DER HESSISCHE DATENSCHUTZBEAUFTRAGTE

39. Tätigkeitsbericht

Neununddreißigster Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2010
gemäß § 30 des Hessischen Datenschutzgesetzes
vom 7. Januar 1999

Beiträge zum Datenschutz
Herausgegeben vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
Gustav-Stresemann-Ring 1, 65189 Wiesbaden
Postfach 31 63, 65021 Wiesbaden

Telefon: (06 11) 14 08-0
Telefax: (06 11) 14 08 -9 00 oder 14 08-9 01
E-Mail: poststelle@datenschutz.hessen.de
Internet: www.datenschutz.hessen.de

Herstellung: Druckerei Chmielorz GmbH, Ostring 13, 65205 Wiesbaden-Nordenstadt

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 39. Tätigkeitsbericht

ABl.	Amtsblatt des Hessischen Kultusministeriums
ABl. EG	Amtsblatt der Europäischen Union
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AO	Abgabenordnung
Art.	Artikel
AsylVfG	Asylverfahrensgesetz
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BKADV	BKA-Daten-Verordnung
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern
BPolG	Bundespolizeigesetz
BRDrucks.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BStatG	Bundesstatistikgesetz
BTDrucks.	Bundestagsdrucksache
Buchst.	Buchstabe
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
bzw.	beziehungsweise
ca.	circa
CDU	Christlich Demokratische Union Deutschlands
d. h.	das heißt
DB AG	Deutsche Bahn Aktiengesellschaft
DRG	Diagnosis Related Groups
DV	Datenverarbeitung
EAC	**E**xtended **A**ccess **C**ontrol
EAN	**E**uropean **A**rticle **N**umber (Artikelnummer)
EC	Electronic Cash
EFS	**E**ncrypted **F**ile **S**ystem
EG	Europäische Gemeinschaft
eGK	elektronische Gesundheitskarte
eID	elektronischer Identitätsnachweis
eID	elektronische Identifizierung
ELSTAM	Elektronische Lohnsteuerabzugsmerkmale
et al.	et alii (und andere)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUROJUST	Europäische Stelle zur justiziellen Zusammenarbeit
EUROPOL	Europäisches Polizeiamt
FDP	Freie Demokratische Partei

FEB	Fahrerlaubnisbehörde
FeV	Fahrerlaubnis-Verordnung
ff.	fortfolgende/r/s
gem.	gemäß
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GIT	Gemeinsame IT-Stelle der hessischen Justiz
GK	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GTIN	**G**lobal **T**rade **I**tem **N**umber (Artikelidentnummer)
GwG	Geldwäschegesetz
HARIS	Hessisches Analyse- und Recherchesystem
HBG	Hessisches Beamtengesetz
HBKG	Hessisches Brand- und Katastrophenschutzgesetz
HBS	Hessische Bezügestelle
HDSG	Hessisches Datenschutzgesetz
HeDok	Hessisches Dokumentenmanagementsystem
HessLStatG	Hessisches Landesstatistikgesetz
HGB	Handelsgesetzbuch
HGöGD	Hessisches Gesetz über den öffentlichen Gesundheitsdienst
HI	Hessisches Immobilienmanagement
HKHG	Hessisches Krankenhausgesetz
HLfV	Hessisches Landesamt für Verfassungsschutz
HMDIS	Hessisches Ministerium des Innern und für Sport
HMDJIE	Hessisches Ministerium der Justiz, für Integration und Europa
HMG	Hessisches Meldegesetz
HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HRDG	Hessisches Rettungsdienstgesetz
HSchG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HStVollzG	Hessisches Gesetz über den Vollzug der Freiheitsstrafe und der Sicherungsverwahrung
http	Hypertext Transfer Protocol
HUVollzG	Hessisches Untersuchungshaftvollzugsgesetz
HVwVfgG	Hessisches Verwaltungsverfahrensgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. S. d.	im Sinne der/des
IT	Informationstechnik
KBA	Kraftfahrt-Bundesamt
KAG	Gesetz über Kommunale Abgaben
KAN	Kriminalaktennachweis
KIS	Krankenhausinformationssystem
KJC	KreisJobCenter
KWG	Kreditwesengesetz
LBG	Land- und forstwirtschaftliche Berufsgenossenschaft
LfV	Landesamt für Verfassungsschutz
LKA	Landeskriminalamt
LTDrucks.	Landtagsdrucksache
LUSD	Lehrer- und Schüler-Datenbank
LUSD-ID	LUSD-Identifikationsnummer
MDK	Medizinischer Dienst der Krankenversicherung
MPU	medizinisch-psychologische Untersuchung

MVZ	Medizinisches Versorgungszentrum
NADIS	Nachrichtendienstliches Informationssystem
NADIS-WN	NADIS als Wissensnetz
NJW	Neue Juristische Wochenschrift
nPA	neuer Personalausweis
Nr.	Nummer
NZA-RR	Neue Zeitschrift für Arbeitsrecht-Rechtsprechungsreport
OFD	Oberfinanzdirektion
OTP	One-Time Password (Einmal-Passwort)
OWASP	Open Web Application Security Project
OWiG	Gesetz über Ordnungswidrigkeiten
PAuswG	Personalausweisgesetz
PC	Personal Computer
PIN	Personal Identification Number (persönliche Geheimzahl)
ppp	**P**ublic **P**rivate **P**artnership
PUK	**P**ersonal **U**nblocking **K**ey (persönliche geheime Entsperrnummer)
RFID	Radio Frequency Identification
RP	Regierungspräsidium
s.	siehe
s. a.	siehe auch
SAP R/3 HR	in der Hessischen Landesverwaltung eingesetztes DV-System zur Personaldatenverarbeitung
SDÜ	Schengener Duchführungsübereinkommen
SEPA	Single Euro Payments Area
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
sog.	sogenannte/r/s
SPD	Sozialdemokratische Partei Deutschlands
SSL	**S**ecure **S**ocket **L**ayer
StAnz.	Staatsanzeiger für das Land Hessen
StatRegG	Statistikregistergesetz
StGB	Strafgesetzbuch
StichprobenV	Stichprobenverordnung Zensusgesetz 2011
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVollzG	(Bundes-)Strafvollzugsgesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFTP	Terrorist Finance Tracking Program
u. a.	unter anderem
URL	Uniform Resource Locator
USB	Universal Serial Bus (universeller Anschluss beim PC)
usw.	und so weiter
VerfSchG	Gesetz über das Landesamt für Verfassungsschutz
VG	Verwaltungsgericht
vgl.	vergleiche
VLAN	**V**irtual **L**ogical **A**rea **N**etwork
VPN	**V**irtual **P**rivate **N**etwork
z. B.	zum Beispiel
ZensG	Zensusgesetz
ZensVorbG	Zensusvorbereitungsgesetz
Ziff.	Ziffer
ZPM	Zentrales Personalmanagement (eine Organisationseinheit

	des Staatlichen Schulamtes Darmstadt

Register der Rechtsvorschriften

AEUV	Vertrag über die Arbeitsweise der Europäischen Union i.d.F. des Vertrags von Lissabon vom 13. Dez. 2007 (ABlEG 2007/C 306/1)
AfE	Erlass zur Aktenführung in den Dienststellen des Landes Hessen (Aktenführungserlass) vom 16. Mai 2007 (StAnz. S. 1123)
AO	Abgabenordnung i. d. F. vom 1. Okt. 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Art. 2 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2474)
AsylVfG	Asylverfahrensgesetz i. d. F. vom 2. Sept. 2008 (BGBl. I S. 1798), zuletzt geändert durch Art. 18 des Gesetzes vom 17. Dez. 2008 (BGBl. I S. 2586)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) i. d. F. vom 25. Feb. 2008 (BGBl. I S. 62), zuletzt geändert durch Art. 4 Abs. 5 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437)
BDSG	Bundesdatenschutzgesetz i. d. F. vom 14. Jan. 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 14. Aug. 2009 (BGBl. I S. 2814)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 2. Jan. 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Gesetz vom 24. Juli 2010 (BGBl. I S. 977)
BKADV	Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen (BKA-Daten-Verordnung) vom 4. Juni 2010 (BGBl. I S. 716), zuletzt geändert durch Art. 2 der Verordnung vom 4. Juni 2010 (BGBl. I S. 716)
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Art. 1 und mittelbare Änderung durch Art. 6 Nr. 1 des Gesetzes vom 6. Juni 2009 (BGBl. I S. 1226)

BPolG	Gesetz über die Bundespolizei (Bundespolizeigesetz) vom 19. Okt. 1994 (BGBl. I S. 2978, 2979), zuletzt geändert durch Art. 2 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2507)
BStatG	Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz) vom 22. Jan. 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 3 des Gesetzes vom 7. Sept. 2007 (BGBl. I S. 2246)
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz) vom 20. Dez. 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Art. 1a des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2499)
EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr Nr. 95/46	EG-Datenschutzrichtlinie vom 24. Okt. 1995 (ABl. EG Nr. L 281 S. 31 vom 23. Nov. 1995), in nationales Recht umgesetzt durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001 (BGBl. I S. 904);
EG-Richtlinie über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten Nr. 2002/22	EG-Universaldienstrichtlinie vom 7. März 2002 (ABl. EG Nr. L 108 S. 51), zuletzt geändert durch Art. 1 der AndRL 2009/136 vom 25. Nov. 2009 (ABl. EG Nr. L 337 S. 11)
EG-Verordnung zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatsangehörige Nr. 380/2008	Verordnung vom 18. Apr. 2008 (ABl. EG Nr. L 115 S. 1) zur Änderung der EG-Verordnung Nr. 1030/2002 vom 16. Juni 2002 (ABl. EG Nr. L 157 S. 1)
EG-Verordnung über Volks- und Wohnungszählungen Nr. 763/2008	Verordnung vom 9. Juli 2008 (ABl. EG Nr. L 218 S. 140)

Erlass über die Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrkraft	Erlass vom 21. Aug. 2009 (ABl. 9/2009 S. 726)
Erlass über IT-Sicherheit und Datenschutz in Schulverwaltungen zur Nutzung von E-Mail und zur Erhebung und Veröffentlichung interner Daten	Erlass vom 27. Nov. 2009 (ABl. 1/2010 S. 11)
FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnis-Verordnung) vom 13. Dez. 2010 (BGBl. I S. 1980), zuletzt geändert durch Art. 1 der Verordnung vom 17. Dez. 2010 (BGBl. I S. 2279)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 21. Juli 2010 (BGBl. I S. 944)
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) vom 13. Aug. 2008 (BGBl. I S. 1690), zuletzt geändert durch Art. 4 Abs. 9 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437)
HBG	Hessisches Beamtengesetz i. d. F. vom 11. Jan. 1989 (GVBl. I S. 26), zuletzt geändert durch Art. 13 des Gesetzes vom 26. März 2010 (GVBl. I S. 114, 116)
HBKG	Hessisches Gesetz über den Brandschutz, die Allgemeine Hilfe und den Katastrophenschutz (Hessisches Brand- und Katastrophenschutzgesetz) vom 17. Dez. 1998, zuletzt geändert durch Gesetz vom 18. Nov. 2009 (GVBl. I S. 423)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 7. Jan. 1999 (GVBl. I S. 98)
Hessisches Ausführungsgesetz zum Zensusgesetz 2011	vom 23. Juni 2010 (GVBl. I S. 178)
Hessisches Dolmetscher- und Übersetzergesetz	vom 20. Mai 2010 (GVBl. I S. 146)

HessLStatG	Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz) vom 19. Mai 1987 (GVBl. I S. 67, zuletzt geändert durch Art. 2 des Gesetzes vom 23. Juni 2010 (GVBl. I S. 178, 181)
HGB	Handelsgesetzbuch i. d. bereinigten Fassung vom 10. Mai 1897 (BGBl. III, Gliederungsnummer 4100-1), zuletzt geändert durch Art. 18 des Gesetzes vom 8. Dez. 2010 (BGBl. I S. 1768)
HGöGD	Hessisches Gesetz über den öffentlichen Gesundheitsdienst vom 28. Sept. 2007 (GVBl. I S. 659), zuletzt geändert durch Art. 2 des Gesetzes vom 24. März 2010 (GVBl. I S. 123)
HKHG	Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2002) i. d. F. 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)
HRDG	Gesetz zur Neuordnung des Rettungsdienstes in Hessen (Hessisches Rettungsdienstgesetz) vom 24. Nov. 1998, zuletzt geändert durch Art. 21 des Gesetzes vom 21. März 2005 (GVBl. I S. 218, 226)
HSchG	Hessisches Schulgesetz i. d. F. vom 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. 14), zuletzt geändert durch Art. 1 des Gesetzes vom 14. Dez. 2009 (GVBl. I S. 635)
HStVollzG	Hessisches Gesetz über den Vollzug der Freiheitsstrafe und der Sicherungsverwahrung vom 28. Juni 2010 (GVBl. I S. 185)
HUVollzG	Hessisches Untersuchungshaftvollzugsgesetz vom 28. Juni 2010 (GVBl. I S. 185, 208)
HVwVfgG	Hessisches Verwaltungsverfahrensgesetz i. d. F. vom 15. Jan. 2010 (GVBl. I S. 18)

KAG	Gesetz über Kommunale Abgaben vom 17. März 1970 (GVBl. I S. 2259), zuletzt geändert durch Gesetz vom 31. Jan. 2005 (GVBl. I S. 54)
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz) i. d. F. vom 9. Sept. 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 1 des Gesetzes vom 19. Nov. 2010 (BGBl. I S. 1592)
MRRG	Melderechtsrahmengesetz i. d. F. der Bekanntmachung vom 19. April 2002 (BGBl. I S. 1342), zuletzt geändert durch Art. 23 des Gesetzes vom 8. Dez. 2010 (BGBl. I S. 1768)
OWiG	Gesetz über Ordnungswidrigkeiten i. d. F. vom 19. Feb. 1987 (BGBl. I S. 602), zuletzt geändert durch Art. 2 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2353)
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) i. d. F. vom 18. Juni 2009 (BGBl. I S. 1346)
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 (Art. 1 des Gesetzes vom 11. Dez. 1975, BGBl. I S. 3015), zuletzt geändert durch Art. 7 Abs. 5 des Gesetzes vom 7. Juli 2009 (BGBl. I S. 1707)
SGB II	Zweites Buch Sozialgesetzbuch – Grundsicherung für Arbeitsuchende (Art. 1 des Gesetzes vom 24. Dez. 2003 (BGBl. I S. 2954), zuletzt geändert durch Art. 3 des Gesetzes vom 24. Okt. 2010 (BGBl. I S. 1422)
SGB V	Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung (Art. 1 des Gesetzes vom 20. Dez. 1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 18 des Gesetzes vom 9. Dez. 2010 (BGBl. I S. 1885)

SGB IX	Neuntes Buch Sozialgesetzbuch – Rehabilitation und Teilhabe behinderter Menschen (Art. 1 des Gesetzes vom 19. Juni 2001, BGBl. I S. 1046), zuletzt geändert durch Art. 4 des Gesetzes vom 5. Aug. 2010 (BGBl. I S. 1127)
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz (Art. 1 des Gesetzes vom 18. Aug. 1980, BGBl. I S. 1469 und Art. 1 des Gesetzes vom 4. Nov. 1982, BGBl. I S. 1450) i. d. F. vom 18. Jan. 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 5 des Gesetzes vom 5. Aug. 2010 (BGBl. I S. 1127)
StatRegG	Gesetz über den Aufbau und die Führung eines Statistikregisters (Statistikregistergesetz) vom 16. Juni 1998 (BGBl. I S. 1300), zuletzt geändert durch Art. 12 des Gesetzes vom 10. Nov. 2006 (BGBl. I S. 2553)
StGB	Strafgesetzbuch i. d. F. vom 13. Nov. 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 3 des Gesetzes vom 2. Okt. 2009 (BGBl. I S. 3214)
StPO	Strafprozessordnung i. d. F. vom 7. Apr. 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 22. Dez. 2010 (BGBl. I S. 2261)
StichprobenV	Verordnung über Verfahren und Umfang der Haushaltebefragung auf Stichprobenbasis zum Zensusgesetz 2011 (Stichprobenverordnung Zensusgesetz 2011) vom 25. Juni 2010 (BGBl. I S. 830)
StVG	Straßenverkehrsgesetz i. d. F. vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 1 des Gesetzes vom 2. Dez. 2010 (BGBl. I S. 1748)
Swift-Abkommen	Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (ABl. EG Nr. L 195 S. 1 vom 27. Juli 2010)
VerfSchG	Gesetz über das Landesamt für Verfassungsschutz vom 19. Dez. 1990 (GVBl. I S. 753), zuletzt geändert durch § 32 des Gesetzes vom 28. Sept. 2007 (GVBl. I S. 623, 633)

Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen	Verordnung vom 4. Feb. 2009 (ABl. 3/2009 S. 131)
Weimarer Reichsverfassung	Die Verfassung des Deutschen Reichs vom 11. Aug. 1919 (RGBl. S. 1383), zuletzt geändert durch Gesetz vom 17. Dez. 1932 (RGBl. I S. 547)
ZensG 2011	Zensusgesetz 2011 vom 8. Juli 2009 (BGBl. I S. 1781)
ZensVorbG 2011	Zensusvorbereitungsgesetz 2011 vom 8. Dez. 2007 (BGBl. I S. 2808)

Kernpunkte

1. In Hessen erging 1970 das weltweit erste Datenschutzgesetz. Auf dieser Grundlage entwickelte sich eine spezifische hessische Datenschutzkultur, die in dem hohen Stellenwert ihren Ausdruck findet, der dem Datenschutz von allen im Landtag vertretenen Parteien eingeräumt wird. Die Entscheidung des Europäischen Gerichtshofs vom 9. März 2010, die der Bundesrepublik Deutschland vorhielt, entgegen der Europäischen Datenschutzrichtlinie nicht für die „völlige Unabhängigkeit" der Kontrollinstanzen gesorgt zu haben, war Auslöser der zu der zum 40. Jahrestag des Hessischen Datenschutzgesetzes von den Fraktionen der CDU, SPD, FDP und Bündnis 90/Die Grünen gemeinsam verabschiedeten Wiesbadener Erklärung vom 8. Oktober 2011. Darin haben sich diese auf Eckpunkte für eine **Neuordnung des Datenschutzes** geeinigt. Die Umsetzung mit dem Ziel einer unabhängigen Datenschutzkontrolle in Hessen muss zügig vorangetrieben werden (Ziff. 1.1).

