnahme des Bundesrates vom 3.4.2009 - erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen - etwa zur verbindlichen Kommunikation mit staatlichen Stellen - hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und Aufdeckung von Pseudonymen.

- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

9.7 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009

Aktueller Handlungsbedarf beim Datenschutz - Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z.B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;
- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;
- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;
- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;
- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;
- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z.B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;
- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;
- die Videoüberwachung in Staat und Gesellschaft einzuschränken;
- den Schutz der Meldedaten zu verbessern;
- ein praktikables Datenschutzaudit zu schaffen;
- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

9.8 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009

Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weitreichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weitreichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

9.9 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009

Staatsvertrag zum IT-Planungsrat - Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

9.10 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009

"Reality-TV" - keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

"Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige "Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen – wobei auch schon einmal eine Wohnung zwangsgeöffnet wird – oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleiben oder gar ausfällig werden. Aufgrund des Erfolgs derartiger "Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen "Reality"-Reportagen Abstand zu nehmen.

9.11 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009

Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem "Europa der Bürger". Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z.B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.

- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen - auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST - im weiteren Verfahren einzusetzen.

9.12 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2009

Krankenhausinformationssysteme datenschutzgerecht gestalten!

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

10. Orientierungshilfen

10.1 Protokollierung

Herausgegeben vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (gesetzliche Grundlagen sind an die Hessische Rechtslage angepasst) - Stand: 2. November 2009

Inhalt

1. Einleitung

Sowohl die Datenschutzgesetze der Länder als auch das Bundesdatenschutzgesetz enthalten Regelungen, aus denen sich die Pflicht zur Protokollierung ergibt oder zumindest ableiten lässt. In einigen Landesdatenschutzgesetzen findet man das Regelungsziel Revisionsfähigkeit, das insbesondere durch die Maßnahme der Protokollierung umgesetzt werden kann. Das Bundesdatenschutzgesetz (BDSG) und andere Landesdatenschutzgesetze normieren Kontrollziele wie Eingabekontrolle oder Verantwortlichkeitskontrolle, aus denen sich ebenfalls die Pflicht zur Protokollierung ableiten lässt. Im BDSG zeigt sich am Beispiel der Anlage zu § 9, dass praktisch keine der dort konkret aufgeführten technisch-organisatorischen Maßnahmen ohne das Vorsehen einer Nachweismöglichkeit, die typischerweise in Form eines Protokolls geschieht, umsetzbar ist. Für eine Reihe von Verwaltungsverfahren gelten zudem bereichsspezifische, vom Datenschutzrecht des Bundes bzw. des betreffenden Landes abweichende, oft wesentlich konkretere Protokollierungsvorschriften (Beispiele: Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze usw.).

Obwohl die Datenschutzgesetze von Bund und Ländern Regelungen enthalten, aus denen sich die Pflicht zur Protokollierung ableiten lässt, gibt es nur wenige Vorgaben für die konkrete Ausgestaltung der Protokollierung. Dennoch haben sich auf Basis der Anforderungen erprobte Vorgehensweisen entwickelt, die in diesem Text als grundlegende Empfehlungen dargestellt werden.

2. Grundsätze

Die Zweckbindung von Protokolldaten ist in den Datenschutzgesetzen von Bund und Ländern explizit geregelt (z.B. § 31 BDSG oder § 13 Abs. 5 HDSG sowie § 34 Abs. 6 HDSG). Die Protokollierung dient allein dem Zweck der Aufrechterhaltung von Datenschutz und Datensicherheit und darf grundsätzlich nicht für eine automatisierte Verhaltens- und Leistungskontrolle der Beschäftigten genutzt werden.

Alle Protokolldaten unterliegen also einer strikten Zweckbindung. Diese strikte Zweckbindung ist die Konsequenz aus dem Umstand, dass Protokollierungsdaten einen umfassenden Einblick in die Tätigkeiten der Administratoren, Nutzer bzw. Anwender ermöglichen, sie aber auch für die genannten Kontrollzwecke erforderlich sind.
Für die Gestaltung der Protokollierungsverfahren gilt der Grundsatz der Erforderlichkeit. Art, Umfang und Dauer der Protokollierung sind demnach auf das zur Erfüllung des Protokollierungszwecks erforderlichen Maß zu beschränken.

Für die technische Ausgestaltung und Auswahl der Verfahren der Protokollierung ist das Gebot der Datensparsamkeit und Datenvermeidung zu befolgen. Hierbei sind insbesondere die Möglichkeiten zur Pseudonymisierung oder Anonymisierung zu berücksichtigen. Im Falle der Pseudonymisierung ist das Verfahren darzustellen, mit dem die Zuordnung zwischen Person und Pseudonym geregelt ist.

3. Zweck und Anforderungen an eine Protokollierung

Der Zweck der Protokollierung besteht darin, ein Verfahren zur Verarbeitung personenbezogener Daten so transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezoge-

ner Daten nachweisbar ist. Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat.

Entsprechend den allgemeinen Anforderungen an Datensicherheit und Datenschutz - oder allgemeiner: an Beweissicherheit und Revisionsfestigkeit - und der gleichzeitig auszuschließenden automatisierten Leistungs- und Verhaltenskontrolle der an der Datenverarbeitung beteiligten Personen, müssen Protokolldaten mit Personenbezug zweckgebunden, vollständig und datensparsam eingerichtet sein. Sie müssen die tatsächlich erfolgten Operationen, die beteiligten Anwendungen, Maschinen und Personen mit Zeitbezug korrekt dokumentieren. Dabei besteht regelhaft ein Zielwiderspruch zwischen der Vollständigkeit und der Datensparsamkeit. Dieser Konflikt lässt sich nur vor dem Hintergrund der verfahrensspezifischen Bedingungen so weit auflösen, um so einen bestmöglichen Ausgleich der Ziele zu erreichen. Protokolldaten dürfen nicht nachträglich verändert werden können und nur Berechtigten zugänglich sein.