2. Eine **Stärkung des Datenschutzes** in Hessen durch die Neuordnung kann nur erreicht werden, wenn die Politik in Umsetzung der Wiesbadener Erklärung dem Hessischen Datenschutzbeauftragten eine der anspruchsvollen Aufgabe in Höhe und Qualität angemessene Personal- und Sachausstattung gewährt. Die in den letzten Jahren zu verzeichnende Steigerung der Datenschutzanfragen hatte zur Folge, dass Kontrollen aber auch Beratungen zurückstehen mussten. Allein mit Synergieeffekten kann deshalb noch nicht einmal die Steigerung der Fallzahlen aufgefangen, geschweige denn aktiv das Datenschutzniveau verbessert werden (Ziff. 1.1.2).

3. Neben diesen organisatorischen Maßnahmen ist eine **Aktualisierung des Datenschutzrechts** erforderlich, die dem kommunikativen Konzept der informationellen Selbstbestimmung Rechnung trägt. Das autonome Verfügungsrecht über die eigenen Daten geht über das Recht, von Datenzugriffen verschont zu bleiben, hinaus. Ein eng verstandenes Konzept von „Privacy" schöpft das Konzept der informationellen Selbstbestimmung nicht aus.

4. Der **Zensus 2011** (Volkszählung) wird keine Vollerhebung bei allen Bürgerinnen und Bürgern sein, vielmehr soll die Bevölkerungsanzahl und -struktur weitgehend registergestützt ermittelt werden. Das Hessische Statistische Landesamt hat mich in die komplexen Vorbereitungen für die im Jahr 2011 vorgesehene Volkszählung (Zensus 2011) eingebunden, um die Einhaltung des Datenschutzes sicherzustellen (Ziff. 3.3).

5. Zum 1. November 2010 wurde **der neue Personalausweis** eingeführt. Er eröffnet – neben der reinen Identifizierungsfunktion – zusätzliche Nutzungsoptionen (Authentisierung und Prüfung von Altersangaben bei über das Internet abgewickelten Rechtsgeschäften, digitale Signatur), über die der Besitzer des Ausweises entscheiden kann. Schon allein aus diesem Grund ist streng darauf zu achten, dass mit dem neuen Personalausweis sorgfältig umgegangen wird: er darf weder hinterlegt noch kopiert werden. Das Sperrkennwort und die Telefonnummer, unter der man den Ausweis sperren lassen kann, müssen sorgfältig aufbewahrt werden, damit sie im Fall des Ausweisverlustes zur Hand sind, um durch schnelle Sperrung Missbrauch zu verhindern (Ziff. 3.4).

6. Die **Videoüberwachung im Umfeld von Bahnhöfen** wird häufig im Wege einer sog. Sicherheitspartnerschaft von kommunalen Ordnungsbehörden, Landes- und Bundespolizei betrieben. Dabei müssen die unterschiedlichen Zuständigkeiten berücksichtigt werden und insbesondere, dass im Bereich der Eisenbahnen weder die Kommunen noch die Landespolizei eigene Überwachungsbefugnisse besitzen. Die Befugnis zur Überwachung der öffentlichen Bahnanlagen kann nur durch öffentlich-rechtlichen Vertrag von der Bundespolizei – nicht der DB AG – auf Kommunen oder Landespolizei übertragen werden (Ziff. 4.1.3).

7. **Einsichts- und Auskunftsrechte von Betroffenen** gegenüber Verwaltungen und öffentlichen Unternehmen sind häufig Thema von Beschwerden. Mit der Rechtslage nach allgemeinem Datenschutzrecht befasst sich der Beitrag unter Ziff. 4.1.2, während verschiedenste spezialgesetzliche Aspekte in den Beiträgen Ziff. 4.4.2 (Aufenthaltsgenehmigungsverfahren), 4.7.5 (Unfallversicherung), 6.1.1 (Auskunft über Telefonaufzeichnungen durch Kreditinstitute) und 6.1.2 (Auskunft gegenüber dem Kreditinstitut im Erbfall) behandelt werden.

8. Ein Ergebnis der Prüfung des Justizzentrums Wiesbaden ist, dass insbesondere bei **ppp-Projekten** alle Daten verarbeitenden Stellen frühzeitig in die Planung eingebunden werden müssen, damit sie ihrer Verantwortung gerecht werden können. Nur so kann eine Situation vermieden werden, in der die Mieter eine von Außenstehenden geplante und zur Verfügung gestellte technische Infrastruktur nutzen müssen, ohne diese zu kennen und deren Ausgestaltung beeinflussen zu können (Ziff. 4.2.3).

9. Die Anfang 2010 von der Presse geäußerte Befürchtung, es würden datenschutzrechtlich unzulässige **„schwarze Listen“** über Lehrer geführt, hat sich nicht bestätigt: Das Zentrale

Personal Management beim Staatlichen Schulamt Darmstadt führt zwar für alle hessischen Schulämter eine „Informationsliste zur Vermeidung der Wiedereinstellung ungeeigneter Lehrkräfte“, deren Inhalt war aber nicht zu beanstanden. Nachbesserungen waren allerdings hinsichtlich der Transparenz des Verfahrens erforderlich (Ziff. 4.5.2).

10. Umfang und Inhalt **amtsärztlicher Gutachten** und die damit verbundenen Datenübermittlungen bieten häufig Anlass zu Anfragen. Gutachten, die von Arbeitgebern oder Dienstherrn in Auftrag gegeben werden, z.B. für Einstellungsuntersuchungen oder zur Prüfung der Dienstfähigkeit, müssen sich streng an dem konkret formulierten Auftrag orientieren, der sich wiederum im Rahmen der Erforderlichkeit halten muss. Betroffene sind vor Beginn der Untersuchung über deren Zweck und die Datenempfänger zu informieren. Dem Auftraggeber wird grundsätzlich nur das Untersuchungsergebnis sowie Aussagen zur Verwendungsfähigkeit des Betroffenen mitgeteilt, während der untersuchten Person regelmäßig Einsicht in das komplette Gutachten zusteht (Ziff. 4.7.3).

11. Im Berichtszeitraum musste ich in einem Fall von meinem **Beanstandung**srecht Gebrauch machen. Es handelte sich um eine initiative unzulässige Übermittlung von Daten an die Staatsanwaltschaft, die aus offiziellen Registern bereits getilgt waren. Die beanstandete Stelle zeigte sich hinsichtlich der rechtlichen Bewertung uneinsichtig (Ziff. 5.3).

1. Einführung

1.1
Allgemeines

Hessen ist das Ursprungsland der Datenschutzgesetzgebung. Am 7. Oktober 1970 (GVBl. I S. 625) entstand mit dem Hessischen Datenschutzgesetz das „Pionierwerk“ des deutschen Datenschutzrechts (vgl. Kloepfer, Informationsrecht, 2002, S. 281). Auf der Grundlage dieses Gesetzes, bestärkt durch das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, entwickelte sich eine spezifische hessische Datenschutzkultur. Diese fand ihren Ausdruck in der besonderen Wertschätzung, die dem Datenschutz von allen im Landtag vertretenen Parteien über die Parteigrenzen hinweg entgegengebracht wird. Dem steht nicht entgegen, dass zu Fragen der Ausgestaltung des Datenschutzes unterschiedliche Ansichten der Parteien bestanden und bestehen. So hielt man in der CDU-Fraktion die Trennung von privatem und öffentlichem Bereich beim Datenschutz verfassungsrechtlich für geboten und gemeinschaftsrechtlich die Zuständigkeit des Regierungspräsidiums Darmstadt für den privaten Bereich für zulässig. Demgegenüber hatte ich in meinem 37. Tätigkeitsbericht für das Jahr 2008 ausgeführt: „... der deutsche Datenschutz steht gegenwärtig auf dem gemeinschaftsrechtlichen Prüfstand. Bezogen auf die gemeinschaftsrechtlich gebotene Unabhängigkeit des (gesamten) Datenschutzes ist wieder ein hessisches Vorbild gefragt. Das Problem liegt in der Kollision von institutioneller Unabhängigkeit des Datenschutzes und der Ministerialverantwortlichkeit. Einen ministerialfreien Datenschutz gibt es in Deutschland aus verfassungsrechtlichen Gründen, d. h. mit Rücksicht auf die nationale Ausgestaltung der Gewaltenteilung, aus verständlichen Gründen nicht. Bei einer Zusammenführung von privatem und öffentlichem Bereich ließe sich die Gewaltenteilung jedoch auch jenseits der Ministerialverantwortlichkeit wahren. Es kommt nur darauf an, Unabhängigkeitsprinzip und Verantwortlichkeitsprinzip zu harmonisieren. Aus der Sicht des Hessischen Datenschutzbeauftragten ist das realisierbar, wenn dem HDSB unter Beibehaltung seiner Unabhängigkeit auch der private Bereich in der Zuständigkeit des Landes übertragen und dabei seine parlamentarische Verantwortlichkeit verstärkt würde“ (37. Tätigkeitsbericht, Ziff. 1.1). In diesem Zusammenhang wurde darauf hingewiesen, dass die Einzelheiten noch sorgfältiger Prüfung bedürften. Die erwähnten Vorgaben des EU-Rechts folgen unmittelbar aus Art. 28 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 vom 23. November 1995, S. 31 – 50).

Art. 28 EG-Richtlinie 95/46

(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.
Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.

(3) Jede Kontrollstelle verfügt insbesondere über:

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;

- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;

- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.
  Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.

Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.

(5) Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.

Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.

(7) Die Mitgliedstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.

1.1.1
Wiesbadener Erklärung

Diese Vorgabe veranlasste die Sozialdemokratische Fraktion im Hessischen Landtag, den Gesetzentwurf für ein Gesetz zur Neuordnung des Datenschutzes und Wahrung der Unabhängigkeit des Datenschutzbeauftragten in Hessen vorzulegen (LTDrucks. 18/375). Das Erfordernis der Ministerialverantwortlichkeit blieb weiterhin kontrovers.

In seiner Sitzung vom 25. Juni 2009 fasste der Innenausschuss des Hessischen Landtags folgenden Beschluss:
„Der Innenausschuss bittet den Hessischen Datenschutzbeauftragten, zu dem Gesetzentwurf LTDrucks. 18/375 ein Gutachten zu erstellen."

Abfassung und Vorlage des Gutachtens verzögerten sich wegen des beim EuGH anhängigen, die Thematik unmittelbar betreffenden Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland (Rechtssache C – 518/07). Mit Urteil vom 9. März 2010 (vgl. etwa NJW 2010, 1265) entschied der EuGH, dass die Bundesrepublik Deutschland die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr fehlerhaft umgesetzt habe. Das Erfordernis, dass die Behörde die Aufgabe der Aufsicht über die Einhaltung von Datenschutzbestimmungen im nicht öffentlichen Bereich „in völliger Unabhängigkeit"

wahrzunehmen habe, sei nicht erfüllt. In meinem erwähnten Rechtsgutachten (vgl. Homepage www.datenschutz.hessen.de) gelangte ich zu dem Ergebnis, dass die Bundesrepublik Deutschland an diese Interpretation gebunden ist. Ein Kompetenzverstoß europäischer Organe, der eine Ultra-vires-Kontrolle durch das Bundesverfassungsgericht rechtfertigen könnte, ist nicht ersichtlich (vgl. BVerfG, Beschluss vom 6. Juli 2010 – 2 BvR 2261/06). Der hessische Landesgesetzgeber steht damit, wie alle Gesetzgeber in der Bundesrepublik Deutschland, gegenwärtig in der Pflicht, die Datenschutzkontrolle im Einklang mit dem EU-Recht neu zu gestalten und der Kommission hierüber Bericht zu erstatten.

In dieser Situation bewährte sich die hessische Datenschutzkultur. Zum 40. Jubiläum des Hessischen Datenschutzgesetzes beschlossen die Fraktionen der CDU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN die „Wiesbadener Erklärung“, die die Einrichtung einer unabhängigen obersten Landesbehörde für den öffentlichen und privaten Bereich vorsieht. Konkret bedeutet das die Übertragung der Aufgaben des privaten Bereichs auf den bisher völlig unabhängigen Hessischen Datenschutzbeauftragten.

Wiesbadener Erklärung zur Neuordnung des Datenschutzes in Hessen

Das Hessische Datenschutzgesetz vom 7. Oktober 1970, in Kraft getreten am 13. Oktober 1970, ist das erste und älteste Datenschutzgesetz der Welt. Hessen gilt damit als Stammland des Datenschutzes. Mit Urteil vom 9. März 2010 hat der Europäische Gerichtshof die Bundesrepublik Deutschland verpflichtet, die für die Überwachung der Verarbeitung personenbezogener Daten im nicht öffentlichen Bereich zuständigen Kontrollstellen in den Bundesländern in völliger Unabhängigkeit gemäß der Richtlinie 95/46/EG zu organisieren.

Die Fraktionen der CDU, der SPD, der FDP und von BÜNDNIS 90/DIE GRÜNEN erarbeiten derzeit eine gemeinsame gesetzliche Regelung zur Neuordnung des Datenschutzes in Hessen, die voraussichtlich im November-Plenum in den Hessischen Landtag eingebracht werden wird.

Diese Regelung wird folgende Eckpunkte beinhalten:

1. Die Zuständigkeit für Überwachung und Schutz bei der Verarbeitung personenbezogener Daten wird in Hessen für den öffentlichen und den privaten (= nicht öffentlichen) Bereich unter dem Dach des Hessischen Datenschutzbeauftragten zusammengeführt.

2. Der Hessische Datenschutzbeauftragte übt sein Amt in völliger Unabhängigkeit aus. Bei Maßnahmen des Datenschutzbeauftragten gegenüber privaten Dritten ist der Verwaltungsrechtsweg eröffnet.

3. Der Hessische Datenschutzbeauftragte wird weiterhin auf Vorschlag der Landesregierung und für die Dauer der jeweiligen Wahlperiode vom Landtag gewählt. Das Amt des Hessischen Datenschutzbeauftragten wird von der nächsten Neuwahl an als hauptamtliche Tätigkeit ausgeübt.

4. Der Hessische Datenschutzbeauftragte ist dem Landtag gegenüber informations- und berichtspflichtig.

5. Zur Parlamentarischen Kontrolle wird der Landtag einen Unterausschuss Datenschutz einrichten.

1.1.2
Konsequenzen

Die Zusammenlegung des öffentlichen und privaten Bereichs ergibt nur dann einen Sinn, wenn mit ihr eine Verbesserung des Datenschutzes und der Schlagkraft der Datenschutzkontrolle verbunden ist. Dies macht es erforderlich, dass die Erweiterung der Aufgabenstellung des HDSB ihren Niederschlag in einer entsprechenden personellen und sächlichen Ausstattung findet. Diese Konsequenzen wären auch ohne die Zusammenlegung zu ziehen, da sich die Fallzahlen und Aufgabenstellungen des Datenschutzes in der jüngsten Vergangenheit sprunghaft vermehrt haben. Die anschließende kurze Darstellung der Situation des aktuellen und künftigen Datenschutzes soll dies verdeutlichen.

1.2
Grundlagen des Datenschutzes

1.2.1
Rechtliche Einordnung

Die verfassungsrechtliche und einfachgesetzliche Einordnung des Datenschutzes wurde bereits in der Einführung zum 38. Tätigkeitsbericht ausführlich vorgenommen. Darauf wird

verwiesen. Der Datenschutz erstreckt sich auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 2 Abs. 1 HDSG). Der Begriff umfasst alle Informationen, die über eine Bezugsperson etwas aussagen oder mit ihr in Verbindung zu bringen sind. Jedes Datum ist relevant. Der Datenschutz ist umfassend, hängt aber in seiner Intensität von der Bedeutung der einzelnen Daten im Rahmen der Gesamtrechtsordnung ab. Staatliche, gesamtgesellschaftliche und individuelle Informationsansprüche können danach Eingriffe in den Datenschutz legitimieren. Es gilt dann das hinter dem Datenschutz stehende Schutzgut zu ermitteln, zu gewichten und mit der ggf. vorhandenen Eingriffsermächtigung abzuwägen. Bei der Abwägung spielt eine Rolle, dass der Datenschutz verfassungsrechtlich verankert ist. Er ist ein Teilaspekt des allgemeinen Persönlichkeitsrechts und wie dieses zwischen Menschenwürde (Art. 1 Abs. 1 GG) und allgemeiner Handlungsfreiheit (Art. 2 Abs. 1 GG) positioniert. Die Annahme eines einheitlichen singulären Datenschutzgrundrechts wird diesem Ansatz nicht gerecht. Vielmehr setzt sich das Datenschutzgrundrecht aus einem Geflecht benannter und unbenannter Grundrechte zusammen, deren Bedeutung und Gewicht im konkreten Zusammenhang zu ermitteln sind (vgl. 1. Kammer des Ersten Senats des Bundesverfassungsgerichts, Beschluss vom 18. Januar 2010 – 1 BvR 1477/08 – NJW 2010, 1587; BGH Urteil vom 1. April 2010 – VI ZA 1258/08 -, NJW 2010, 3025).

1.2.2
Teilaspekte

Über die Teilaspekte des Datenschutzgrundrechts wurde in den vorangegangenen Tätigkeitsberichten ausführlich berichtet.