Die ordnungsgemäße Funktion des Protokollierungsverfahrens und die Gültigkeit von Protokolldaten muss durch geeignete Tests sichergestellt werden. Diese sollten ein gezieltes Durchführen von zu protokollierenden Ereignissen und eine darauf folgende Überprüfung, ob diese Ereignisse sich in den Protokolldaten wiederfinden lassen, umfassen. Solche Tests sind immer dann notwendig, wenn die protokollierenden Systeme oder Systemteile verändert werden. Dies gilt insbesondere, wenn die Änderung am System einer datenschutzrechtlichen Freigabe bedarf.

Anforderungen an Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollten mit kryptologischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden.

4. Arten von Protokolldaten

Bei der Protokollierung ist zwischen den Aktivitäten der Maschinen, der Administratoren sowie der Nutzer und Anwender zu unterscheiden. Administratoren können einen besonderen Einfluss auf die Strukturen eines IT-Systems ausüben, weshalb sie bei der Nutzung administrativer Rechte einer besonderen Kontrolle unterliegen. Die Nutzung administrativer Rechte muss zu einem Eintrag im Protokoll führen.

Unter Nutzung administrativer Rechte sind üblicherweise Maßnahmen zur Installation, Modifikation und Konfiguration von Hard- und Software zu verstehen.

Während die Protokollierung der Maschinen und der administrativen Tätigkeiten den Charakter einer Systemüberwachung hat, dient die Protokollierung der Benutzeraktivitäten im Wesentlichen der Verfahrensüberwachung.

Beide Protokollierungsformen dienen dazu, die Ordnungsmäßigkeit der Datenverarbeitung nachzuweisen bzw. auf Anforderung nachweisen zu können.

4.1 Protokollierung administrativer Tätigkeiten

Es müssen die Ereignisse und Tätigkeiten protokolliert werden, die die Funktionsweise der informationstechnischen Geräte sowie der Programme, der Dateien, die Speicherorganisation und die Nutzungsrechte einer automatisierten Verarbeitung personenbezogener Daten verändern.

Dabei ist auch zu beachten, dass die Protokollierung auch explizit zum Schutz der Administratoren vor unberechtigten Vorwürfen hinsichtlich eines möglichen Missbrauchs dienen kann. Ohne eine entsprechende Protokollierung administrativer Tätigkeiten könnten solche Vorwürfe gegen Administratoren nicht nachhaltig entkräftet werden.

Administrationstätigkeiten, wie bspw. die Verwaltung einer Datenbank, müssen unter einer personalisierten Administrationskennung durchgeführt werden, während die restliche nichtadministrative Arbeit mit normalen Benutzerrechten unter der allgemeinen Nutzerprotokollierung erfolgt.

Es muss verhindert werden, dass

- ein ändernder Zugriff auf die Protokolldaten durch diejenigen Personen stattfinden kann, deren Tätigkeiten durch die Protokolldaten dokumentiert werden;
- ein lesender Zugriff auf die Protokolldaten aus anderen Gründen als der Aufrechterhaltung von Datenschutz und Datensicherheit erfolgen kann.

4.2 Protokollierung der Nutzung von IuK-Systemen

Bei der Benutzung von Verfahren zur automatisierten Verarbeitung personenbezogener Daten müssen die Tätigkeiten protokolliert werden, die zum Nachweis einer korrekten, rechtskonformen Verarbeitung notwendig sind.

Die Inhalte der Protokolldaten orientieren sich hierbei an der konkret durchgeführten Datenverarbeitung und am Schutzbedarf der verarbeiteten Daten. Näheres zur inhaltlichen Ausgestaltung findet sich im folgenden Abschnitt.

Üblicherweise müssen die Tätigkeiten der

- Authentifizierung und Autorisierung,
- der Dateneingabe und -veränderung,

- der Dateneinsicht,
- der Datenübermittlung und
- der Datenlöschung

protokolliert werden.

5. Qualität der Protokolldaten

Entsprechend dem Zweck der Protokollierung müssen die in Protokolldaten aufgeführten Aktionen so aggregiert werden können bzw. sein, dass sie der kontrollierenden Instanz helfen, einen Sachverhalt zu rekonstruieren und zu bewerten.

5.1 Inhalt

Protokolldaten müssen Auskunft geben über

- den Zeitpunkt einer Tätigkeit bzw. eines Ereignisses,
- die zutreffende Bezeichnung einer Tätigkeit oder eines Ereignisses,
- die mit der Tätigkeit oder dem Ereignis befasste Person bzw. Systemkomponente und
- den Zweck der Tätigkeit.

Der Zeitpunkt sollte anhand einer zumindest innerhalb der Organisation synchronisierten Zeitquelle bestimmt werden. Art und Weise der Zeitdarstellung müssen eindeutig und zumindest sekundengenau aufgelöst sein.

Die Darstellung der Tätigkeit bzw. des Ereignisses muss eindeutig Auskunft geben, welche Tätigkeit durchgeführt wurde bzw. welche Ereignisse und Operationen auf dem System stattfanden.

Auslöser eines zu protokollierenden Ereignisses ist in der Regel eine Person. Diese muss eindeutig bestimmbar sein. Grundsätzlich sollte die Person deshalb über einen direkt zuordenbaren Bezeichner - beispielsweise durch eine personenbezogene Zugangskennung - benannt werden. Als weitere Auslöser agieren darüber hinaus aber auch Server, Dienste bzw. Services, die automatisiert Protokolldaten erzeugen.

Bei einem Zugriff, bei dem Daten geändert wurden, muss die geänderte Teilmenge klar eingegrenzt benannt werden. Bei datenbankgestützten Systemen erfolgt dies üblicherweise durch Angabe eines oder mehrerer eindeutiger und nichtleerer Feldinhalte - im Allgemeinen Primärschlüssel. Bei einem ändernden Zugriff sollten die Daten vor und nach der Änderung protokolliert werden. Bei datenbankgestützten Systemen geschieht dies üblicherweise durch Benennung der geänderten Datenbankfelder und die Angabe der Feldinhalte vor und nach der Änderung.

Bei einem Zugriff, bei dem Daten nur gelesen wurden, müssen die Daten benannt werden, in die Einsicht genommen wurde. Die Darstellung erfolgt bei datenbankgestützten Systemen üblicherweise durch Angabe des Primärschlüssels und den Bezeichnern der übermittelten Datenfelder.

Der Zweck der Tätigkeit führt viele einzelne Operationen zu einem Vorgang zusammen. So kann beispielsweise das Anlegen eines neuen Benutzers eine Vielzahl von schreibenden und lesenden Zugriffen auf einem System auslösen. Diese einzelnen Operationen müssen dann aggregiert zu Aktionen oder Tätigkeiten zusammengeführt werden können.

5.2 Format

Die Protokolldaten müssen in einem durch gängige Analysewerkzeuge auswertbaren Format vorliegen.

Die Erfahrung hat gezeigt, dass Protokolldaten, die im CSV-Format vorliegen, zusammen mit den frei verfügbaren Tools awk oder grep die operativen Anforderungen an eine maschinell unterstützte Kontrollierbarkeit von Protokolldaten erfüllen. Das CSV-Format fasst üblicherweise einen Protokolleintrag in einer Zeile zusammen. Die Zeile wird in die abgrenzbaren Teilbereiche - beispielsweise Datum, Benutzerkennung, Tätigkeit - durch ein Trennzeichen aufgeteilt. Üblicherweise wird als Trennzeichen das Komma oder Semikolon verwendet. Sollten die Trennzeichen auch innerhalb eines abgrenzbaren Teilbereichs vorkommen, so sollten diese Teilbereiche durch Hochkomma eingeschlossen werden.

6. Technische und organisatorische Aspekte

Bei der Einführung von IuK-Technologie muss der gesamte Lebenszyklus eines Verfahrens betrachtet werden. Dieselbe Anforderung muss deshalb auch an die in diesem Verfahren anfallenden Protokolldaten gestellt werden.

6.1 Erzeugen

Für jedes Verfahren muss in einem Konzept festgelegt werden, welche Tätigkeiten im jeweiligen Verfahren zur Verarbeitung personenbezogener Daten nachzuweisen sind.

Die Notwendigkeit ergibt sich aus

- gesetzlichen Anforderungen,
- Anforderungen aus dem organisationsinternen Datenschutzmanagement und
- Anforderungen aus verbundenen oder übergeordneten Organisationen.

Üblicherweise ergibt sich aus den gesetzlichen Rahmenbedingungen bei vollständig automatisierten Verfahren der Zwang zur Protokollierung ändernder Zugriffe auf personenbezogene Daten.

Eine Protokollierung lesender Zugriffe ist ebenso aus Gründen der datenschutzrechtlichen Revisionssicherheit grundsätzlich erforderlich, insbesondere wenn ein Verfahrensschritt für den Nutzer direkt auf die Ermittlung personenbezogener Daten abzielt. Bei einem hinreichend fein differenzierten Zugriffsschutz kann der Umfang der Protokollierung reduziert werden.

Aufgrund einer Bestandsaufnahme der geltenden Anforderungen muss das Verfahren daraufhin betrachtet werden, welche Tätigkeiten durch Protokolle dokumentiert werden müssen. Für jede Tätigkeit muss der Inhalt der Protokolldaten festgelegt werden. Diese Festlegungen sollten in die Dokumentation des Verfahrens aufgenommen werden.

Die Protokolldaten müssen vollumfängliche Auskunft geben. Jede als relevant eingestufte Tätigkeit muss deshalb zu einem Protokolleintrag führen.

IuK-Systeme, die einen direkten Zugriff auf personenbezogene Daten haben, müssen eine Protokollierung durchführen. Üblicherweise wird der Zugriff auf personenbezogene Daten über ein oder mehrere zentrale Systeme gesteuert. In diesem Fall kann die Protokollierung auf diese Systeme beschränkt werden.

Änderungen an der Konfiguration der Protokollierung müssen einen Eintrag im Protokoll erzeugen.

6.2 Übertragen

Werden Protokolldaten mit Personenbezug und/oder erhöhtem Schutzbedarf über Netze übertragen (z.B. bei zentraler Protokollspeicherung oder entfernter Auswertung), sind zur Wahrung der Vertraulichkeit, Integrität und Authentizität geeignete und für den Schutzbedarf angemessene kryptografische Verfahren nach dem Stand der Technik zu nutzen.

Voraussetzung für eine revisionssichere und datenschutzgerechte Protokollierung ist die vollständige Übertragung der Protokolldaten. Deshalb ist das verbindungsorientierte Transportprotokoll (TCP) dem verbindungslosen Transportprotokoll (UDP) vorzuziehen.

6.3 Speichern

Die Art und der Umfang der Speicherung der Protokolldaten muss festgelegt werden. Wenn eine Tätigkeit protokolliert wird, dann bedeutet dies aber auch, dass genau in diesem Moment der Erzeugung des Protokolldatums auch eine Kontrolle dieser Daten bzw. der Tätigkeiten geschehen kann. Es muss aus Gründen der Datensparsamkeit geprüft werden, ob ein derartiges, sofortiges Überprüfen von Tätigkeiten ohne Speicherung der Daten hinreicht und keine weitere, später erfolgende Kontrollmöglichkeit vorgesehen werden muss.