Zentrales unbenanntes Datenschutzgrundrecht ist das Recht auf informationelle Selbstbestimmung. Zur Positionierung dieses Grundrechts finden sich erhellende Ausführungen in der Entscheidung des BGH zum Bewertungsforum vom 23. Juni 2009 (VI ZA 196/08 – BGHZ 181, 328). Neben die informationelle Selbstbestimmung tritt das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme.

Aber auch benannte Freiheitsrechte spielen als Datenschutzgrundrechte eine Rolle (beispielsweise das Fernmeldegeheimnis, zu dem sich Ausführungen im Beschluss des BGH vom 14. Januar 2010 (VII ZB 111/08 – BGHZ 184, 75) finden. Die Vielzahl dieser Grundrechte haben den Eindruck erweckt als habe die Bundesrepublik Deutschland ein Monopol auf den

Datenschutz. Der Eindruck wird bestärkt durch die verbreitete Behauptung, der ausländische Datenschutz bleibe hinter dem deutschen Datenschutz zurück. Dies ist zumindest ungenau. Die Videoüberwachung wird beispielsweise in Frankreich durch die Verfassungsrechtsprechung in Schranken gehalten. Die Funktion eines Datenschutzgrundrechts erfüllt in den USA das „right of privacy“ wie in Deutschland das allgemeine Persönlichkeitsrecht auf dem Gebiet des Zivilrechts, genauer des Medienrechts. Zurückgeführt wird diese Rechtsposition auf einen berühmten Aufsatz von Samuel D. Warren und Louis D. Brandeis im Havard Law Review von 1890, in dem Zugriffe der Presse in den privaten Bereich für illegal erklärt wurden. In der Rechtsprechung setzte sich diese Konzeption lange Zeit nicht durch, ähnlich wie in Deutschland das Reichsgericht ein allgemeines Persönlichkeitsrecht nicht akzeptierte. Ein Umschwung trat in den USA 1928 in der Entscheidung des Supreme Court Olmstead v. U. S. [277 U. S. 438 (1928)] ein. In Deutschland durch die Leserbriefentscheidung des BGH von 1953 (BGHZ 1334). Seitdem war das allgemeine Persönlichkeitsrecht in der Rechtsprechung anerkannt. Die Entwicklung verlagerte sich vom Privatrecht in den verfassungsrechtlichen Bereich. In der Entscheidung aus dem Jahr 1967 – Katz v. U. S. [389 U. S. 347 (1927)] erklärte der Supreme Court die Benutzung von Abhörgeräten ohne entsprechende Rechtsgrundlage für unzulässig. Er stützte die Entscheidung dabei auf den vierten Zusatz zur amerikanischen Verfassung, der den Datenschutz nicht expressis verbis regelte. In den USA war somit der Datenschutz als Grundrecht lange vor der informationellen Selbstbestimmung in der Bundesrepublik Deutschland anerkannt. Er wurde freilich als das „right to be left alone“ konstruiert und trug dem Zugangsaspekt dieses Grundrechts noch nicht Rechnung. Dieser Aspekt findet Berücksichtigung beim Konzept der informationellen Selbstbestimmung, die nicht nur das Recht vermittelt für sich selbst zu sein, sondern auch einen Zugangsschutz bedeutet. Die informationelle Selbstbestimmung geht damit über das traditionelle Grundrechteverständnis beim Datenschutz hinaus und kann nicht durch Privacyanleihen in den Vereinigten Staaten ersetzt werden.

1.3
Rechtsentwicklung

Die Entwicklung auf dem Gebiet des Datenschutzrechts nahm einen sprunghaften Verlauf. Sowohl Gesetzgeber wie auch Rechtsprechung beschäftigten sich intensiv mit der Materie. Einen Überblick über die Entwicklung des Datenschutzrechts vermitteln Gola, Klug – Die Entwicklung des Datenschutzrechts 2009/2010, NJW 2010, 2483 f. Die Entwicklung der

Gesetzgebung ist im vorliegenden Tätigkeitsbericht im jeweiligen Sachzusammenhang gewürdigt.

Die wichtigsten Entscheidungen des Europäischen Gerichtshofs auf dem Gebiet des Europarechtes sind die erwähnte Entscheidung vom 9. März 2010 und die Entscheidung zu den Agrarsubventionen (Urteil vom 9. November 2010 – C – 92/09 und C – 93/09 –, Schecke und Eifert, DÖV 2011, 93). Aus der Rechtsprechung des Bundesverfassungsgerichts steht im Vordergrund das Interesse zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256, 263, 586/08; BVerfGE 125, 260) mit der das Bundesverfassungsgericht die streitgegenständliche Regelung der Vorratsspeicherung für verfassungswidrig erklärte, jedoch der Vorratsspeicherung als solcher keinen Riegel vorschob. Die Interpretation der Entscheidung ist in vollem Gang. Praktisch bedeutsam ist aber auch der Beschluss vom 21. September 2010, mit der die Verfassungsbeschwerde gegen den Zensus 2011 abgelehnt wurde. Es ist somit nicht damit zu rechnen, dass der Zensus 2011 zu einem zweiten Volkszählungsurteil führen wird.

Aufmerksamkeit verdient auch der Beschluss des Kammergerichts vom 22. August 2010 [1 Ws (B) 51/07 – 2 Ss 23/07; Beck 2010 22034], der die Auskunftspflicht von Berufsgeheimnisträgern gegenüber der Datenschutzbehörde relativiert. Das Bundesverwaltungsgericht beschäftigte sich im Urteil vom 9. Juni 2010 (BvR 6 C 5.09) mit der Verbunddatei „Gewalttäter Sport“ – für die durch die „Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen“ vom 4. Juni 2010 (BKADV; BGBl. I S. 716) mit gleichsam heilender Wirkung eine Rechtsgrundlage geschaffen worden ist. Das Urteil deutet jedoch nicht auf ein distanziertes Verhältnis zum Datenschutz. Das ergibt sich beispielsweise aus dem Beschluss vom 28. Oktober 2010, der im vorangegangenen Tätigkeitsbericht nicht berücksichtigt werden konnte, mit dem das Bundesverwaltungsgericht eine Entscheidung des Europäischen Gerichtshofs eingeholt hat zu der Frage, ob die Richtlinie 2002/22/EG dahingehend auszulegen ist, „dass es den Mitgliedstaaten erlaubt ist, Unternehmen, die Teilnehmern Telefonnummern zuweisen, zu verpflichten, Daten von Teilnehmern, denen dieses Unternehmen nicht selbst Telefonnummern zugewiesen hat, zum Zwecke der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten Teilnehmerverzeichnisse zur Verfügung zu stellen, soweit diese Daten dem Unternehmen vorliegen“.

Auf allgemeines Interesse sollte auch die Entscheidung des VG Wiesbaden vom 6. Oktober 2010 (6 K 280/10.WI, 6 K 280/10; BeckRs 2010, 54526) stoßen. Darin wird moniert, dass eine Rechtsgrundlage, die eine Datenübermittlung an die Nato erlaubt, im BKA-Gesetz fehle.

Prozessual interessant ist ferner das Urteil des VG Wiesbaden vom 4. März 2010 (6 K 1371/09.WI), mit dem ein Kostenerstattungsanspruch im Verfahren über die Löschung personenbezogener Daten nach dem Schengener Durchführungsübereinkommen bejaht wurde.

2. Europa

2.1
SWIFT-Abkommen

Am 1. August 2010 ist das neue sog. SWIFT-Abkommen in Kraft getreten. Das Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus ermöglicht US-Behörden, Auslandsüberweisungen der Kunden von in Europa tätigen Finanzinstituten zu kontrollieren. Im Vorfeld wurde mein Haus mehrmals unter anderen auch von amerikanischen Behörden um Stellungnahme gebeten.

2.1.1
SWIFT

Die als SWIFT-Abkommen bekannte völkerrechtliche Vereinbarung gilt nicht nur für SWIFT, sondern für jeden Anbieter von internationalen Zahlungsverkehrsdiensten (Art. 3). SWIFT (Society for Worldwide Interbank Financial Telecommunication) ist lediglich der größte und momentan im Abkommen auch der einzig genannte Dienstleister auf diesem Sektor. Es handelt sich um eine in Belgien ansässige internationale Genossenschaft von Geldinstituten, die weltweit täglich ca. 16 Millionen Nachrichten zwischen mehr als 9.000 Finanzinstituten in 200 Ländern abwickelt. Über SWIFT wird nicht – wie häufig in der Diskussion fälschlich angenommen – Geld ausgetauscht, sondern es werden ausschließlich Nachrichten übermittelt. In diesen Nachrichten teilt z. B. eine Bank einer anderen mit, dass für deren Kunde ein Überweisungsauftrag vorliegt, dessen Gegenwert sich die Empfängerbank zu einem bestimmten Termin von einem bestimmten Verrechnungskonto holen und an den Zahlungsempfänger weitergeben möge. Außerdem gibt es Nachrichtentypen für z. B. Kontoauszüge, das Dokumentengeschäft, für Wertpapier- und Devisenhandelsgeschäfte.

2.1.2
TFTP

Bis 2009 betrieb SWIFT sein Telekommunikationsnetz aus zwei Rechenzentren, eines in den Niederlanden und eines in den USA, auf denen die Datenbestände jeweils gespiegelt waren.

Nach den Terroranschlägen am 11. September 2001 in New York entwickelte das US-Finanzministerium das Programm zum Aufspüren der Finanzierung des Terrorismus (Terrorist Finance Tracking Program – TFTP). Das Programm soll dazu beitragen, Terroristen und deren Geldgeber zu ermitteln und zu verfolgen, indem die Geldströme zur Finanzierung des Terrorismus aufgedeckt und überwacht werden. Als wesentliche Informationsquelle nutzt es die bei SWIFT gespeicherten Transaktionsdaten. Das US-Finanzministerium verlangte von SWIFT, gestützt auf eine Verordnung des US-Präsidenten (Executive Order 13224 vom 23. September 2001), unter Strafandrohung (administrative subpoena) die Herausgabe der Daten. Dies geschah jahrelang ohne Kenntnis der Öffentlichkeit. Nachdem US-Zeitungen 2006 den regelmäßigen Zugriff des US-Finanzministeriums auf die SWIFT-Daten enthüllt hatten, reagierte SWIFT auf die nachfolgende Kritik, die nicht nur von Datenschützern und dem Europaparlament geübt wurde, und errichtete ein weiteres Betriebszentrum in der Schweiz. Dort und gespiegelt in den Niederlanden und nicht mehr auf dem Server in den USA werden seit dem Jahreswechsel 2009/2010 die Transaktionsdaten aus Europa gespeichert. Sie sind damit dem Zugriff amerikanischer Behörden entzogen.

2.1.3
Neuverhandlungen

Um sicherzustellen, dass dem US-Finanzministerium auch weiterhin die für das TFTP benötigten Daten zur Verfügung stehen, bedurfte es nunmehr eines internationalen Abkommens. Daher erteilten die 27 Mitgliedstaaten der Europäischen Union dem Vorsitz der EU im Juli 2009 ein Mandat für die Aushandlung eines entsprechenden Abkommens mit den USA. Dem am 30. November 2009 unterzeichneten Interimsabkommen zwischen der Europäischen Union und den USA, das am 1. Februar 2010 in Kraft treten und spätestens nach neun Monaten durch ein langfristiges Abkommen ersetzt werden sollte [KOM (2009) 703 endgültig vom 12. Dezember 2009], verweigerte das Europäische Parlament am 11. Februar 2010 seine Zustimmung (P7_TA(2010)0029; ABl. EG Nr. C 110 E/183 vom 29. April 2010). Die Kommission handelte daraufhin mit den USA ein geändertes Abkommen aus, das am 28. Juni 2010 unterzeichnet wurde, dem das Europäische Parlament am 8. Juli 2010 zugestimmt hat und das am 1. August 2010 in Kraft getreten ist (ABl. EG Nr. L 195 S. 1 vom 27. Juli 2010).

2.1.4
Datenpakete

Das US-Finanzministerium erhält von SWIFT Zahlungsverkehrsdaten und damit verbundene Daten, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Terrorismus und Terrorismusfinanzierung notwendig sind. Dazu gehören Angaben zur Identifizierung des Auftraggebers und des Empfängers (Name, Anschrift, Personalausweis- oder Passnummer), Kontonummern und Informationen über Art und Höhe der Finanztransaktionen. Problematisch ist, dass SWIFT technisch bedingt keine Daten zu einzelnen verdächtigen Personen übermitteln kann, da das Unternehmen in seinen Datenbeständen nicht nach Kriterien wie Name, Anschrift oder Kontonummer suchen kann. SWIFT kann nur Datenpakete mit Daten über eine Vielzahl von Personen zur Verfügung stellen. Es könnten z. B. die Daten zu allen Überweisungen, die in einem definierten Zeitraum aus einer Region wie Frankfurt oder Hessen in ein bestimmtes Land erfolgt sind, an das US-Finanzministerium übermittelt werden. In den USA werden die Datenpakete geöffnet und die Daten der verdächtigen Personen extrahiert. Folglich werden weit überwiegend Bankdaten unbescholtener Bürger an das US-Finanzministerium übermittelt und können dort bis zu fünf Jahre gespeichert bleiben (Art. 6 Abs. 4 des Abkommens).

2.1.5
Übermittlungsverfahren

Die Datenübermittlung erfolgt auf Antrag. Das US-Finanzministerium stellt dem Anbieter eines internationalen Zahlungsverkehrsdienstes im Hoheitsgebiet der USA eine Vorlageanordnung (production order) zu. Darin müssen die angeforderten Datenkategorien bezeichnet sein, es muss begründet sein, warum die Daten zur Verhütung, Ermittlung, Aufdeckung und Verfolgung von Terrorismus und Terrorismusfinanzierung notwendig sind und das Ersuchen muss so eng wie möglich gefasst sein, um die Menge der angeforderten Daten auf ein Minimum zu beschränken. Daten, die sich auf den Einheitlichen Euro-Zahlungsverkehrsraum beziehen (Single Euro Payments Area – SEPA), dürfen nicht angefordert werden. Es geht bei dem SWIFT-Abkommen mithin nur um Auslandsüberweisungen in Drittstaaten außerhalb der EU; Inlandsüberweisungen oder Überweisungen innerhalb der EU werden nicht erfasst. Zeitgleich schickt das US-Finanzministerium eine Kopie des Ersuchens an EUROPOL. Die europäische Polizeibehörde überprüft, ob das Ersuchen die Anforderungen des Abkommens erfüllt. Erst nachdem EUROPOL dem Anbieter bestätigt hat, dass das Ersuchen rechtmäßig ist, wird es in der EU und den USA wirksam und verpflichtet den Anbieter zur Datenübermittlung. Kritisch ist, dass die Kontrollkompetenz mit EUROPOL einer Institution übertragen worden ist, die selbst als Strafverfolgungsbehörde an den Ergebnissen, die US-

Fahnder aus den SWIFT-Daten gewinnen, interessiert ist und darauf zugreifen kann (s. a. Ziff. 2.4). EUROPOL ist berechtigt, einen Verbindungsbeamten zum US-Finanzministerium zu entsenden.

2.1.6
Verarbeitungsbedingungen

Die übermittelten Daten unterliegen einer Zweckbindung. Das US-Finanzministerium darf die Daten nur für Zwecke der Terrorismusbekämpfung verwenden. Die Daten dürfen nicht mit anderen Datenbanken verknüpft und weder bearbeitet, verändert noch ergänzt werden. Datamining und jede andere Art automatischer Profilerstellung oder computergestützter Filterung schließt das Abkommen ausdrücklich aus. TFTP-Daten dürfen nur an die für Strafverfolgung, öffentliche Sicherheit und Terrorismusbekämpfung zuständigen Behörden in den USA, den EU-Mitgliedstaaten und Drittstaaten, EUROPOL, EUROJUST und entsprechenden anderen internationalen Einrichtungen weitergegeben werden. Rohdaten dürfen nicht weitergegeben werden, sondern nur die Ergebnisse einer individualisierten Suchabfrage. Gewinnt das US-Finanzministerium über das TFTP Informationen, die der Europäischen Union bei der Terrorismusbekämpfung nützlich sein können, muss es diese den zuständigen Behörden so schnell wie möglich zur Verfügung stellen. Diese Behörden können ihrerseits das US-Finanzministerium um TFTP-Suchabfragen ersuchen, die das Ministerium unverzüglich auszuführen hat.

2.1.7
Auskunfts- und Beschwerderechte

Das Abkommen räumt den von einer Datenverarbeitung im Rahmen des TFTP Betroffenen ein Auskunfts- und Beschwerderecht ein. Der Antrag auf Auskunft ist an die zuständige nationale Datenschutzbehörde zu richten, die ihn an den Datenschutzbeauftragten des US-Finanzministeriums weiterleitet. Gleiches gilt für das Ersuchen auf Berichtigung, Löschung oder Sperrung. Der Datenschutzbeauftragte des US-Finanzministeriums teilt der nationalen Behörde unverzüglich mit, ob die Auskunft erteilt werden kann bzw. die Daten berichtigt, gesperrt oder gelöscht worden sind. Gegen die Entscheidung des US-Finanzministeriums können EU-Bürger mit denselben administrativen und gerichtlichen Rechtsmitteln vorgehen wie US-Bürger. Der Datenschutzbeauftragte muss in seiner Mitteilung die Rechtsbehelfe benennen.

2.1.8
Laufzeit

Das Abkommen gilt zunächst für fünf Jahre und verlängert sich automatisch um jeweils ein Jahr, sofern nicht eine Partei sechs Monate vor Ablauf eines Einjahreszeitraums der anderen Partei ihre Absicht mitteilt, das Abkommen nicht zu verlängern. Außerdem kann jede Partei das Abkommen mit einer Frist von sechs Tagen kündigen.

2.1.9
Evaluierung und Kontrollen

Spätestens sechs Monate nach Inkrafttreten des Abkommens und danach in regelmäßigen Abständen haben die Kommission und das US-Finanzministerium gemeinsam die im Abkommen enthaltenen Garantien, Kontrollen und Reziprozitätsbestimmungen zu evaluieren. Der Überprüfungsdelegation der EU müssen Vertreter von zwei Datenschutzbehörden angehören. Die Bewertungskriterien sind im Abkommen detailliert festgelegt. Die USA haben sich außerdem damit einverstanden erklärt, die Einhaltung der Zweckbindung und der im Abkommen garantierten Verarbeitungsbedingungen durch unabhängige Prüfer kontrollieren zu lassen. Einer der Prüfer soll von der Europäischen Kommission ernannt werden. Das Europäische Parlament hat seine Zustimmung zum Abkommen mit der Empfehlung an die Kommission verbunden, ihm drei Bewerber für die Position der unabhängigen Person zu benennen. Das Parlament ist der Ansicht, da Art. 8 der Charta der Grundrechte der EU verlange, dass die Verarbeitung personenbezogener Daten der Überwachung einer unabhängigen Stelle unterliege, das Verfahren dem entsprechen müsse, das vom Europäischen Parlament und dem Rat für die Ernennung des Europäischen Datenschutzbeauftragten durchgeführt wurde (Legislative Entschließung des Europäischen Parlaments vom 8. Juli 2010, P7_TA(2010)0279).

Spätestens drei Jahre nach Inkrafttreten des Abkommens haben Kommission und US-Finanzministerium außerdem einen gemeinsamen Bericht über den Nutzen der bereitgestellten TFTP-Daten unter besonderer Berücksichtigung des Nutzens der Daten, die mehrere Jahre gespeichert worden sind, zu erstellen.

2.1.10
Europäisches Auswertungssystem

Im Abkommen wird die Europäische Kommission verpflichtet, eine Studie über die mögliche Einführung eines dem TFTP vergleichbaren EU-Systems durchzuführen, das eine gezieltere Datenübermittlung erlauben würde. Sollte sich im Anschluss die EU für die Einführung eines eigenen Systems entscheiden, wollen die USA dabei behilflich sein. In der vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments abgegebenen Empfehlung vom 5. Juli 2010 zu dem Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens (A7-0224/2010) teilt der Berichterstatter mit, dass der Rat und die Kommission rechtsverbindlich zugesagt hätten, einen rechtlichen und technischen Rahmen einzurichten, um die Extraktion von Daten auf europäischem Boden zu ermöglichen. Dadurch werde mittelfristig gewährleistet, dass keine Übermittlung großer Datenmengen an US-Behörden mehr vorkämen. Die Kommission werde nach einem Jahr einen Vorschlag für den rechtlichen und technischen Rahmen vorlegen. Nach drei Jahren werde die Kommission einen Fortschrittsbericht über das Extraktionssystem der EU erstellen. Dieser Bericht ermögliche dem Parlament, zu überprüfen, ob Kommission und Rat ihre Zusagen eingehalten hätten und evtl. Änderungen am Abkommen mit den USA zu verlangen.

2.1.11
Abwägung

Bei aller Kritik am SWIFT-Abkommen darf nicht außer Acht gelassen werden, dass das Terrorist Finance Tracking Program der USA ein wirksames Instrument im Kampf gegen den Terrorismus zu sein scheint und die Europäische Union über kein gleichwertiges Datenauswertungssystem verfügt. Laut einer Presseerklärung des Rates der EU (Informationsvermerk vom November 2009) sind aufgrund des Programms zum Aufspüren der Finanzierung des Terrorismus bis Ende 2009 mehr als 1.450 Hinweise an Regierungen in Europa und 800 Hinweise an nichteuropäische Regierungen ergangen. Informationen aus dem TFTP hätten europäischen Behörden in hohem Maße bei den Ermittlungen im Zusammenhang mit geplanten Anschlägen der Al-Quaida auf Transatlantikflüge zwischen der EU und den USA geholfen. Mit Hilfe der TFTP-Daten sollen auch die Aktivitäten der sog. Sauerland-Gruppe, eine Terrorzelle der radikal-islamistische Vereinigung islamische Dschihad-Union 2007 aufgedeckt worden sein. Die Gruppe plante Sprengstoffanschläge in Deutschland.

2.2
Einheitlicher Rechtsrahmen für den Datenschutz auf europäischer Ebene

Die Europäische Kommission plant einen neuen einheitlichen Rechtsrahmen für den Datenschutz. Dabei wird auch eine Neuorganisation der datenschutzrechtlichen Kontrolle im Bereich der polizeilichen und justiziellen Zusammenarbeit angestrebt.

Der am 1. Dezember 2009 in Kraft getretene Vertrag von Lissabon verändert die bisherigen europäischen Verträge. Eine der wichtigen Änderungen für den Datenschutz besteht darin, dass die bisherige Säulenstruktur wegfällt und somit der Bereich der polizeilichen und justiziellen Zusammenarbeit vergemeinschaftet wird.

Die Kommission hat diese Änderung des Primärrechts zum Anlass genommen ein Projekt zu starten, um neue einheitliche Datenschutzregelungen für Europa zu schaffen. Grundlage dafür ist Art. 16 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

Art. 16 Abs. 2 AEUV

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

Nach Erklärung 20 zu Art. 16 AEUV sind beim Erlass von Vorschriften Auswirkungen auf die nationale Sicherheit gebührend zu berücksichtigen. In Erklärung 21 wird angemerkt, dass es erforderlich sein könnte, im Bereich der polizeilichen und justiziellen Zusammenarbeit spezifische auf Art. 16 AEUV gestützte Vorschriften zu erlassen.

Derzeit sieht es danach aus, dass der zu schaffende neue Rechtsrahmen grundsätzlich sowohl für die ehemalige Erste Säule als auch für die ehemalige Dritte Säule, also die polizeiliche und justizielle Zusammenarbeit, gelten soll. Übereinstimmung herrscht auch darüber, dass es für den Bereich der Datenverarbeitung bei den Sicherheitsbehörden spezielle Datenschutzregelungen geben soll; bspw. wäre das Auskunftsrecht für die

Betroffenen – wie auch im deutschen Recht – bereichsspezifisch mit den aus Sicht der Sicherheitsbehörden erforderlichen Einschränkungen zu regeln.

Gleichfalls in der Diskussion ist in diesem Zusammenhang eine Neuordnung der verschiedenen im Bereich der polizeilichen und justiziellen Zusammenarbeit bestehenden datenschutzrechtlichen Kontrollinstanzen, wie den Gemeinsamen Kontrollinstanzen für EUROPOL, Schengen, Zoll, EUROJUST. Meine Mitarbeiterin war als derzeitige Vorsitzende der Gemeinsamen Kontrollinstanz Schengen zu mehreren Anhörungen der Kommission, insbesondere auch der zuständigen Kommissarin Viviane Reding, geladen. Sie hat sich dabei für eine effiziente und bürgerfreundliche Datenschutzkontrolle ausgesprochen. Vieles spricht dafür, es bei dem Modell der Gemeinsamen Kontrollinstanz zu belassen, die verschiedenen bestehenden Instanzen aber – soweit dies ihre Besonderheiten zulassen – zusammen zu führen. Vorteil dieser Konstruktion ist, dass die Mitgliedstaaten, um deren Daten es zum großen Teil geht, auf diese Weise unmittelbar an der Kontrolle der Datenverarbeitung auf europäischer Ebene beteiligt werden. Für eine Zusammenlegung sprechen sowohl Synergieeffekte, als auch ein Mehr an Bürgerfreundlichkeit, da es der Bürger dann nur noch mit einer Instanz zu tun hat. Eine wirksame Kontrolle setzt eine entsprechende persönliche und sachliche Ausstattung sowohl des Sekretariats der Gemeinsamen Kontrollinstanz als auch der nationalen Datenschutzbeauftragten voraus.

Fest steht auch, dass ein beratendes Gremium (für die Kommission, den Rat und das Parlament), ähnlich wie es für den Bereich der ehemaligen Ersten Säule in Form der Artikel 29-Gruppe seit langem existiert, dringend vonnöten ist.

Die Kommission hat im November 2010 eine Mitteilung über ein Gesamtkonzept für den Datenschutz in der Europäischen Union vorgelegt (BRDrucks. 707/10). Mitte 2011 soll ein Entwurf für einen Rechtsakt zur Diskussion gestellt werden.

2.3
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. Meine Mitarbeiterin ist derzeit Vorsitzende der Kontrollinstanz.

Der Beitrag stellt die Arbeitsschwerpunkte der Sitzungen der Kontrollinstanz im Berichtszeitraum dar.

2.3.1
Schengener Informationssystem der zweiten Generation (SIS II)

In den letzten Tätigkeitsberichten (u. a. 37. Tätigkeitsbericht, Ziff. 2.1.1.1; 38. Tätigkeitsbericht, Ziff. 2.2.1) hatte ich von unterschiedlichen Prognosen für den Ausbau des SIS zu einem leistungsfähigeren SIS II berichtet. Zeitweise stand die Realisierung von SIS II ganz in Frage, da die erforderlichen Tests unbefriedigend ausfielen. Dann wieder wurden der Zeitrahmen verlängert und erneute Tests angesetzt. Im Oktober 2010 hat das Europäische Parlament eingegriffen und beschlossen, die für 2011 vorgesehenen 30 Millionen Euro für das SIS II zu sperren. Diese Summe soll für die Einrichtung der neuen Datenbank erst dann freigegeben werden, wenn die EU-Kommission einen realistischen und verbindlichen Zeitplan für die Fertigstellung des Informationssystems präsentiert. Aber auch nach positiver Einschätzung soll SIS II vor Mitte des Jahres 2013 keinesfalls betriebsbereit sein.

2.3.2
Gemeinsame Überprüfung der Ausschreibungen von Drittausländern zur Einreiseverweigerung

Im 37. Tätigkeitsbericht (Ziff. 2.1.1.3) hatte ich berichtet, dass die GK einen follow-up-check, der im Jahr 2004 schengenweit vorgenommenen Prüfung der Ausschreibungen nach Art. 96 SDÜ vornehmen will. Bei der Ausschreibungskategorie nach Art. 96 handelt es sich um Ausschreibungen von Drittausländern, die zur Einreiseverweigerung ausgeschrieben sind. Das Prüfverfahren zog sich lange hin, da einzelne Schengen-Länder die erforderlichen Prüfungen nicht fristgerecht durchführten. Im Herbst 2010 konnte der Prüfbericht endlich abgeschlossen werden. Eine der wichtigsten darin aufgestellten Forderungen besteht darin, die in jedem Land nach nationalem Recht festgelegten Fristen für die Ausschreibung anzugleichen, um eine einheitliche Anwendung zu gewährleisten. Die meisten Fehler fanden sich immer noch bei dem nicht rechtmäßig angewandten Verfahren zur Löschung bzw. zur Überprüfung, ob die weitere Speicherung noch erforderlich ist.

2.3.3
Gemeinsame Überprüfung der Ausschreibungen zur Auslieferungsfestnahme

In ihrer Oktobersitzung hat die GK weiterhin eine gemeinsame Überprüfung von Ausschreibungen nach Art. 95 SDÜ beschlossen. Dabei geht es um Personen, die wegen einer Straftat mit Haftbefehl gesucht werden.

Die Personenausschreibungskategorie hat nach den Ausschreibungen von Drittausländern zur Einreiseverweigerung (Art. 96 SDÜ) die meisten Datensätze: Im Jahr 2010 betrug die Zahl für Deutschland 5.168.

Art. 95 Abs. 1 und 2 SDÜ

(1) Daten in Bezug auf Personen, um deren Festnahme mit dem Ziel der Auslieferung ersucht wird, werden auf Antrag der Justizbehörde der ersuchenden Vertragspartei aufgenommen.

(2) …..Die ausschreibende Vertragspartei teilt den ersuchten Vertragsparteien gleichzeitig mit der Ausschreibung auf möglichst schnellem Wege folgende für den zugrunde liegenden Sachverhalt wesentliche Informationen mit:

a) die um die Festnahme ersuchende Behörde;
b) das Bestehen eines Haftbefehls oder einer Urkunde mit gleicher Rechtswirkung oder eines rechtskräftigen Urteils;
c) die Art und die rechtliche Würdigung der strafbaren Handlung;
d) die Beschreibung der Umstände, unter denen die Straftat begangen wurde; einschließlich der Zeit, des Orts und der Art der Täterschaft;
e) soweit möglich die Folgen der Straftat.

Bei dem in Abs. 2 angesprochenen Haftbefehl handelt es sich um einen nationalen Haftbefehl, der in den europäischen Haftbefehl umgewandelt wird. Mit diesem wird vor allem das Ziel verfolgt, eine einfachere und schnellere Auslieferung der gesuchten Person zu erreichen.

Im Rahmen der geplanten konzertierten Kontrolle sollen eine Vielzahl von Fragestellungen geprüft werden: Rechtmäßigkeit der Ausschreibung, Verfahren der Ausstellung des europäischen Haftbefehls, Einhaltung der Löschungsvorschriften und andere. Der entsprechende Fragebogen wird derzeit entwickelt und soll im nächsten Jahr als Grundlage für eine Überprüfung in allen Schengen-Ländern dienen.

2.3.4

Regelmäßiger Abgleich der Meldevordrucke in Hotels mit dem Schengener Informationssystem

Eine Delegation in der GK warf die Frage auf, ob die in Hotels von den Logiergästen auszufüllenden Meldevordrucke regelmäßig mit dem SIS abgeglichen werden dürfen, oder ob dies nur erfolgen darf, wenn bestimmte Anhaltspunkte für eine Gefahrenlage oder bestimmte Verdachtsgründe bestehen. Hintergrund der Frage ist, dass nach derzeitigem Stand in mehreren Schengen-Ländern ein regelmäßiger Abgleich mit dem SIS stattfindet.

Im SDÜ findet sich bei den allgemeinen Übermittlungsvorschriften außerhalb des SIS eine für den vorliegenden Fall einschlägige Vorschrift.

Art. 45 Abs. 1 SDÜ

Die Vertragsparteien verpflichten sich, die erforderlichen Maßnahmen zu ergreifen, um sicherzustellen, dass

a) der Leiter einer Beherbergungsstätte oder seine Beauftragten darauf hinwirken, dass beherbergte Ausländer, einschließlich der Angehörigen anderer Vertragsparteien sowie anderer Mitgliedstaaten der Europäischen Gemeinschaften, soweit es sich nicht um mitreisende Ehegatten und minderjährige Kinder sowie Teilnehmer von Reisegesellschaften handelt, Meldevordrucke eigenhändig ausfüllen und unterschreiben und sich dabei gegenüber dem Leiter der Beherbergungsstätte oder seinem Beauftragten durch Vorlage eines gültigen Identitätsdokuments ausweisen;

b) die nach Buchstabe a ausgefüllten Meldevordrucke für die zuständigen Behörden bereitgehalten oder diesen übermittelt werden, wenn dies nach deren Feststellung für Zwecke der Gefahrenabwehr, der Strafverfolgung oder der Aufklärung des Schicksals von Vermissten oder Unfallopfern erforderlich ist, soweit im nationalen Recht nichts anderes geregelt ist.

Nach Auffassung der GK kann der Wortlaut des Art. 45 SDÜ nicht derart ausgelegt werden, dass in jedem Fall eine Übermittlung der ausgefüllten Meldevordrucke durch die Hotels an die zuständigen Behörden bzw. ein Abgleich mit dem SIS erfolgen kann. Voraussetzung für ein derartiges Vorgehen ist eine besondere Situation, aus der sich bestimmte Anhaltspunkte

ergeben, z. B., dass sich eine verdächtige Person in einem räumlich begrenzten Bereich aufhält.

Eine weitergehende Frage ist, ob es Art. 45 Abs. 1 Buchst. b SDÜ zulässt, dass im nationalen Recht eine anlasslose Übermittlung an die zuständigen Behörden und ein regelmäßiger Abgleich mit SIS vorgesehen wird. Die deutschen Gesetzgebungsorgane haben eine derartige Regelung im Melderechtsrahmengesetz (MRRG) und im hessischen Meldegesetz (HMG) nicht vorgenommen.

§ 16 Abs. 3 MRRG

Die nach den Absätzen 1 und 2 erhobenen Angaben dürfen nur von den dort genannten Behörden für Zwecke der Gefahrenabwehr oder der Strafverfolgung sowie zur Aufklärung der Schicksale von Vermissten und Unfallopfern ausgewertet und verarbeitet werden, soweit durch Bundes- oder Landesrecht nichts anderes bestimmt ist.

Die entsprechende Vorschrift im hessischen Meldegesetz lautet:

§ 27 Abs. 3 HMG

Die Meldescheine sind von den Verantwortlichen in den Beherbergungsstätten für die Polizeibehörden und Dienststellen, die Staatsanwaltschaft und Meldebehörden zur Einsichtnahme bereitzuhalten. Auf Verlangen sind sie den Polizeibehörden und Dienststellen und den Staatsanwaltschaften zur Mitnahme auf die Dienststelle auszuhändigen und erforderlichenfalls im Einzelfall zum Verbleib zu überlassen.

Hieraus ergibt sich, dass der Gesetzgeber nur eine Übermittlung im Einzelfall zulassen wollte, die an besondere Voraussetzungen gebunden ist.

Die Frage, ob auch eine nationale Regelung anderen Inhalts mit Art. 45 Abs. 1 Buchst. b SDÜ vereinbar wäre, wird von der GK noch geprüft.

2.4
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.

2.4.1
Zugriff von EUROPOL auf das Schengener Informationssystem

EUROPOL hat schon seit einigen Jahren Zugriff auf verschiedene Ausschreibungskategorien im Schenger Informationssystem (SIS). Bisher erfolgt der Zugriff in einem webbasierten System mit eigenen, nur diesen Zugriffen vorbehaltenen Terminals. Es besteht keine Verbindung der PCs zu den sonstigen Informationssystemen von EUROPOL. Die zuständigen EUROPOL-Beamten müssen demgemäß ihren Arbeitsplatz verlassen, um an dem speziellen Rechner den Zugriff auf das SIS vorzunehmen.