Die Zugriffsmöglichkeiten auf Protokolldaten sind zu minimieren, insbesondere für die Systemadministratoren, deren Tätigkeiten anhand dieser Protokolldaten kontrollierbar sein müssen. Um dieser speziellen Anforderung, sowie generell den Anforderungen an Datensicherheit und Datenschutz, gerecht werden zu können, sollten Protokolldaten nicht auf den Produktionsmaschinen, sondern auf eigens vorgehaltenen Protokollservern gespeichert werden. Der Zugriff auf diese dedizierten Protokollserver ist entsprechend zu regeln. Ebenso müssen die üblichen Mechanismen zur Datensicherung, wie das Prüfen des Wiederherstellens von Backups, des Lesen- und Verarbeitenkönnens (Hardware, Formate, Zertifikatehandling) auf den Protokollservern umgesetzt sein.

Die Sammlung von Protokolldaten zu einem festgelegten Zweck ist klar zu bezeichnen.

Hat das Sicherheitskonzept (Risikoanalyse) ergeben, dass von einem erhöhten Schutzbedarf der Protokolldaten auszugehen ist, sollten diese mit kryptografischen Verfahren auf dem Protokollserver ausreichend gesichert werden.

6.4 Auswerten

Als Grundlage für eine datenschutzkonforme Auswertung muss die Art und der Umfang der Auswertung unter Beachtung der engen Zweckbindung der Protokolldaten vorab festgelegt werden ("Protokollierungskonzept"). Dieses Konzept ist Teil der zu erstellenden Risikoanalyse bzw. des Sicherheitskonzepts, die im Zuge der Vorabkontrolle zu fertigen sind.

Da Protokolldaten geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sollten Mitbestimmungsrechte der Personalvertretungen berücksichtigt werden (vgl. § 87 Abs. 1 Nr. 6 BetrVG oder § 74 Abs. 1 Nr. 17 HPVG). Die Art der Auswertung der Protokolldaten und die an der Auswertung Beteiligten sollten daher in einer Dienstvereinbarung geregelt werden.

Die Auswertung personenbezogener Protokolldaten muss also immer im Vier-Augen-Prinzip, unter Beachtung der personalrechtlichen Beteiligungspflichten und unter Einbeziehung der organisationseigenen Datenschutz- und IT-Sicherheitsbeauftragten, erfolgen.

Bereits bei der Planung der Protokollinhalte sind typische Szenarien zur Auswertung betrachtet worden. Für diese Szenarien müssen geeignete Mechanismen zur Auswertung vorgehalten werden. Für die häufigsten Auswertungen sollte bereits im Verfahren selbst eine Möglichkeit zur Auswertung geschaffen werden.

Für speziellere Auswertungen muss dann unter Nutzung einheitlicher Protokollformate (vgl. Abschnitt "Inhalte") eine auf den jeweiligen Zweck zugeschnittene Auswertung durchgeführt werden.

Für die Auswertung von Protokolldaten müssen vorab typische Szenarien geplant werden, in denen Protokolldaten entweder anlassbezogen oder regelmäßig ausgewertet werden. Die Szenarien sollten die zu erwartenden Auskunftsersuchen interner und externer Stellen berücksichtigen.

Werden Protokolldaten einer organisationsexternen Instanz zur Auswertung übergeben, so ist, durch geeignete technische und organisatorische Maßnahmen, eine Weitergabe-, Verwendungs- und Löschkontrolle für diese Daten zu etablieren.

Die Vorgehensweise zur Auswertung der Protokolldaten ist zu dokumentieren und die Durchführung ihrerseits zu protokollieren.

6.5 Löschen

Für jedes Protokolldatum ist bereits vor dem Erzeugen die Aufbewahrungsdauer festzulegen. Für die Aufbewahrung der Protokolle gelten die allgemeinen Löschungsregeln der Datenschutzgesetze. Ein Maßstab ist mithin die "Erforderlichkeit der Aufgabenerfüllung". Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Pflicht zur Löschung.

Somit wird die Länge der Aufbewahrungsdauer maßgeblich durch den geplanten Auswertungszyklus bestimmt. Je nach Verfahrensart können Fristen von nur wenigen Tagen bis hin zu mehreren Monaten zweckmäßig und akzeptabel sein.
Wird diese Dauer überschritten, muss das Datum gelöscht werden.

Mit Blick auf einige Landesdatenschutzgesetze, in denen die Speicherdauer für Protokolldaten selbst bei der Verarbeitung ausschließlich automatisiert gespeicherte Daten auf ein Jahr begrenzt wird (z.B. § 6 Abs. 4 LDSG S-H oder § 22 Abs. 4 DSG M-V), sollte die Speicherdauer grundsätzlich auf höchstens ein Jahr begrenzt werden, soweit nicht spezialgesetzliche Regelungen oder verfahrensspezifische Bedingungen andere Löschfristen zwingend erfordern.

Der Umgang mit Protokolldaten, insbesondere aber das Verfahren zum Löschen der Protokolldaten muss beschrieben sein. Es müssen dabei auch die Protokolldaten in die Löschung einbezogen werden, die auf Datensicherungsmedien oder bei einem Auftragsdatenverarbeiter gespeichert sind.

Bei der Protokollierung von Löschvorgängen für Protokolldaten dürfen keine personenbezogenen Daten in den Inhalten des Lösch-Protokolls enthalten sein. Stattdessen sind gegebenenfalls Hinweise auf Aktenzeichen oder Dateinamen aufzunehmen. Ferner müssen Angaben darüber, welche Person oder welche Systemkomponente die Löschung dieser Protokolldaten zu welchem Zeitpunkt vorgenommen hat, enthalten sein (Beispiel: "Gelöscht Protokolldaten_Fachverfahren_AA200_bis_ZZ620_von 200106_bis_200606, Admin_A, 20090302_1510_35").

Soweit ein Protokoll der Verfahrensdokumentation dient, kann die erforderliche Speicherdauer identisch sein zur Dauer der Dokumentationspflicht und mehrere Jahre betragen. Dies gilt beispielsweise für die Dokumentation, wer wann welche Zugriffsrechte besaß und umfasst das Anlegen und Löschen von Benutzerkennungen und die Vergabe von Zugriffsrechten. Ein anderes Beispiel, bei dem eine langjährige Speicherung erforderlich sein kann, betrifft lesende Zugriffe die eine Datenübermittlung darstellen; dies wäre der Fall, wenn die Daten verarbeitende Stelle einer anderen Daten verarbeitenden Stelle ein Leserecht einräumt, ohne dass eine Auftragsdatenverarbeitung vorliegt. In diesen und anderen Fällen könnten aus den Protokollen Berichte erstellt werden, um das Verfahren zu dokumentieren. Auf die Speicherung der Protokolle kann anschließend verzichtet werden, falls die Berichte gegen nachträgliche Änderungen geschützt sind und festgestellt werden kann, ob sie vollständig sind.

7. Weiterführende Literatur

- DuD - Datenschutz und Datensicherheit, 31. Jahrgang, Heft 10, Oktober 2007, Protokollierungs-Spezial
- DuD - Datenschutz und Datensicherheit, 30. Jahrgang, Heft 5, Mai 2006, Protokollierungs-Spezial
- "Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb" https://www.bsi.bund.de/cln_134/ContentBSI/Publikationen/studien/logdaten/index_htm.html

10.2 Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb

Herausgegeben vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder - Stand 2. November 2009

Inhalt

1. Vorbemerkung

Personenbezogene Daten sind vor der Freigabe eines Systems nicht weniger schutzbedürftig als nach dessen Freigabe. Die Regelungen der Landesdatenschutzgesetze und des Bundesdatenschutzgesetzes gelten für die Verarbeitung personenbezogener Daten ungeachtet der Frage, ob die Datenverarbeitung bereits im Produktivbetrieb oder noch in einer Projektphase erfolgt.

Unabhängig von der jeweiligen Phase, in der sich ein Projekt befindet, ist eine Dokumentation erforderlich, der

- die definierten Ziele,
- die technischen Mittel und Instrumente,
- die Festlegung der einzelnen Projektphasen mit Beginn und Ende,
- die Benennung der verantwortlichen Personen und
- die Entscheidung der verantwortlichen Person über den Beginn einer Projektphase, die Dokumentation des Projektverlaufes sowie die Ergebnisse und Schlussfolgerungen

zu entnehmen sind.

Der Detaillierungsgrad dieser Dokumentation kann sich nach der Entwicklungsphase richten, in der sich ein Verfahren zur Verarbeitung personenbezogener Daten befindet.

Zu unterscheiden ist der Projektbetrieb von dem Produktivbetrieb.

2. Projektbetrieb

2.1 Funktionstest

Der Zweck des Funktionstests ist es, die grundsätzliche Verwendbarkeit von Programmen und Geräten für die nachfolgenden Projektphasen sicherzustellen.

Ein Test zeichnet sich durch die folgenden Merkmale aus:
- Keine Anwender - nur Tester: Es gibt außer einer sehr kleinen Gruppe von Testern keine regulären Anwender des Verfahrens.
- Keine Verbindungen zu anderen und keinen Datenaustausch mit anderen Verfahren im Produktivbetrieb: Ein Test findet in einer isolierten Testumgebung statt.
- Keine personenbezogenen Daten: In einem Test dürfen keine personenbezogenen Daten verarbeitet und auch nicht aus anderen Produktivsystemen übernommen werden. Echtdaten sind vor ihrer Übernahme in das Testverfahren zu anonymisieren.

In Funktionstests werden definitionsgemäß keine personenbezogenen Daten verarbeitet. Deshalb sind im Testbetrieb auch keine datenschutzrechtlichen Anforderungen zu erfüllen. Durch den Ausschluss von Verbindungen mit anderen Produktivsystemen der automatisierten Verarbeitung personenbezogener Daten, sind durch die Funktionstests auch bei anderen Verfahren keine gravierenden Auswirkungen auf deren Datenschutz- und Datensicherheitsniveau zu erwarten.

2.2 Integrations- und Abnahmetest

Der Zweck der Integrations- und Abnahmetests besteht darin, das Konzept und die Implementierung vor dem Auftreten von (z.B. im Funktionstest nicht erkannten) Designschwächen oder Implementierungsfehlern in einer quasi-produktiven Umgebung mit realistischen Lastszenarien abzusichern. Mit Hilfe von Integrations- und Abnahmetests sollen vor einem Pilotbetrieb (siehe Abschnitt 3.1) oder einer Freigabe des Regelbetriebs eventuell vorhandene oder vermutete Risiken ausgeschlossen werden, die unter den Bedingungen des Funktionstests nicht abgeschätzt werden konnten. Derartige Tests sind zeitlich streng limitiert auf detailliert beschriebene Szenarien zu beschränken.

Die Integrations- und Abnahmetests sollten nach Möglichkeit nicht mit personenbezogenen Daten durchgeführt werden.

Personenbezogene Daten dürfen nur im Rahmen zusätzlicher, minimierter Tests verwendet werden. Grundlegende Funktionen müssen bereits im Funktionstest mit ausreichend anonymisierten Daten überprüft werden. Auf derartige erste Funktionstests darf nicht wegen der ohnehin geplanten Integrations- und Abnahmetests verzichtet werden.