EUROPOL hat der GK jetzt einen Vorschlag unterbreitet, in dem die physikalische Trennung der Systeme aufgehoben wird, die EUROPOL-Beamten also von einem Terminal sowohl in das Informationssystem von EUROPOL als auch in das SIS gelangen können. Dieser geplante Zugriff auf das SIS müsste mit den Vorgaben des SDÜ vereinbar sein. Die einschlägige Vorschrift lautet:

Art. 101a Abs. 6 SDÜ

Europol ist verpflichtet,

...

b) unbeschadet der Absätze 4 und 5 es zu unterlassen, Teile des Schengener Informationssystems, zu denen es Zugang hat, oder die hierin gespeicherten Daten, auf die es Zugriff hat, mit einem von oder bei Europol betriebenen Computersystem für die Datenerhebung und -verarbeitung zu verbinden bzw. in ein solches zu übernehmen oder bestimmte Teile des Schengener Informationssystems herunterzuladen oder in anderer Weise zu vervielfältigen;

...

Die GK prüft derzeit, ob die geplante allenfalls logische Trennung diesen Vorgaben entspricht. Fest steht, dass Teile des Schengener Informationssystems nicht mit einem Computersystem

von EUROPOL verbunden werden dürfen, um beispielsweise einen automatisierten Abgleich mit SIS zu verhindern. Für die Frage, ob ein derartiges Verbot auch für eine technische Verbindung zwischen EUROPOL und SIS besteht, kommt es insbesondere auf die Ausgestaltung an. Hier holt die GK Informationen bei EUROPOL ein.

2.4.2
Einbeziehung von EUROPOL in das SWIFT-Abkommen mit den USA

Die GK hat sich weiterhin mit der Rolle von EUROPOL im Abkommen zwischen der EU und den USA über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der EU an die USA im sog. SWIFT- bzw. TFTP-Abkommen (Terrorist Finance Tracking Program; s. Ziff. 2.1) beschäftigt.

Nach diesem Abkommen hat EUROPOL die Aufgabe, Ersuchen der USA um Übermittlung von Zahlungsverkehrsdaten an den Dienstleister SWIFT, auf ihre Konformität mit dem TFTP-Abkommen zu überprüfen. Zum Anderen erhält EUROPOL Informationen von den USA aus dem TFTP für seine eigenen Aufgaben. Hier steht nach Auffassung der GK nicht fest, ob und inwieweit die EUROPOL nach dem Abkommen zugewiesene Prüfungstätigkeit von der Datenverarbeitung nach dem EUROPOL-Mandat getrennt wird.

Es steht weiterhin nicht fest, welche datenschutzrechtliche Kontrollinstanz die Prüfungstätigkeit von EUROPOL überwacht. Da das Abkommen eine rechtlich eigenständige Regelungsmaterie begründet und keine Bezugnahme auf den EUROPOL-Beschluss enthält, bedarf die Frage der Klärung, ob insoweit die Kontrollkompetenz der GK gegeben ist.

Unklar ist weiterhin, wie das im Abkommen vorgesehene Auskunftsrecht für die Bürger hinsichtlich der von den US-Behörden gespeicherten Daten umgesetzt wird.

Die GK hat deshalb beschlossen, einen Kontrollbesuch bei EUROPOL vorzunehmen, um diese Fragen zu klären. Dabei wird EUROPOL auch aufgefordert, die Kriterien offenzulegen nach denen die oben beschriebene Prüfung der Übermittlung von Zahlungsverkehrsdaten stattfindet.

2.4.3
Grundsatz der Verfügbarkeit von Informationen

Auch für EUROPOL ergeben sich Konsequenzen aus dem erstmals im Haager Programm (ABl. EG 2005/C 53/01 vom 3. März 2005) aufgestellten Verfügbarkeitsgrundsatz. Nach dieser Prämisse soll der Austausch strafverfolgungsrelevanter Informationen überall in der EU nach denselben Bedingungen erfolgen. Grundsätzlich sollen die zuständigen Behörden in einem Mitgliedstaat die für ihre Arbeit erforderlichen Informationen, über die ein anderer Staat verfügt, für den von ihnen erklärten Zweck erhalten können.

Es gibt derzeit Pläne, diesen Grundsatz für EUROPOL fruchtbar zu machen. Dabei geht es um den Abgleich von Daten mit Informationen in anderen Informationssystemen auf europäischer, später auch auf nationaler Ebene.

In einer ersten Phase sollen alle bei EUROPOL eingehenden Informationen mit den dort in verschiedenen Informationssammlungen existierenden Daten abgeglichen werden. In einer zweiten Phase sollen Daten von EUROPOL mit Informationen, die in anderen europäischen Informationssystemen gespeichert sind, wie bspw. SIS oder Interpol abgeglichen werden. Der dritte Schritt wäre der Abgleich von EUROPOL-Daten mit den in Frage kommenden nationalen Informationssystemen.

Während Phase 2 und 3 noch in der Zukunft liegen und es grundlegender gesetzgeberischer Änderungen bedürfte, sind die Pläne für Phase 1 konkret. Die GK ist in die Prüfung dieses Vorhabens einbezogen.

2.4.4
Kontrolle von EUROPOL

Die GK hat im Jahr 2010 wieder eine Kontrolle bei EUROPOL durchgeführt. Der Bericht über diese Kontrolle ist vertraulich.

3. Bund

3.1
Ausbau des Nachrichtendienstlichen Informationssystems NADIS zu einem Wissens- und Informationsmanagementsystem

Das Nachrichtendienstliche Informationssystem NADIS, an dem sich das Bundesamt für Verfassungsschutz und die Landesämter beteiligen, wird von einer einfachen Aktenhinweisdatei zu einem modernen Wissens- und Informationsmanagementsystem ausgebaut. Dieser Ausbau birgt auch datenschutzrechtliche Probleme.

3.1.1
NADIS – bisheriges System

NADIS ist ein seit Anfang der 1970er-Jahre betriebenes Datenverbundsystem, an dem alle Verfassungsschutzbehörden des Bundes und der Länder im automatisierten Verfahren beteiligt sind. Nach § 6 BVerfSchG sind die Verfassungsschutzbehörden des Bundes und der Länder verpflichtet, zum Zwecke der gegenseitigen Unterrichtung beim BfV eine gemeinsame Datei zu führen. Diese Datei ist derzeit eine sog. Hinweisdatei, die dem Auffinden von Akten und der dazu notwendigen Identifizierung von Personen im Rahmen der Aufgabenerfüllung des Verfassungsschutzes dient. Sie darf ausschließlich die Daten enthalten, die für diese Zwecke erforderlich sind. Dazu zählen die – allerdings „sprechenden“ – Aktenzeichen der bei der aktenführenden Stelle vorhandenen Aktenbestände und personenbezogene Grunddaten der Betroffenen. Angaben zum Inhalt der Akten, die über die Aktenfundstelle und die personenbezogenen Grunddaten hinausgehen, dürfen aus NADIS nicht ersichtlich sein. Derartige Informationen können die Verbundteilnehmer bei begründetem Anlass nur durch eine Einzelfallanfrage bei der aktenführenden Stelle einholen. Anfang 2008 waren vom Bund und den Ländern gemeinsam in NADIS über eine Millionen personenbezogene Eintragungen enthalten, davon mehr als 50 Prozent aufgrund von Sicherheitsüberprüfungen.

3.1.2
Künftiges Konzept – NADIS als Wissensnetz (NADIS-WN)

Nach Aussage von Vertretern des BMI und des LfV ist die heute eingesetzte Technik von NADIS veraltet und nicht mehr in der Lage, den gewachsenen Anforderungen zur

Sicherstellung eines auch zukünftig leistungsfähigen Verfassungsschutzverbunds gerecht zu werden. Pläne für ein Nachfolgesystem existieren deshalb seit mehreren Jahren. Bekannt ist mir ein Konzept aus dem Jahr 2007, in dem die neuen fachlichen Anforderungen näher beschrieben sind. Im April 2008 stoppte Bundesinnenminister Schäuble die Planung des Nachfolgesystems NADIS-WN aus Kostengründen. Über die Wiederaufnahme der Arbeiten wurde endgültig 2009 entschieden.

3.1.2.1
Das System

Das derzeit im Aufbau befindliche Wissens- und Informationsmanagementsystem ist ein modernes Wissensnetz. Es beinhaltet ein Dokumentenmanagementsystem zur Bearbeitung der Akten in digitaler Form und dient außerdem der Optimierung der Arbeitsabläufe. Ein weiterer Vorteil ist die strukturierte Erfassung von Informationen zum Beispiel in Form von Katalogen. Dadurch lassen sich die hinterlegten Informationen umfassend analysieren: In Sekundenschnelle können die vielfältigen Beziehungen zwischen Personen und Sachen hergestellt und grafisch dargestellt werden. Die Funktionalität ist daher mit einem einfachen Hinweissystem nicht mehr zu vergleichen.

Die Entwicklung des Gesamtsystems, das in fünf Versionen bis zur kompletten Ausbaustufe im Fachkonzept beschrieben ist, erfolgt zentral durch das BMI unter Beteiligung der Bundesländer. NADIS-WN soll im Oktober 2011 in einer ersten Version (WN 1.0) in Wirkbetrieb gehen. Das System soll in weiteren Ausbaustufen die Möglichkeit bieten, einzelne Amtsdateien des BfV und der Landesämter für Verfassungsschutz abzulösen bzw. zu integrieren.

Bei der Umsetzung und Programmierung werden schon heute zukünftige Anforderungen technisch berücksichtigt und zum Teil auch schon realisiert. Alle Funktionalitäten können heute noch nicht abschließend benannt werden. Es gibt zurzeit mehrere länderübergreifende Arbeitsgruppen, die die Einführung des Projektes fachlich unterstützen. Die Programmierung erfolgt schrittweise und die einzelnen Releases werden in den verschiedenen LfV auf ihre Funktionalität hin getestet. Die Testergebnisse führen zu weiteren Anforderungen. Diese werden zeitnah angepasst, da es sich hierbei um eine sog. agile Softwareentwicklung handelt.

Datenschutzrechtlich wird das Projekt vom BfDI begleitet, die Landesdatenschutzbeauftragten sind lediglich über Ihre LfV beteiligt. Leider ist das BMI der Aufforderung des BfDI und der LfD

nicht gefolgt, – wie es bei der Konzeption einer Verbunddatei sinnvoll wäre – auch einige LfD an den Beratungen zwischen BfDI und BMI teilnehmen zu lassen. Stattdessen soll eine zweimal jährlich erfolgende Unterrichtung durch die Gesamtprojektleitung für NADIS-WN in einem Arbeitskreis des BfDI und der LfD erfolgen.

3.1.2.2
Rechtliche Probleme

3.1.2.2.1
Textdatei

Das BVerfSchG enthält in der für Verbunddateien zwischen Bund und Ländern einschlägigen Norm verschiedene Einschränkungen. Die hier maßgebliche Restriktion lautet:

> § 6 Satz 1 und 8 BVerfSchG
>
> Die Verfassungsschutzbehörden sind verpflichtet, beim Bundesamt für Verfassungsschutz zur Erfüllung der Unterrichtungspflichten nach § 5 gemeinsame Dateien zu führen, die sie im automatisierten Verfahren nutzen. Diese Dateien enthalten nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind.
> …
> Die Führung von Textdateien oder Dateien, die weitere als die in Satz 2 genannten Daten enthalten, ist unter den Voraussetzungen dieses Paragraphen nur zulässig für eng umgrenzte Anwendungsgebiete zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten.

Danach geht das Gesetz als Regelfall von der Aktenhinweisdatei aus und lässt nur für bestimmte Ausnahmen Textdateien zu. Ausgeschlossen ist de lege lata z. B. das Führen einer Textdatei für einen relativ umfangreichen Aufgabenbereich des Verfassungsschutzes, nämlich die Beobachtung des nichtgewalttätigen Extremismus. Im Widerspruch hierzu sieht die technische Ausgestaltung von NADIS-WN einen Einsatz für alle Aufgabenbereiche des Verfassungsschutzes vor. Bis zu einer Gesetzesnovellierung will man bei der Nutzung des Systems allerdings die sich aus der geltenden Rechtslage ergebenden Beschränkungen einhalten.

Nach meinem Kenntnisstand gibt es derzeit noch keine konkreten Pläne für eine entsprechende Änderung des § 6 Satz 8 BVerfSchG.

Diese Vorgehensweise bedeutet, dass die Technik mit umfangreichen Investitionen vorangeht und dem Gesetzgeber – will er die Investitionen nicht ins Leere laufen lassen – nichts anderes übrig bleibt, als die erforderliche Neuregelung vorzunehmen. Nicht nur aus rechtsstaatlichen Gründen, sondern auch aus datenschutzrechtlicher Sicht halte ich dies für ein problematisches Vorgehen, da die Erforderlichkeit der neuen Technik und weitere Datenschutzgesichtspunkte im Gesetzgebungsverfahren nicht mehr gebührend geprüft werden können.

3.1.2.2.2
Volltext-Recherche

Im Rahmen von NADIS-WN ist die Verarbeitung von ganzen Texten und die Aufnahme von sog. Ursprungsdokumenten in die Datei geplant. Dies hat zur Folge, dass theoretisch nach jedem in einem Dokument vorkommenden Wort oder Datum elektronisch gesucht werden kann, weil das Dokument als Ganzes erfasst wird. In den Akten des Verfassungsschutzes finden sich aber auch Daten unbeteiligter Personen, die nur aufgrund eines zufälligen Zusammenhangs mit der Zielperson erhoben wurden. Würden die Daten dieser unbeteiligten Personen gezielt elektronisch recherchierbar, bedeutete dies einen Paradigmenwechsel: Nach geltender Rechtslage im Bund und in den Ländern dürfen die Verfassungsschutzbehörden nur unter bestimmten Voraussetzungen Daten erheben und verarbeiten, insbesondere wenn bestimmte Anhaltspunkte für ein verfassungsfeindliches Verhalten in der Person des Betroffenen vorliegen. Die zu speichernden Datenarten und Datenfelder werden genau festgelegt und die Datenschutzbeauftragten sind daran zu beteiligen.

Durch eine Volltext-Recherche würden diese datenschutzrechtlichen Sicherungen aufgegeben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Hinzu kommt, dass bei ungenauen Suchbegriffen oder falschen Schreibweisen von Namen eine Vielzahl von Treffern angezeigt würde, die für die Aufgabenerfüllung nicht erforderlich sind. Für die ggf. gänzlich unverdächtigen Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Die Möglichkeiten einer Volltext-Recherche in allen Dokumenten sollte deshalb für NADIS-WN ausgeschlossen sein (s. Entschließung der DSB-Konferenz vom 3./4. November 2010, Ziff. 9.13).

3.2
Verordnung zu § 7 Abs. 6 BKA-Gesetz (Rechtsgrundlage für die Inpol-Dateien)

Vor 13 Jahren wurde im Bundeskriminalamtgesetz festgelegt, dass Näheres über die Art der Daten, die vom Bundeskriminalamt als Zentralstelle gespeichert werden dürfen, in einer Rechtsverordnung zu bestimmen ist. Erst jetzt wurde diese Rechtsverordnung erlassen und damit die Datenverarbeitung im Inpol-Verbund auf eine rechtmäßige Grundlage gestellt.

§ 7 Abs. 6 BKAG schreibt vor, dass in einer Rechtsverordnung Näheres festzulegen ist zur Art der Daten, die in den Verbunddateien beim BKA gespeichert werden dürfen.

§ 7 Abs. 6 BKAG

Das Bundesministerium des Innern bestimmt mit Zustimmung des Bundesrates durch Rechtsverordnung das Nähere über die Art der Daten, die nach den §§ 8 und 9 gespeichert werden dürfen.

In der amtlichen Begründung für diese Regelung heißt es ausdrücklich, dass eine solche Rechtsverordnung zu den „Voraussetzungen für die Speicherung personenbezogener Daten in Zentral- und Verbunddateien“ gehört (BTDrucks. 13/1550, S. 30).

Während die Datenschutzbeauftragten wiederholt auf den Erlass einer entsprechenden Rechtsverordnung gedrängt hatten, wurde von der Polizei – gestützt vom Bundesinnenministerium – die Meinung vertreten, diese Vorschrift habe nur deklaratorischen Charakter. Die Regelungen des BKAG reichten als Grundlage für einen Eingriff in das Recht auf informationelle Selbstbestimmung aller Betroffenen und damit für eine zulässige Datenverarbeitung aus. Daran hatten auch vereinzelte Entscheidungen von Verwaltungsgerichten in Verfahren zu Löschungsanträgen nichts geändert.

In die Diskussion war allerdings Bewegung gekommen, als das Oberverwaltungsgericht Lüneburg im Dezember 2008 (11 LC 229/08) zur Datei Gewalttäter Sport urteilte, dass die Rechtsgrundlage für die Datenverarbeitung fehle und deshalb die Daten des Klägers zu löschen seien. Am 9. Juni 2010 ist schließlich die Verordnung über die Art der Daten, die nach

den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen (BKA-Daten-Verordnung – BKADV) in Kraft getreten (BGBl. I S. 716).

Damit ist eine sehr differenzierte Regelung entstanden, die auch für zukünftige neue kriminologische Entwicklungen offen sein soll.

Die Verordnung enthält zunächst eine Festlegung der Personendaten von Beschuldigten und anderer zur Identifizierung geeigneter Merkmale. Dem folgt eine Aufzählung weiterer personenbezogener Daten, die zu Beschuldigten einer Straftat gespeichert werden dürfen. Im Anschluss werden Daten bezeichnet, die jeweils für bestimmte Zwecke, z. B. zur Fahndung oder zur Durchführung erkennungsdienstlicher Maßnahmen erhoben werden dürfen. Schließlich wird noch festgelegt, für welche Kategorien von Dateien des BKA als Zentralstelle die Errichtungsanordnungen welche der konkretisierten Datenkategorien vorsehen dürfen.