Zu Testzwecken darf eine Kopie der erforderlichen Originaldatensätze verwendet werden, wenn eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder falls sich im Ausnahmefall trotz Nachbildung im Funktionstest ein Fehler aus dem Produktionsbetrieb nicht ermitteln, sondern nur mit Originaldaten aufklären lässt. Unter diesen Voraussetzungen können personenbezogene Daten zu Testzwecken verwendet werden wenn,

- eine bereichsspezifische Rechtsvorschrift dies nicht ausdrücklich untersagt,
- eine Anonymisierung der Originaldaten für die vorgesehene Test-Konstellation mit einem unvertretbar hohen Aufwand verbunden wäre,
- die verantwortliche Stelle dem Vorgehen schriftlich zugestimmt hat,
- bei der Durchführung oder Auswertung des Tests die schutzwürdigen Belange der Betroffenen und die Datensicherheit angemessen berücksichtigt werden,

- sichergestellt ist, dass nur die für die Fehlerbehebung und Durchführung des Tests erforderlichen Personen die Daten nutzen können und
- Zugang zu diesen Daten nur Personen erhalten, die den jeweils maßgebenden Vertraulichkeitsgrundsätzen und insbesondere datenschutzrechtlichen Vorschriften unterliegen.

Der Kopierzugriff auf die Originaldaten ist zu protokollieren. Nach Beendigung des Tests ist die benutzte Kopie der Originaldaten unverzüglich aus dem Testbereich zu löschen bzw. im Testbereich zu anonymisieren. Die Verwendung von Originaldatenkopien mit Anlass, Begründung, Umfang und Dauer, die getroffenen Sicherheitsmaßnahmen sowie die vorangehenden Tests mit Testdaten sind revisionssicher zu dokumentieren.

Der/die behördliche Datenschutzbeauftragte bzw. - soweit ein solcher nicht bestellt wurde - der/die Landesdatenschutzbeauftragte sowie die betroffenen Daten verarbeitenden Stellen - soweit nicht mit der Fachlichen Leitstelle identisch - sind vorab zu informieren.

Die Integrations- und Abnahmetests müssen in einer definierten und kontrollierten Umgebung stattfinden.

Gegenstand der Integrations- und Abnahmetests ist insbesondere auch der Test und die eventuell notwendige Korrektur der erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen. Sie dienen als Grundlage für die Erstellung des Sicherheitskonzepts und der Risikoanalyse für den späteren Regelbetrieb. Die Durchführung von Integrations- und Abnahmetests ist Voraussetzung, um das System unter Sicherheitsgesichtspunkten für den Regelbetrieb freigeben zu können.

Werden personenbezogene Daten im Integrations- und Abnahmetest verwendet, dann bedarf es hierzu zumindest einer Kurzfassung eines IT-Konzeptes sowie eines auf die Testbedingungen angepassten Sicherheitskonzeptes.

3. Produktivbetrieb

3.1 Pilotbetrieb

Der Zweck des Pilotbetriebs besteht darin, einen Echtbetrieb in einem nach zeitlich und sachlich begrenzten Bereich durchzuführen, um die definierten Anforderungen technischer und organisatorischer Art erfahrungsgestützt auf ihre Praxistauglichkeit prüfen und gegebenenfalls verändern zu können.
Innerhalb des Pilotbetriebs wird in der Regel der führende Datenbestand bearbeitet. Ist beispielsweise eine stichtagsbezogene Umstellung von Alt- auf Neuverfahren erforderlich, kann ein Parallelbetrieb zwischen Alt- und Neuverfahren vorübergehend erforderlich sein. Es sollte aber kein Parallelbetrieb stattfinden, bei dem ein eventuell noch vorhandenes Alt-Verfahren das führende System bleibt. In einem Piloten dürfen in einem zeitlich definierten Rahmen personenbezogene Daten verarbeitet werden.

Voraussetzung für einen Pilotbetrieb ist ein IT-Konzept, aus dem sich der Zweck des Verfahrens sowie das Ziel des Pilotbetriebes ergeben.

Soweit im Piloten personenbezogene Daten verarbeitet werden, bedarf es eines vollständigen Sicherheitskonzepts und einer auf dem Sicherheitskonzept aufbauenden Risikoanalyse. Wird der Pilotbetrieb nur in einem einschränkten Umfang aufgenommen, kann sich auch das Sicherheitskonzept auf diesen begrenzten Funktionsumfang beschränken. Entspricht der Pilot bereits dem Regelbetrieb der Verarbeitung personenbezogener Daten, so hat sich das Sicherheitskonzept vollständig an diesen Anforderungen zu orientieren.

Sollen im Piloten die Wirksamkeit der in dem Sicherheitskonzept beschriebenen technischen und organisatorischen Maßnahmen unter Realbedingungen überprüft werden, so muss das Sicherheitskonzept Aussagen über die Minimierung der gegebenenfalls für personenbezogene Daten auftretenden Risiken treffen.

Ein Pilotbetrieb bedarf grundsätzlich der Freigabe durch die Leitung, wenn personenbezogene Daten verarbeitet werden. Für den Pilotbetrieb kann die Freigabe auch an eine "befugte Person" delegiert werden.

3.2 Regelbetrieb

Der Zweck des Regelbetriebes besteht darin, ein automatisiertes Verfahren gemäß den definierten Anforderungen und vereinbarten Zielen zu betreiben. Die geltenden Regeln zur ordnungsgemäßen Verarbeitung personenbezogener Daten sind zu beachten.

Der Regelbetrieb erfolgt mit der Freigabe durch die Leitung. Die Freigabe hat schriftlich zu erfolgen.

Vor dem Beginn des Regelbetriebs sind die eingesetzten Programme und Sicherheitsmaßnahmen zu testen. Solche Tests dürfen beispielsweise mit personenbezogenen Daten von Personen durchgeführt werden, die für das Verfahren verantwortlich oder Mitarbeiter des Projekts sind und diesen Tests zugestimmt haben. Gut dokumentierte Funktionstests, Integrations- und Abnahmetests aus den vorherigen Projektphasen können den Aufwand für die notwendigen Tests vor der Freigabe des Verfahrens erheblich reduzieren.

10.3 Biometrische Authentisierung - Möglichkeiten und Grenzen

Herausgegeben vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (erarbeitet unter Federführung des Berliner Beauftragten für Datenschutz und Informationsfreiheit) - Stand 2. November 2009

Die Authentisierung von Personen mit bestimmten körperlichen Merkmalen wie z.B. Fingerabdrücken, Gesichtsgeometrie oder Irismuster wird gelegentlich als Alternative zu den Authentisierungsverfahren durch Besitz und/oder Wissen angesehen. In diesem Papier geht es nicht um die spezifischen Datenschutzfragen beim Einsatz biometrischer Verfahren, sondern um die Möglichkeiten und Grenzen dieser Verfahren bei der Authentisierung.

Die biometrische Authentisierung setzt zunächst die Erfassung eines biometrischen Merkmals einer Person mittels optischer, thermischer, chemosensorischer, akustischer oder drucksensitiver Verfahren für spätere Vergleichszwecke voraus. Aus den erfassten Rohdaten wird mittels geeigneter Algorithmen ein sog. Template (Muster) berechnet und zentral oder dezentral für spätere Vergleiche (z.B. auf einer Chipkarte) abgespeichert. Dabei ist sicherzustellen, dass eine Rekonstruktion des biometrischen Merkmals durch Rückrechnung aus dem Template ausgeschlossen ist.

Beim eigentlichen Authentisierungsvorgang wird mit den gleichen Erfassungssystemen das biometrische Merkmal erfasst und ebenfalls mit den gleichen geeigneten Algorithmen aus dem aktuellen Merkmal die sog. biometrische Signatur berechnet. Die biometrische Signatur wird dann mit dem hinterlegten Template computergestützt verglichen. Das Ergebnis dieses Vergleichs führt dann zur automatisierten Entscheidung, ob die Authentisierung zum Erfolg führt oder nicht.

Die wichtigsten Erkennungsarten bei der Überprüfung sind die biometrische Verifikation (1:1-Vergleich) und die biometrische Identifikation (1:n-Vergleich). Bei der Verifikation wird die Identität durch den Vergleich der biometrischen Signatur mit genau einem Template geprüft, das dezentral, zum Beispiel auf einem bei der zu verifizierenden Person befindlichen Chip gespeichert werden kann. Bei der Identifikation wird die biometrische Signatur mit einer Vielzahl von Templates verglichen, die zentral in einer Datenbank gespeichert sind.

Aus datenschutzrechtlicher Sicht ist wegen der Datensparsamkeit und -vermeidung der biometrischen Verifikation eindeutig der Vorzug vor der biometrischen Identifikation zu geben. Dies gilt insbesondere bei einer dezentralen Speicherung der Referenzdaten.

Die Treffsicherheit biometrischer Verfahren folgt im Gegensatz zu den kausalen Verfahren der Authentisierung durch Besitz und/oder Wissen Gesetzen der Wahrscheinlichkeit. Es ist stets davon auszugehen, dass die biometrische Signatur und das Template nie ganz gleich sein werden. Der Vergleich zwischen Signatur und Template kann daher nur einen Grad von Ähnlichkeit ermitteln.
Je nach den Anforderungen an die Treffsicherheit des biometrischen Erkennungssystems muss ein Schwellenwert für die Ähnlichkeit festgelegt werden, über dem die Berechtigung vergeben (Acceptance) und unter dem sie verweigert (Rejection) wird. Je höher (oder geringer) der Schwellenwert gewählt wird, desto geringer (oder höher) ist die Wahrscheinlichkeit, dass eine Berechtigung unzutreffend erteilt wird. Andererseits steigt (sinkt) mit dem Schwellenwert die Wahrscheinlichkeit, dass jemand unberechtigt abgewiesen wird.

Die Wahrscheinlichkeit, dass jemand unrichtigerweise zurückgewiesen wird, wird als "False Rejection Rate" (FRR) bezeichnet; die Wahrscheinlichkeit, dass jemand unberechtigterweise eine Berechtigung erteilt bekommt, wird als "False Acceptance Rate" (FAR) bezeichnet. Unter Kalibrierung versteht man die für eine konkrete Anwendung sinnvolle Vergabe von FRR bzw. FAR. Wenn eine der beiden Größen festgelegt bzw. beschränkt wird, ergibt sich die Festlegung bzw. Beschränkung für die andere wegen der wechselseitigen Abhängigkeit aus dem jeweiligen konkreten biometrischen Verfahren.

Die "Equal Error Rate" ist der Wert, für den FRR = FAR gilt. Sie kann ein sinnvoller Kompromiss hinsichtlich der Sicherheitskalibrierung sein. Es gibt jedoch Anwendungsszenarien, bei denen die FAR im Vergleich zur FRR sehr niedrig sein muss, z.B. beim Zutritt/Zugang zum Hochsicherheitsbereich eines Kernkraftwerkes. Und es gibt Anwendungen, bei denen die FRR beispielsweise aus Performancegründen sehr niedrig sein muss und man eine höhere FAR gerne in Kauf nimmt. Das wäre bei der Zugangskontrolle für Besucher eines großen Fußballspiels der Fall, wenn wenige unberechtigt eingelassene Besucher akzeptiert werden.