Mit diesem Punkt wird eine wesentliche Anforderung der Datenschutzbeauftragten umgesetzt. Beim Erlass von Errichtungsanordnungen gem. § 34 Abs. 1 BKAG war wiederholt der Eindruck entstanden, dass routinemäßig alle Datenfelder vorgesehen waren, die theoretisch im Inpol-Verbund-System abbildbar sind.

§ 34 BKAG

(1) Das Bundeskriminalamt hat für jede bei ihm zur Erfüllung seiner Aufgaben geführte automatisierte Datei mit personenbezogenen Daten in einer Errichtungsanordnung, die der Zustimmung des Bundesministeriums des Innern bedarf, festzulegen:

1. Bezeichnung der Datei,
2. Rechtsgrundlage und Zweck der Datei,
3. Personenkreis, über den Daten gespeichert werden,
4. Art der zu speichernden personenbezogenen Daten,
5. Arten der personenbezogenen Daten, die der Erschließung der Datei dienen,
6. Anlieferung oder Eingabe der zu speichernden Daten,
7. Voraussetzungen, unter denen in der Datei gespeicherte personenbezogene Daten an welche Empfänger und in welchem Verfahren übermittelt werden,
8. Prüffristen und Speicherungsdauer,
9. Protokollierung.

Der Bundesbeauftragte für den Datenschutz ist vor Erlass einer Errichtungsanordnung anzuhören.

(2) Bei Dateien des polizeilichen Informationssystems bedarf die Errichtungsanordnung auch der Zustimmung der zuständigen Innenministerien und Senatsinnenverwaltungen der Länder.

Nicht immer hat sich der Zusammenhang zwischen dem Zweck der Datei und den vorgesehenen Datenfeldern erschlossen. So war es jahrelang Praxis auch in Falldateien, die der Ermittlungsunterstützung dienen, alle Personalien aufzunehmen, obwohl diese sowohl im Kriminalaktennachweis (KAN) als auch in den Fahndungsdateien enthalten sind, so dass es zu Doppelspeicherungen zum Teil sogar zu unterschiedlichen Speicherungen für die selbe Person kommen konnte.

In der Sache wird sich vermutlich an der Praxis der Polizei zur Speicherung von Daten in den diversen Dateien nichts Wesentliches ändern. Es bleibt zu hoffen, dass bei der zukünftigen Errichtung neuer Dateien für die Errichtungsanordnung nicht einfach der Katalog möglicher Datenfelder aus der Rechtsverordnung abgeschrieben wird, sondern eine genaue Analyse dahingehend erfolgt, welche dieser Felder gerade für den Zweck dieser konkreten Datei erforderlich sind.

3.3
Volkszählung (Zensus) 2011

Das Bundesverfassungsgericht verlangt in seinem Volkszählungsurteil von 1983 bei der Datenerhebung für statistische Zwecke eine frühzeitige Beteiligung unabhängiger Datenschutzbeauftragter und sieht in dieser Beteiligung einen wesentlichen Faktor für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung (BVerfGE 65, 1, 46). Sowohl der Hessische Landtag als auch die Landesregierung und das Hessische Statistische Landesamt haben sich an diese Vorgabe gehalten und mein Haus in die Vorbereitung des Zensus 2011 einbezogen.

3.3.1
Methodenwechsel

Im Mai 2011 findet in Deutschland wieder eine Volkszählung statt, allerdings spricht die amtliche Statistik nicht mehr von Volkszählung, weil sie befürchtet, der Begriff könne negative Assoziationen wecken. Die Volkszählung 2011 heißt offiziell deshalb Zensus.

Seit mehr als 30 Jahren gab es keine Volkszählung mehr in Deutschland. Die letzten Volkszählungen erfolgten 1987 in der alten Bundesrepublik und 1981 in der ehemaligen DDR. Dass die auf dieser Grundlage fortgeschriebenen Bevölkerungszahlen und die darauf aufbauenden Statistiken mittlerweile einen Grad an Ungenauigkeit aufweisen, der eine neue Datenbasis erforderlich macht, dürfte kaum zu bestreiten sein.

Im Unterschied zu den vorangegangenen Volkszählungen erfolgt der Zensus 2011 registergestützt. Es wird nicht mehr jeder Einwohner befragt, sondern in erster Linie werden Verwaltungsregister ausgewertet und lediglich ergänzend Befragungen durchgeführt. Wichtigste Datenquellen sind die ca. 5.200 Melderegister der mehr als 11.000 Kommunen und die Register der Bundesagentur für Arbeit, in denen 27 Millionen sozialversicherungspflichtige Beschäftigte, die Empfänger von Arbeitslosengeld und die Arbeitssuchenden erfasst sind. Bei den öffentlichen Arbeitgebern werden erwerbsstatistische Angaben zu den 1,8 Millionen Beamten, Richtern und Soldaten erhoben. Ergänzend zur Auswertung der Verwaltungsregister werden alle Gebäude- und Wohnungseigentümer, außerdem in einer Haushaltsbefragung rund 7,9 Millionen Einwohner und die Bewohner in Wohnheimen und Gemeinschaftsunterkünften wie Internaten, Studentenwohnheimen, Klöstern und Seniorenwohnheimen unmittelbar befragt. Mittels der sog. Haushaltsgenerierung werden die aus den Registern übernommenen mit den aus den Befragungen gewonnenen Daten zusammengeführt.

3.3.2
Rechtsgrundlagen

Ein ganzes Bündel von Gesetzen regelt die künftige Volkszählung. Eine EG-Verordnung, die Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen (ABl. EG Nr. L 218 S. 140 vom 13. August 2008) verpflichtet alle Mitgliedstaaten der EU zur Durchführung einer Volkszählung im Jahr 2011 und schreibt die Erhebungsmerkmale vor, welche die Mitgliedstaaten an die EU zu liefern haben. Zwei Bundesgesetze konkretisieren die europarechtlichen Vorgaben für die Bundesrepublik: Das Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011 (Zensusvorbereitungsgesetz 2011 – ZensVorbG 2011) vom 8. Dezember 2007 (BGBl. I S. 2808) regelt den Aufbau eines Anschriften- und Gebäuderegisters beim Statistischen Bundesamt. Das Register dient der Vorbereitung der Volks-, Gebäude- und Wohnungszählung. Das Gesetz über den registergestützten Zensus im

Jahre 2011 (Zensusgesetz 2011 – ZensG 2011) vom 8. Juli 2009 (BGBl. I S. 1781) legt fest, welche Merkmale erhoben werden, regelt die Auskunftspflicht und Einzelheiten zum Zusammenführen, Speichern und Löschen der Daten. Die Verordnung über Verfahren und Umfang der Haushaltsbefragung auf Stichprobenbasis zum Zensusgesetz 2011 (Stichprobenverordnung Zensusgesetz 2011 – StichprobenV) vom 25. Juni 2010 (BGBl. I S. 830) definiert das Stichprobenverfahren und den Stichprobenumfang für die Haushaltsbefragung, die im Rahmen des Zensus 2011 durchgeführt wird. Im Hessischen Ausführungsgesetz zum Zensusgesetz 2011 vom 23. Juni 2010 (GVBl. I S. 178) hat der Hessische Landtag bestimmt, welche Aufgaben das Hessische Statistische Landesamt zu erfüllen hat, wie die Erhebungsstellen zu organisieren und die Erhebungsbeauftragten zu rekrutieren und einzusetzen sind und wie mit Erhebungsunterlagen zu verfahren ist. Außerdem enthält das Ausführungsgesetz eine Verfahrensvorschrift zur Ahndung von Ordnungswidrigkeiten.

3.3.3
Merkmal „Religionszugehörigkeit“

Umstritten war die Aufnahme der Frage nach der Religionszugehörigkeit in das Fragenprogramm der Volkszählung. Die Bundesrepublik ist europarechtlich nicht gezwungen, im Rahmen der Volkszählung nach der Religionszugehörigkeit zu fragen. In dem von der EU-Kommission vorgelegten Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Volks- und Wohnungszählungen [KOM(2007) 69 endgültig BRDrucks. 147/07] zählte das Merkmal Religion nicht zum obligatorischen Erhebungsprogramm, sondern zu den empfohlenen Themen (Anhang Nr. 1.3.2). Das Europäische Parlament sprach sich in einer Legislativen Entschließung vom 20. Februar 2008 [P6_TA(2008)0056] jedoch dafür aus, die von der Kommission im Verordnungsentwurf als Empfehlung an die Mitgliedstaaten vorgeschlagenen Angaben und damit auch das Merkmal Religion zu streichen. In der EG-Verordnung über Volks- und Wohnungszählungen ist das Merkmal dementsprechend nicht enthalten.

Die Frage nach der Religionszugehörigkeit ist auf Wunsch der öffentlich-rechtlichen Religionsgesellschaften in den Fragenkatalog des Zensus aufgenommen worden. Verfassungsrechtlich ist dagegen nichts einzuwenden. Art. 140 GG in Verbindung mit Art. 136 Abs. 3 Satz 2 Weimarer Reichsverfassung erlaubt ausdrücklich diese Frage im Rahmen einer statistischen Erhebung (vgl. auch BVerfGE 65, 1, 38f.). Sowohl in der Weimarer Republik als auch bei den bislang vier in der Bundesrepublik durchgeführten Volkszählungen wurde dieses

Merkmal erhoben und hat damit eine gewisse Tradition. Beim Zensus 2011 wird die Religionszugehörigkeit zweifach erfragt. Auskunftspflicht besteht für die Frage nach der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft (z. B. römisch-katholische oder evangelische Kirche, jüdische Gemeinde). Freiwillig ist dagegen die Antwort auf die Frage zum Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung.

3.3.4
Auftragsdatenverarbeitung

Das Hessische Statistische Landesamt lässt einen Teil der Zensusarbeiten von Privatunternehmen erledigen. Druck und Versand der Erhebungsunterlagen für die Gebäude- und Wohnungszählung erfolgen durch ein Unternehmen in Einbeck, das zur Deutschen Post AG gehört. Ein Bamberger Betrieb, systemformMedicard ein Tochterunternehmen der Schweizer Post, erfasst die Erhebungsbögen aus der Gebäude- und Wohnungszählung und der Haushaltsstichprobe. Die Auslagerung von Druck und Versand der Erhebungsunterlagen und der Beleglesung ist datenschutzrechtlich zulässig. Weder das Statistikgeheimnis des § 16 BStatG noch die Regelung zur Zusammenarbeit der statistischen Ämter in § 3a BStatG hindern das Hessische Statistische Landesamt, private oder öffentliche Stellen mit Erhebungsarbeiten zu beauftragen.

§ 3a BStatG soll den Statistikämtern eine Übertragung von Funktionen auf andere Statistikämter ermöglichen, die Vorschrift zielt auf Funktionsübertragung und nicht auf Auftragsdatenverarbeitung. Die Statistikämter sollen ihre Aufgaben nach dem Prinzip „Einer oder einige für alle“ ämterübergreifend erledigen können und sich zu diesem Zweck gegenseitig Einzelangaben übermitteln dürfen (vgl. auch Beschlussempfehlung und Bericht zum Entwurf für das Gesetz zur Änderung des Statistikregistergesetzes und sonstiger Statistikgesetze vom 23. Februar 2005 – BTDrucks. 15/4955, S. 5). Bis auf die hoheitlichen Maßnahmen der Heranziehung zur Auskunftserteilung und zur Durchsetzung der Auskunftspflicht kann auf der Rechtsgrundlage § 3a BStatG ein Statistikamt einzelne Bundesstatistiken vollständig für andere Statistikämter erledigen. Dass der Gesetzgeber in diesen Fällen von einer Funktionsübertragung ausgeht, belegt zudem § 16 Abs. 2 Satz 2 BStatG. Die Norm gestattet den Statistikämtern im Rahmen der Zusammenarbeit nach § 3a BStatG die Übermittlung von Einzeldaten. Übermittlung und Auftragsdatenverarbeitung schließen nach dem allgemeinen Datenschutzrecht einander aus.

Auch das besondere Amtsgeheimnis, dem die Zensusdaten unterliegen, steht einer Auftragsdatenverarbeitung nicht entgegen. Das in § 16 BStatG geregelte Statistikgeheimnis legt die zulässigen Datenübermittlungen abschließend fest, trifft aber keine Aussage zur Auftragsdatenverarbeitung. Da die Bundesländer den Zensus 2011 wie fast sämtliche Bundesstatistiken als eigene Angelegenheiten durchführen, regeln sie das Verfahren selbst (Art. 84 GG). § 6 Abs. 1 HessLStatG gestattet dem Hessischen Statistischen Landesamt ausdrücklich, bei der Durchführung von amtlichen Statistiken einzelne Arbeiten auf Externe zu übertragen. Ein Rückgriff auf die Vorschrift zur Auftragsdatenverarbeitung im HDSG ist daher nicht erforderlich. Das Gesetz differenziert nicht zwischen öffentlich-rechtlichen und privatrechtlichen Auftragnehmern. Es verlangt jedoch, dass neben den Anforderungen des allgemeinen Datenschutzrechts die besonderen Schutzanforderungen des Statistikgeheimnisses erfüllt sein müssen. Danach kommt es lediglich darauf an, dass der Auftragnehmer den durch das besondere Amtsgeheimnis gewährten zusätzlichen Schutz des Rechts auf informationelle Selbstbestimmung der Bürger durch entsprechende personelle, technische und organisatorische Maßnahmen gewährleistet. Dabei ist ein strenger Maßstab anzulegen.

Im Übrigen war und ist Auftragsdatenverarbeitung bei der Durchführung von Bundesstatistiken in Hessen der Regelfall. Das Hessische Statistische Landesamt lässt die Datenverarbeitung weitgehend durch die Hessische Zentrale für Datenverarbeitung erledigen. Bei der letzten Volkszählung im Jahr 1987 stützte sich das Landesamt ebenfalls in großem Umfang auf Auftragsdatenverarbeitung.

3.4
Der neue Personalausweis

Seit dem 1. November 2010 ist der neue Personalausweis eingeführt. Über den Ausweis wurde oft und kontrovers diskutiert. Die Diskussion konzentrierte sich insbesondere auf die sog. eID-Funktion, d.h. die Identifizierung im Internet. Es gibt aber noch andere Problempunkte, auf die ich hinweisen möchte.

In meinem 37. Tätigkeitsbericht (Ziff. 3.1) habe ich das Konzept zum neuen elektronischen Personalausweis, oft als nPA abgekürzt, ausführlich beschrieben. Auch in diesem Jahr gab es häufig Berichte zum neuen Personalausweis. Da mit dem Ausweis insbesondere neue

Funktionen zur Internetnutzung bereitgestellt werden sollen, stand insbesondere das Thema der elektronischen Identifizierung (eID) im Brennpunkt des Interesses.

Vorab ist darauf hinzuweisen, dass nicht mehr verlangt werden darf, den Ausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben (§ 1 Abs. 1 Satz 3 PAuswG). Das ist wichtig, da es die mit dem neuen Ausweis verbundenen Möglichkeiten erfordern, ihn permanent unter Kontrolle zu behalten. Im täglichen Leben kommt es jedoch häufig vor, dass der Ausweis hinterlegt werden soll. Ein typisches Beispiel ist der Zutritt zu besonders gesicherten Gebäuden – wie etwa das Hessische Ministerium des Innern und für Sport. Hier ist es unbedingt erforderlich, dass die Abläufe geändert werden. Aber auch die Politik muss eventuell tätig werden, denn im Ausland muss man in Hotels oft den Ausweis hinterlegen. Hier stellt sich die Frage, wie man sich als Reisender verhalten soll.

§ 1 Abs 1 PAuswG

Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind verpflichtet, einen Ausweis zu besitzen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten. Sie müssen ihn auf Verlangen einer zur Feststellung der Identität berechtigten Behörde vorlegen. Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Dies gilt nicht für zur Identitätsfeststellung berechtigte Behörden sowie in den Fällen der Einziehung und Sicherstellung.

3.4.1
Technik

Die beschriebene Technik spielt vor allem eine Rolle, wenn der Bürger die eID-Funktion oder die qualifizierte elektronische Signatur nutzen möchte. Ansonsten kann man den Ausweis wie bisher als Identitätsnachweis einsetzen.

3.4.1.1
Ausweis

Der Ausweis ist eine Chipkarte mit einer kontaktlosen Schnittstelle, einem sog. RFID-Chip, auf dem die gleichen Daten wie beim heutigen Personalausweis gespeichert sind. Hinsichtlich der

RFID-Problematik möchte ich auf meine Aussagen zum Reisepass verweisen, siehe 34. Tätigkeitsbericht (Ziff. 4.2), wonach ich aktuell keine Probleme sehe.

3.4.1.2
Kartenleser

Es werden zur Zeit drei Kartenleservarianten auf dem Markt angeboten.

Der **Basisleser** verfügt über keine PIN-Tastatur. Er stellt die Verbindung zwischen PC und Ausweis her, aber die Eingabe der PIN zur Aktivierung des Ausweises erfolgt über die PC-Tastatur. Bei dieser Technik wurden erfolgreiche Angriffe mit Hilfe von Schadsoftware (Stichwort Trojaner) demonstriert.

Der **Standardleser** verfügt über eine Zifferntastatur, über die bei der Aktivierung des Ausweises die PIN eingegeben wird. Die über das Jahr vorgestellten Angriffe wären bei diesem Leser nicht erfolgreich gewesen und andere, theoretisch denkbare Angriffe wären sehr viel aufwendiger.

Der **Komfortleser** verfügt zusätzlich noch über ein Anzeigefeld und eine kontaktbehaftete Schnittstelle, wie sie bei herkömmlichen Signaturkarten oder der elektronischen Gesundheitskarte (eGK) benötigt wird.

Aus meiner Sicht bietet der Ausweis in Kombination mit einem Basisleser zwar eine höhere Sicherheit als die üblichen Identifizierungsverfahren mit Benutzerkennung und Passwort, aber es ist trotzdem angeraten, mit einem Standard- oder Komfortleser zu arbeiten. Dadurch werden erfolgreiche Angriffe, bei denen der Angreifer die Identität „stiehlt“, wesentlich erschwert (siehe Ziff. 3.4.3.2).

Passämter erhalten eine andere Technik für den Zugriff auf Ausweise, da sie Änderungen vornehmen dürfen. Sie benötigen eine sogenannte EAC-Box (EAC: extended access control; Kommunikationsprotokoll das nur berechtigte, zertifikatsbasierte Zugriffe zulässt), um auf Ausweise zugreifen und Daten ändern zu können. Die EAC-Box ist gegen unberechtigte Zugriffe besonders gesichert.

3.4.1.3
Bürgerclient oder AusweisApp

Das AusweisApp, früher Bürgerclient genannt, ist eine kostenlose Software, die das BMI in Auftrag gegeben hat. Sie soll auf dem PC des Bürgers installiert werden und die Kommunikation zwischen dem PC und dem Diensteanbieter sichern. Neben anderen Funktionen

– fordert sie zur PIN-Eingabe auf. (Aus Sicherheitsgründen sollte dies über die Tastatur des Kartenlesers erfolgen),
– zeigt sie die Daten an, die nach dem Berechtigungszertifikat übermittelt werden dürfen,
– bietet sie die Möglichkeit, bestimmte Daten von der Übermittlung auszuschließen,
– stellt sie sicher, dass die Datenübertragung verschlüsselt erfolgt und
– prüft sie, ob der Server, an den die Daten übertragen werden sollen, mit dem im Berechtigungszertifikat genannten Server übereinstimmt.

Das AusweisApp wurde zwar vom BMI in Auftrag gegeben, aber der Quellcode ist im Internet veröffentlicht. Daher hat jeder die Möglichkeit, das Programm zu prüfen. Die Software wird nur unter www.ausweisapp.bund.de zum Herunterladen bereitgestellt. Dritte dürfen sie nicht anbieten, sondern müssen auf die genannte Seite verlinken.

3.4.1.4
Berechtigungszertifikate für Diensteanbieter

Diensteanbieter, die im Internet tätig sind, benötigen ein Berechtigungszertifikat. Sie können Zertifikate beantragen, mit denen sie sich zum Nachweis der Identität bestimmte, auf dem Pass gespeicherte Daten übermitteln lassen können. Das Zertifikat kann auch auf eine Altersverifikation reduziert sein, z. B. der Ausweisinhaber ist älter als 18 Jahre oder eine Bestätigung, dass er in einem bestimmten Ort wohnt. Weiterhin kann das Zertifikat die Berechtigung so eng fassen, dass der Diensteanbieter nur ein dienste- und kartenspezifisches Kennzeichen, mit anderen Worten ein Pseudonym, erhält. Dabei sollen nur zuverlässige Anbieter ein Berechtigungszertifikat erhalten und die Daten, die sie für den im Antrag genannten Geschäftszweck erhalten dürfen, werden ebenfalls im Zertifikat abschließend genannt. In dem Zertifikat wird auch der „Fingerprint“ des Verschlüsselungszertifikats des Diensteanbieters gespeichert.

Die Kriterien, nach denen die Prüfung erfolgen soll, wurden in einem Katalog unter Beteiligung von Datenschutzbeauftragten erarbeitet. Als Vergabestelle für Berechtigungszertifikate (§ 7 Abs. 4 i.V.m. § 4 Abs. 3 PAuswG) wurde das Bundesverwaltungsamt (BVA) bestimmt. Das BVA ist auch Sperrlistenbetreiber (§ 7 Abs. 4 i.V.m. § 4 Abs. 3 PAuswG). Das BVA erteilt die Berechtigungen für längstens drei Jahre und stellt die Berechtigungszertifikate über jederzeit öffentlich erreichbare Kommunikationsverbindungen zur Verfügung. Da es kein Verzeichnis gibt, in dem ungültige Berechtigungszertifikate geführt werden, hat man sich entschieden, die Zertifikate nur für zwei Tage gültig sein zu lassen, dann müssen sie erneuert werden.

§ 4 Abs. 3 PAuswG

Das Bundesministerium des Innern bestimmt den Ausweishersteller, die Vergabestelle für Berechtigungszertifikate und den Sperrlistenbetreiber und macht deren Namen im Bundesanzeiger bekannt.

§ 7 Abs. 4 PAuswG

Für die Erteilung und Aufhebung von Berechtigungen nach § 21 ist die Vergabestelle für Berechtigungszertifikate nach § 4 Abs. 3 zuständig. Für das Führen einer Sperrliste nach § 10 Abs. 4 Satz 1 ist der Sperrlistenbetreiber nach § 4 Abs. 3 zuständig.

§ 21 Abs. 3 PAuswG

Die Berechtigung ist zu befristen. Die Gültigkeitsdauer darf einen Zeitraum von drei Jahren nicht überschreiten. Die Berechtigung darf nur von dem im Berechtigungszertifikat angegebenen Diensteanbieter und nur zu dem darin vorgesehenen Zweck verwendet werden. Die Berechtigung kann mit Nebenbestimmungen versehen und auf entsprechenden Antrag wiederholt erteilt werden.

Bei Datenschutzverstößen des Dienstanbieters kann die Zulassung zurückgenommen werden. Wenn das BVA aus diesem oder anderen Gründen die Berechtigung zurücknimmt, werden keine Berechtigungszertifikate mehr generiert und zur Verfügung gestellt. Dann erhält der Anbieter kein neues Zertifikat und nach spätestens 48 Stunden kann er die eID-Funktion nicht

mehr nutzen. Nach der Gesetzeslage darf er bereits ab dem Zeitpunkt, zu dem ihm bekannt wurde dass die Berechtigung zurückgenommen bzw. widerrufen ist, Zertifikate nicht mehr nutzen (§ 21 Abs. 6 PAuswG).

§ 21 Abs. 5 und Abs. 6 PAuswG

(5) Die Berechtigung ist zurückzunehmen, wenn der Diensteanbieter diese durch Angaben erwirkt hat, die in wesentlicher Beziehung unrichtig oder unvollständig waren. Sie ist zu widerrufen, wenn sie nicht oder nicht im gleichen Umfang hätte erteilt werden dürfen. Die Berechtigung soll zurückgenommen oder widerrufen werden, wenn die für den Diensteanbieter zuständige Datenschutzaufsichtsbehörde die Rücknahme oder den Widerruf verlangt, weil Tatsachen die Annahme rechtfertigen, dass der Diensteanbieter die auf Grund der Nutzung des Berechtigungszertifikates erhaltenen personenbezogenen Daten in unzulässiger Weise verarbeitet oder nutzt.

(6) Mit Bekanntgabe der Rücknahme oder des Widerrufs der Berechtigung darf der Diensteanbieter vorhandene Berechtigungszertifikate nicht mehr verwenden. Dies gilt nicht, solange und soweit die sofortige Vollziehung (§ 30) ausgesetzt worden ist.

3.4.1.5
PC des Bürgers

Der PC beim Bürger ist hinsichtlich der Datensicherheit der neuralgische Punkt. Damit die eID-Funktion und die elektronische Signatur korrekt genutzt werden können, darf er nicht mit Schadsoftware verseucht sein. Die damit verbundenen Pflichten des Ausweisinhabers sind in § 27 Abs. 2 und 3 PAuswG beschrieben.

§ 27 Abs. 2 und 3 PAuswG

(2) Der Personalausweisinhaber hat zumutbare Maßnahmen zu treffen, damit keine andere Person Kenntnis von der Geheimnummer erlangt. Die Geheimnummer darf insbesondere nicht auf dem Personalausweis vermerkt oder in anderer Weise zusammen mit diesem aufbewahrt werden. Ist dem Personalausweisinhaber bekannt, dass die Geheimnummer Dritten zur Kenntnis gelangt ist, soll er diese unverzüglich ändern oder die Funktion des elektronischen Identitätsnachweises ausschalten lassen.

(3) Der Personalausweisinhaber soll durch technische und organisatorische Maßnahmen gewährleisten, dass der elektronische Identitätsnachweis gemäß § 18 nur in einer Umgebung eingesetzt wird, die nach dem jeweiligen Stand der Technik als sicher anzusehen ist. Dabei soll er insbesondere solche technischen Systeme und Bestandteile einsetzen, die vom Bundesamt für Sicherheit in der Informationstechnik als für diesen Einsatzzweck sicher bewertet werden.

Er muss sich daher informieren, wie er eine nach dem Stand der Technik sichere Umgebung erreichen kann. Dazu gehört ein aktueller Virenscanner, eine Firewall und Softwareupdates der Hersteller, die Sicherheitslücken beheben. Genauere Hinweise befinden sich im Internet auf der Homepage des BSI (Bundesamt für Sicherheit in der Informationstechnik). Man muss aber feststellen, dass es keine 100%ige Sicherheit gibt. Deshalb wird es immer Unsicherheiten geben. Der Einsatz eines Basislesers bietet in diesem Zusammenhang eine höhere Sicherheit im Vergleich zu Benutzerkennung und Passwort, jedoch ist auch er angreifbar durch sogenannte Trojaner (vgl. Ziff. 3.4.1.2)

3.4.2
Beantragung und Ausgabe

3.4.2.1
Fingerabdrücke

Auf Wunsch des Bürgers können auf dem Personalausweis Fingerabdrücke gespeichert werden. Deshalb sind die Anforderungen an eine datenschutzrechtlich korrekte Abwicklung eines Antrages identisch mit den Anforderungen beim Reisepass. Dies betrifft insbesondere

– die sichere Übertragung der Antragsdaten,
– die Kontrolle, ob die richtigen Fingerabdrücke gespeichert sind und
– die rechtzeitige, vollständige Löschung der Fingerabdrücke in den Passämtern und bei allen anderen Stellen.

In diesen Punkten sind die Behörden dafür verantwortlich, dass die rechtlichen Vorgaben erfüllt werden.

Falls man Fingerabdrücke auf dem nPA gespeichert hat, kann bei einer Kontrolle geprüft werden, ob die gespeicherten und die präsentierten Fingerabdrücke übereinstimmen. Dazu muss jedoch ein geeignetes Lesegerät mit einem entsprechenden

Zugriffsberechtigungszertifikat zur Verfügung stehen. Das erhalten allerdings nur öffentliche Stellen, die hoheitliche Kontrollen durchführen dürfen. Angesichts der Tatsache, dass die Speicherung der Fingerabdrücke freiwillig ist und viele Personen Ausweisdokumente ohne diese Option haben, werden nach meiner Einschätzung auf lange Zeit Kontrollen auf die hergebrachte Art und Weise ablaufen.

Ich sehe derzeit keinen Grund, warum ein Bürger Fingerabdrücke auf dem Personalausweis speichern lassen sollte.

3.4.2.2
Der elektronische Identitätsnachweis – eID-Funktion

Der elektronische Identitätsnachweis, auch eID-Funktion genannt, ist standardmäßig aktiviert. Nur bei Personen unter 18 Jahren ist diese Funktion bei Ausgabe des Ausweises deaktiviert. Bei der Ausgabe, aber auch zu jedem anderen Zeitpunkt, kann die Personalausweisbehörde den Status ändern. Der Bürger sollte sich bei der Ausgabe entscheiden, ob er die Funktion nutzen will und dann den Status entsprechend setzen lassen. Für die Personalausweisbehörden bedeutet das eine besondere Verpflichtung, die Bürgerinnen und Bürger darüber aufzuklären, was sie mit dem elektronischen Identitätsnachweis machen können, welche Vorteile er ihnen bringen kann und welche Risiken damit verbunden sein können.

Aber auch der Bürger selbst ist gefordert sich zu informieren. In seine Überlegungen sollte einfließen, ob er das Internet nicht oder nur in geringem Maße nutzt.

In jedem Fall, auch wenn er die Funktion deaktivieren lässt, muss er seinen PIN-Brief (PIN = Geheimnummer) mit der Transport-PIN, seine PUK (Entsperrnummer) und sein Sperrkennwort sicher aufbewahren. Besonders das Sperrkennwort ist wichtig. Wenn man seinen Ausweis verliert oder er gestohlen wurde, sollte man **in jedem Fall** den Ausweis sperren lassen; hierzu wird das Sperrkennwort benötigt. Das Sperrwort wird zusätzlich im Register der Personalausweisbehörde gespeichert. Sollte der Bürger sein Sperrkennwort verlegt oder vergessen haben, so kann er es sich von der Personalausweisbehörde nennen lassen. Das geht nur während der Öffnungszeiten, da er sich dazu ausweisen muss. Wenn er seinen Ausweis verloren hat, ist dieser Weg am Wochenende oder aus der Ferne meist nicht gangbar.

Die Transport-PIN wird gebraucht, um den Ausweis zu aktivieren. Wenn der Ausweis das erste Mal auf einen Kartenleser gelegt wird, wird die 5-stellige Transport-PIN abgefragt. Wurde sie richtig eingegeben, muss man anschließend sofort eine 6-stellige PIN vergeben, die ab diesem Zeitpunkt die Nutzung des Ausweises freigibt.

3.4.3
Nutzung

Der neue Ausweis ist so gestaltet, dass er wie der bisherige Ausweis genutzt werden kann. Er hat also die Funktion des Identitätsnachweises. Mit der eID-Funktion kann dieser Nachweis jetzt auch im Internet geführt werden.

3.4.3.1
Identitätsprüfung durch Augenschein

Mit dem nPA kann man sich wie bisher gegenüber Behörden und anderen Stellen ausweisen, indem man ihn vorzeigt.

3.4.3.2
Internet, eID-Funktion

Bürgerinnen und Bürger bzw. Kundinnen und Kunden können sich entscheiden, die eID-Funktion (siehe Ziff. 3.4.2.2) zu nutzen. Sie können sich sogar fallweise entscheiden und bei einigen Anbietern weiterhin eine Benutzerkennung und ein Passwort nutzen. Diese Option dürfte es noch längere Zeit geben, da die eID-Funktion erst nach einigen Jahren einer Mehrzahl die elektronischen Verfahren nutzenden Personen zur Verfügung stehen wird.

Bei mehreren Prüfungen ist die neue Funktion aber unverzichtbar. Wenn ein Diensteanbieter eine belastbare Angabe zu Alter oder Wohnort braucht, wird dies durch die eID ermöglicht. Bei der Altersverifikation, beispielsweise wenn der Zugriff auf bestimmte Filme zum Download erst ab 18 Jahren zulässig ist, könnte er sich auf die Funktion des Personalausweises verlassen. Gleiches gilt, wenn nur die Bürger einer bestimmten Kommune Zugriff auf bestimmte Informationen erhalten sollen.

Eine weitere wichtige Neuerung ist die technisch sichere Pseudonymgenerierung; denn der nPA lässt es zu, Pseudonyme zu generieren. Die Pseudonyme sind karten- und dienstspezifisch, d.h. für unterschiedliche Ausweise werden verschiedene Pseudonyme generiert, aber derselbe Ausweis erzeugt bei unterschiedlichen Diensten wiederum unterschiedliche Pseudonyme. Ein Pseudonym ist auch nicht auf einen bestimmten Ausweis rückführbar. Verschiedene Diensteanbieter können daher die Aktivitäten unter Pseudonymen nicht gegeneinander abgleichen, um Nutzerprofile zu erstellen oder zu erhalten.

Um diese Möglichkeiten einzusetzen, benötigt der Kunde einen PC mit Internetanschluss, das AusweisApp, einen Kartenleser, sinnvollerweise mit integrierter PIN-Tastatur (s. Ziff. 3.4.1.2), und den Ausweis mit aktivierter eID-Funktion. Wenn der Kunde ein Angebot sieht, das die Funktion nutzt, wird das AusweisApp aktiviert. Er wird dann aufgefordert, den Ausweis auf den Kartenleser zu legen, das Zertifikat und die zur Übermittlung gewünschten Daten werden angezeigt. Er kann jetzt einzelne auf dem Ausweis gespeicherte Daten von der Übertragung ausschließen. Danach muss er die PIN eingeben und die Übertragung findet statt. Bei erfolgreichem Identitätsnachweis sollte der Ausweis sofort vom Kartenleser genommen werden, damit der Ausweis unter keinen Umständen mehr ungewollt oder ferngesteuert aktiviert werden kann.

Das Sperrkennwort und die Telefonnummer, unter der man den Ausweis sperren kann, sollten sorgfältig aufbewahrt werden. Wenn ein Ausweis verloren geht oder sogar gestohlen wird, muss der Ausweis umgehend gesperrt werden. Dazu ruft man die angegebene Nummer oder die Personalausweisstelle an und lässt unter Angabe der Personalien und Nennung des Sperrkennwortes den Ausweis sperren. Dies sollte man auch tun, wenn die eID-Funktion nicht aktiviert ist, da es unter Umständen einem Dieb gelingen könnte, die eID-Funktion zu aktivieren und dann mit dem gestohlenen Ausweis zu handeln.

3.4.3.3
Qualifizierte elektronische Signatur

Zusätzlich zu den beschriebenen Funktionen kann auf dem Ausweis auch eine qualifizierte elektronische Signatur aufgebracht werden. Die Signaturfunktion erlaubt es, elektronisch Verträge zu schließen, die der Schriftform bedürfen. Sie ist anders als die eID-Funktion nicht automatisch aktiviert, sondern sie muss vom Bürger bei einem privaten Anbieter beantragt werden. Dieser stellt zusätzlich Kosten in Rechnung.