Von den vielen übrigen "Rates", die etwas über das biometrische System aussagen, sei noch die "Failure to Enroll Rate" (FTE) erwähnt, die die Wahrscheinlichkeit benennt, dass von einer Person aus medizinischen Gründen kein brauchbares Template zu späteren Vergleichszwecken gewonnen werden kann. Dies gilt vor allem für Fingerabdrücke, bei denen FTEs von ca. 2 % der Gesamtbevölkerung ermittelt worden sind.

FRR und FAR sind abhängig von der Qualität des biometrischen Systems hinsichtlich der Genauigkeit der Erfassung, der Qualität der Template- und Signatur-Berechnung und der Genauigkeit des Vergleichs, von der Kalibrierung des biometrischen Systems, also der Wahl der Schwellenwerte und der Kooperation der Betroffenen.

Bei allzu kleiner FAR wird die FRR zu groß, d.h. z.B., bei einem Zutrittskontrollsystem bleiben zu viele Berechtigte vor der Tür. Dagegen führt eine allzu kleine FRR zu einer großen FAR, d.h. zu viele Unberechtigte können die Tür durchschreiten.

1. Die kausalen Verfahren der Authentisierung mit Besitz und/oder Wissen
Beim kausalen Authentifizierungsvorgang, d.h. der Prüfung, ob der Besitz vorhanden und das Wissen korrekt wiedergegeben wurde, ist eine Ja-Nein-Entscheidung möglich. Diese Verfahren treffen aber keine 100-prozentige, eindeutige und zutreffende Entscheidung, ob die zu authentifizierende Person wirklich anwesend ist oder nicht. Vielmehr wird unterstellt bzw. angenommen, dass wenn Besitz und Wissen im Authentisierungsverfahren mit dem der zu authentifizierenden Person übereinstimmen, [nur] diese Person anwesend ist. Es kann keine Wahrscheinlichkeit dafür berechnet, hergeleitet oder angegeben werden, dass diese Annahme oder Unterstellung zutrifft. Auch eine Lebenderkennung ist damit nicht verbunden.

   Es gibt eine Fülle von Beispielen, die belegen, dass ein korrekter Ablauf des Authentisierungsverfahrens nicht sicherstellt, dass auch die richtige Person das System nutzt.

   So können die Authentisierungsmittel beispielsweise
   - weitergegeben sein,
   - gestohlen (Besitz) oder erpresst (Wissen) sein,
   - der Besitz technisch dupliziert und das Wissen durch technische Manipulation ganz oder teilweise in falsche Hände gekommen sein (vgl. hierzu u.a. die vielfältigen Manipulationen an Geldausgabeautomaten),
   - der richtige Benutzer zwar anwesend sein und das Authentisierungsverfahren bedienen, die anschließende Nutzung des Systems aber mit oder ohne Anwendung von Gewalt ausschließlich durch Dritte erfolgen etc.

2. Biometrische Authentisierung
Bei der biometrischen Authentisierung kann immerhin mit einer berechenbaren bzw. hohen Wahrscheinlichkeit davon ausgegangen werden, dass die richtige Person anwesend ist, wenn das biometrische Merkmal dauerhaft und direkt mit ihr verbunden ist. Dies gilt insbesondere für biometrische Merkmale, die nicht wie der Fingerabdruck an vielen Orten ständig hinterlassen werden. Hierbei ist natürlich auch zu berücksichtigen, ob das Verfahren eine Lebenderkennung beinhaltet.

   Die tatsächliche Bindung des biometrischen Merkmals an die Person ist als echter Vorteil gegenüber personenbezogenen Merkmalen wie Besitz und Wissen zu werten, bei denen die Anwesenheit der Person nur angenommen werden kann.

3. Besondere Vorkehrungen bei biometrischer Authentisierung
Die biometrischen Daten sind - im Gegensatz zu UserID und Passwort und zu Verfahren von Besitz und Wissen - eindeutig und potenziell lebenslang mit der Betroffenen verbunden.

   Deshalb sind für biometrische Authentisierungsverfahren - unabhängig vom verwendeten biometrischen Verfahren - besondere Vorkehrungen zu treffen:

   a) Die Verbindung zwischen biometrischen und anderen Identitätsdaten muss sicher geschützt werden.

   b) Der Schutz des Speichersystems der biometrischen Referenzdaten ist für Datensicherheit und Datenschutz des Verfahrens von grundlegender Bedeutung. Dabei sollte keine zentrale, sondern eine dezentrale Speicherung der Referenzdaten, z.B. auf einer Chipkarte, realisiert werden.

   c) Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden. Dies erfordert den Einsatz kryptografischer Verfahren.

      Die biometrischen Daten sind nicht geheim und sie können nach Bekanntwerden oder Missbrauch nicht verändert oder gesperrt werden. Deshalb ist Folgendes wichtig:

   d) Die biometrischen Daten dürfen nicht allein zur Authentisierung herangezogen werden, sondern sie sind mit sperr- und veränderbaren Daten wie Besitz und Wissen wirksam zu koppeln.

   Die Stärke biometrischer Verfahren kann sich bei der biometrischen Authentisierung wegen der Nicht-Änderbarkeit und Nicht-Sperrbarkeit biometrischer Merkmale nur entfalten, wenn die genannten Anforderungen erfüllt sind und die mit der Verarbeitung der biometrischen Daten verbundenen Risiken insgesamt wirksam beherrscht werden. Wenn eine Methode mit Besitz und Wissen durch die biometrische Authentisierung ergänzt wird, verleiht dies damit dem kausalen Verfahren höhere Sicherheit vor Kompromittierung.