Mit dieser Option soll die Infrastruktur der qualifizierten elektronischen Signatur in der Bundesrepublik Deutschland gefördert werden; denn anders als im Nachbarland Österreich, wo es eine Signatur bereits auf Bankkarten, der Gesundheitskarte oder Mobiltelefonen gibt, ist sie in Deutschland nach wie vor nicht verbreitet. Allerdings sollte jeder bei der Beantragung des neuen Personalausweises für sich prüfen, ob er diese Funktionalität tatsächlich braucht.

3.5
Elektronischer Aufenthaltstitel

Das Bundesministerium des Innern hat einen Referentenentwurf vorgelegt, mit dem das Aufenthaltsgesetz, das Gesetz über die allgemeine Freizügigkeit von Unionsbürgern sowie das Asylverfahrensgesetz geändert werden. Über das HMDIS erhielt ich Gelegenheit, aus datenschutzrechtlicher Sicht zu dem Entwurf Stellung zu nehmen.

Mit der Verordnung zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatsangehörige [EG Nr. 380/2008 vom 18. April 2008 zur Änderung der Verordnung (EG) Nr. 1030/2002] verfolgt die EU das Ziel, einen EU-weit einheitlichen Aufenthaltstitel für alle Drittstaatsangehörigen einzuführen. Dieser soll fälschungssicher sein und der Verhinderung und Bekämpfung der illegalen Einwanderung und des illegalen Aufenthalts dienen.

Um eine verlässlichere Verbindung zwischen dem Inhaber des Aufenthaltstitels und dem Aufenthaltstitel herstellen zu können, sind in den elektronischen Aufenthaltstitel zwingend biometrische Merkmale, nämlich ein Lichtbild sowie zwei Fingerabdrücke aufzunehmen. In der Entwurfsfassung zu den Änderungen des Aufenthaltsgesetzes wurden darüber hinaus auch noch Irisbilder erwähnt. Ich habe in meiner Stellungnahme in Zweifel gezogen, ob die Verordnung der Europäischen Gemeinschaft die Aufnahme weiterer biometrischer Daten auf den elektronischen Aufenthaltstitel überhaupt zulässt. Darüber hinaus hielt ich die Nennung der Irisbilder schon deshalb für nicht erforderlich, weil diese in dem Referentenentwurf als biometrische Daten definiert, im Weiteren allerdings nicht erwähnt wurden. Selbst nach dem Entwurf fanden die Irisbilder danach keinerlei Verwendung.

In einer zweiten Fassung des Referentenentwurfes wurden die Irisbilder als biometrische Daten gestrichen.

Weiter wurde in dem ursprünglichen Entwurf unter den sichtbar auf den elektronischen Aufenthaltstitel aufzubringenden Feldern das Feld „Anmerkungen“ genannt, ohne dass aus dem Gesetzestext selbst oder aus der Begründung hierzu näher vorherging, welche Art von Anmerkungen damit gemeint waren. In meiner Stellungnahme forderte ich deshalb, dass der Begriff „Anmerkungen“ inhaltlich konkreter erläutert werden müsste, um dem Gebot der Normenklarheit gerecht zu werden. Diese Anregung wurde aufgegriffen und in der Begründung klargestellt, dass unter dem Feld „Anmerkungen“ nur aufenthaltsrechtlich relevante Eintragungen vorgenommen werden dürfen. Hierunter fallen z. B. die Rechtsgrundlage für den Aufenthalt, ein Hinweis auf die Gestattung der Erwerbstätigkeit oder sonstige Nebenbestimmungen, die ggf. auf einem Zusatzblatt zum elektronischen Aufenthaltstitel aufgeführt sind.

Der elektronische Aufenthaltstitel soll genau wie der neue Personalausweis mit den Zusatzfunktionen „eID“ (elektronischer Identitätsnachweis; s. a. Ziff. 3.4.2.2) sowie einer Möglichkeit zur Erstellung einer qualifizierten elektronischen Signatur (elektronische Unterschrift; s. a. Ziff. 3.4.3.3) ausgestattet werden. Der Referentenentwurf verweist für die näheren Bestimmungen hierzu auf eine noch zu erstellende Aufenthaltsverordnung. In der Diskussion sind allerdings bereits jetzt praktische Fragen wie z. B. die Frage der Freischaltung der eID-Funktion aufgetreten. Vor allem von den Ausländerbehörden wurde diskutiert, ob die eID-Funktion bei der Auslieferung standardmäßig freigeschaltet sein soll oder dies nur eine Option ist, die auf Antrag freigeschaltet wird. Ich habe hierzu parallel zu der gleichen Fragestellung bei dem neuen Personalausweis die Ansicht vertreten, dass die eID-Funktion generell inaktiv sein und nur auf Wunsch eine Freischaltung erfolgen sollte.

Im Rahmen dieser Diskussion habe ich ebenfalls darauf hingewiesen, dass meiner Ansicht nach das Sperrkennwort, mit dem die eID-Funktion der Karte bei Verlust gesperrt werden kann standardmäßig und nicht nur auf besonderen Wunsch des Betroffenen ausgegeben werden sollte.

Insgesamt erscheint zudem fraglich, ob sämtliche Regelungen die Zusatzfunktionen eID und Signaturerstellungseinheit betreffend überhaupt in einer Verordnung regelbar sind und nicht vielmehr Gegenstand des Gesetzes sein müssten.

Schließlich habe ich eine Regelung zur Löschung der Fingerabdruckdaten, die zur Erstellung des elektronischen Aufenthaltstitels erhoben und gespeichert werden müssen, eingefordert.

In dem nunmehr vorliegenden Gesetzentwurf der Bundesregierung (BTDrucks. 17/3354 vom 21. Okt. 2010) wurden meine Anregungen nicht berücksichtigt.

4. Land

4.1 Querschnitt

4.1.1
Die behördlichen Datenschutzbeauftragten als Ansprechpartner für Bürgerinnen und Bürger sowie den Hessischen Datenschutzbeauftragten

Es genügt nicht, dass ein behördlicher Datenschutzbeauftragter bestellt ist; die Person muss auch als Amtsinhaber intern und extern bekannt sein. Dies schließt eine Bekanntgabe an Beschäftigte und insbesondere die Telefonzentrale ebenso ein wie die Aufführung im Organisationsplan und die Bekanntgabe auf der Homepage.

§ 5 Abs. 1 HDSG schreibt für jede öffentliche Stelle vor, dass sie einen Datenschutzbeauftragten sowie einen stellvertretenden Datenschutzbeauftragten bestellt.

§ 5 Abs. 1 HDSG

Die datenverarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Bestellt werden dürfen nur Beschäftigte, die dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt werden. Für die Wahrnehmung seiner Aufgaben nach Abs. 2 muss der behördliche Datenschutzbeauftragte die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Wegen dieser Tätigkeit, bei der er frei von Weisungen ist, darf er nicht benachteiligt werden. Er ist insoweit unmittelbar der Leitung der datenverarbeitenden Stelle zu unterstellen; in Gemeinden und Gemeindeverbänden kann er auch einem hauptamtlichen Beigeordneten unterstellt werden. Der behördliche Datenschutzbeauftragte ist im erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen sowie mit den zur Erfüllung seiner Aufgaben notwendigen räumlichen, personellen und sachlichen Mitteln auszustatten. Die Beschäftigten der datenverarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden.

Nach dem Gesetz ist der oder die Datenschutzbeauftragte unmittelbar der Leitung der datenverarbeitenden Stelle zu unterstellen; in Kommunen genügt die Unterstellung unter einen hauptamtlichen Beigeordneten. Das Amt ist somit als Stabsfunktion ausgestaltet. Aufgabe des

oder der Datenschutzbeauftragten ist die Unterstützung der Daten verarbeitenden Stelle bei der Umsetzung der datenschutzrechtlichen Regelungen.

Die mit der Funktion des behördlichen Datenschutzbeauftragten beauftragte Person stellt gleichzeitig ein wichtiges Bindeglied zwischen den Bürgerinnen und Bürgern und der Verwaltung dar. Vor allem im kommunalen Bereich ist sie hinsichtlich datenschutzrechtlicher Einzelfragen zunächst der erste Anlaufpunkt für Fragen der Bürgerinnen und Bürger ebenso wie für Fragen der Beschäftigten. Aber auch die Verbindung zwischen der Verwaltung und dem Hessischen Datenschutzbeauftragten läuft in vielen Fällen über diese Person. Sei es, dass sie Fragestellungen an den Hessischen Datenschutzbeauftragten weiterleitet oder auch dass dieser sie bittet, vor Ort einen Sachverhalt zu ermitteln.

Um diese wichtige Aufgabe angemessen erfüllen zu können, muss der oder die behördliche Datenschutzbeauftragte aber auch für Außenstehende auffindbar und ansprechbar sein. In vielen Organigrammen oder vergleichbaren Darstellungen zur Struktur der Behörde – wie sie auf den Homepages der meisten Behörden inzwischen selbstverständlich sind – findet man zwar die Frauenbeauftragte, die Personal- oder die Schwerbehindertenvertretung; der Datenschutzbeauftragte jedoch ist dort nicht aufgeführt. So enthält z.B. auch der mit Erlass des Hessischen Innenministeriums vom 18. April 2010 über die Organisation und Zuständigkeit der hessischen Polizeipräsidien vorgeschriebene Rahmenorganisationsplan zwar die Interessenvertretungen, nicht aber den behördlichen Datenschutzbeauftragten (s. StAnz. 2010 S. 1402 ff., Anlage 2).

Häufig habe ich zudem die Erfahrung machen müssen, dass selbst in der Telefonzentrale einer Behörde nicht bekannt ist, wer diese Funktion ausfüllt. Dies bestätigen mir auch entsprechende Anfragen von Bürgerinnen und Bürgern.

Die Funktion eines internen Datenschutzbeauftragten ist ein wichtiger Teil des Transparenzgrundsatzes nach der EG-Datenschutzrichtlinie: Seine Existenz befreit die Dienststelle von der Meldepflicht der einzelnen Datenverarbeitungen, denn er bzw. sie führt die Verfahrensverzeichnisse und hat sie zur Einsicht für jedermann vorzuhalten (§ 5 Abs. 2 Nr. 4 HDSG).

§ 5 Abs. 2 Nr. 4 HDSG

(2) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die datenverarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu

unterstützen und Hinweise zur Umsetzung zu geben. Zu seinen Aufgaben gehört es insbesondere

.....

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

.....

Von Transparenz kann nicht die Rede sein, wenn nicht bekannt ist, wer dieses Amt ausübt.

Es ist deshalb sicherzustellen, dass allen Bediensteten, insbesondere aber der Telefonzentrale bekannt ist, wer die Funktion des bzw. der internen Datenschutzbeauftragten ausübt.

Im Interesse einer bürgerfreundlichen Gestaltung auch der Außendarstellung einer Behörde etwa durch eine Homepage kann ich nur dringend empfehlen, dass der oder die behördliche Datenschutzbeauftragte seinen bzw. ihren gesetzlich zugewiesenen Platz auch im dort eingestellten Organisationsplan erhält.

4.1.2
Einsichts- und Auskunftsrecht des Bürgers gegenüber der Verwaltung

Die Daten verarbeitenden Stellen sind verpflichtet, einer Person Einsicht in Akten oder Auskunft aus Akten zu gewähren, die zu ihr geführt werden. Verschiedentlich musste ich Personen, die dieses Recht in Anspruch nehmen wollten, bei der Durchsetzung behilflich sein.

In einem Fall wurde einer Bürgerin die Einsicht in eine beim Gesundheitsamt geführte Akte verweigert. Das Gesundheitsamt hatte ein Akteneinsichtsrecht bzw. einen Auskunftsanspruch der Bürgerin nur in Bezug auf die Schreiben des Amtes an die Bürgerin selbst für rechtlich geboten gesehen. Alle übrigen Schreiben, Vermerke etc. seien geistiges Eigentum der Verfasser und deshalb dem Einsichts- bzw. Auskunftsrecht der Bürgerin entzogen.

Diesen Ausführungen habe ich nachdrücklich widersprochen.

Gesetzliche Grundlage für die Tätigkeit der Gesundheitsämter ist das HGöGD vom 28. September 2007 (GVBl. I S. 659). Gem. § 18 Abs. 4 HGöGD sind die Bestimmungen des

HDSG ergänzend anzuwenden. Nach § 18 Abs. 5 HDSG kann der Betroffene bei der speichernden Stelle Einsicht in die Akten verlangen, die zu seiner Person dort geführt werden. Dieses Akteneinsichtsrecht ist grundsätzlich umfassend und unterliegt allenfalls dann Einschränkungen, wenn personenbezogene Daten Dritter oder geheimhaltungsbedürftige, nicht personenbezogene Daten in der Akte enthalten sind. Personen, die – wie hier – in amtlicher Funktion tätig werden, sind nicht Dritte im Sinne dieser Vorschrift. Andere Gründe für eine Einschränkung des Akteneinsichtsrechts waren im vorliegenden Fall nicht ersichtlich, sodass ich gegenüber der Behörde vorgetragen habe, dass der Bürgerin ein umfassendes, uneingeschränktes Recht auf Einsicht in alle Unterlagen zu gewähren ist. Dabei habe ich hervorgehoben, dass dies auch Aktenvermerke und Notizen betrifft. Das Anlegen von „Nebenakten“ und deren Geheimhaltung gegenüber dem Betroffenen widerspricht dem mit § 18 HDSG angestrebten Ziel der Transparenz der Datenverarbeitung für die Betroffenen. Die Behörde hat daraufhin eine umfassende Akteneinsicht gewährt.

In einem anderen Fall begehrte ein Bürger Einsicht in eine Akte, die bei einer Kommune im Zusammenhang mit einer baurechtlichen Nachbarschaftsstreitigkeit geführt wurde. In dieser Akte waren neben den Informationen und Schreiben des Bürgers selbst und Schreiben an ihn auch eine Vielzahl von Briefen anderer Personen, die sich in dieser Angelegenheit geäußert hatten. Hier bat mich der Bürgermeister um Stellungnahme, ob eine derartige Akteneinsicht gewährt werden könne. Ich habe dem Bürgermeister mitgeteilt, dass zwar gem. § 18 Abs. 5 Akteneinsicht zu gewähren ist, wenn Daten in Akten gespeichert sind, die zur Person des Betroffenen geführt werden. Die Akteneinsicht sei aber dann unzulässig, wenn die Daten des Betroffenen mit Daten Dritter derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großen Aufwand möglich ist. In diesem Fall ist dem Betroffenen 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. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 3 zu erteilen. Im Übrigen kann ihm statt Einsicht Auskunft gewährt werden.

Dieser Fall war hier gegeben. Ich habe dem Bürgermeister deshalb mitgeteilt, dass er entweder die Akte so bereinigen muss, dass Daten Dritter nicht offenbart werden oder er Auskunft über den wesentlichen Inhalt der Akte erteilen soll. Allerdings habe ich verdeutlicht, dass Dritte i. S. d. zitierten Vorschrift nicht Funktionsträger der Verwaltung sind. Deshalb dürfen Notizen der Verwaltung, die dokumentieren, welche Amtsperson was gemacht hat, nicht zurückgehalten werden.

Eine weitere Anfrage betraf die Aufzeichnung der Telefonanrufe in den zentralen Leitstellen der Rettungsdienste. Augrund des § 9 HRDG sind in den zentralen Leitstellen alle ankommenden und abgehenden Funk- und Drahtgespräche auf Tonträger mit Uhrzeit aufzuzeichnen und mindestens sechs Wochen aufzubewahren. Dabei kommt es zwangsläufig zur automatisierten Speicherung von personenbezogenen Daten im Sinne des HDSG. Es wurde seitens der Leitstelle die Frage gestellt, ob für diese Aufzeichnungen der Auskunftsanspruch des § 18 Abs. 3 HDSG gelte.

§ 18 Abs. 3 HDSG

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

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger übermittelter Daten, soweit dies gespeichert ist.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

Ich habe dies ausdrücklich bejaht; denn § 24 Abs. 1 HRDG verweist auf die Bestimmungen des HDSG. Damit besteht ein Anspruch des von der Speicherung Betroffenen hinsichtlich der Tonaufzeichnungen. So muss der Person wegen der ein Notruf abgesetzt worden ist, Auskunft darüber gewährt werden, was die den Notruf absetzende Person der Leitstelle gemeldet hat.

Zu Spezialfällen der Akteneinsichts- und Auskunftsansprüche siehe auch in diesem Tätigkeitsbericht die Beiträge Ziff. 4.4.2 Akteneinsicht im Aufenthaltsgenehmigungsverfahren, Ziff. 4.7.5 Auskunftsanspruch gegenüber einer Unfallversicherung, Ziff. 6.6.1 Auskunftsanspruch des Kunden bei Aufzeichnung von Telefongesprächen durch

Kreditinstitute und Ziff. 6.1.2 Auskunftsanspruch des Erben gegenüber Kreditinstituten bei angeordneter Testamentsvollstreckung.

4.1.3
Datenschutzrechtliche Anforderungen an Sicherheitspartnerschaften

Die Zusammenarbeit von kommunalen Ordnungsbehörden, Landes- und Bundespolizei bei der Videoüberwachung im Umfeld von Bahnhöfen bedarf klarer Zuständigkeitsregelungen i. S. d. Hessischen Gesetzes für öffentliche Sicherheit und Ordnung und des Bundespolizeigesetzes. Insbesondere muss berücksichtigt werden, dass im Bereich der Eisenbahnen weder die Kommunen noch die Landespolizei eigene Überwachungsbefugnisse besitzen.

Bahnhöfe sind häufig Kriminalitätsschwerpunkte in den Kommunen. Insbesondere die weniger frequentierten, kleineren Bahnhöfe sind infolge ihrer häufig abgelegenen Lage Zielobjekt für kriminelles Milieu und Zerstörungen. Die Bundespolizei, die für diesen Bereich die zuständige Gefahrenabwehrbehörde ist, wäre überfordert, wenn sie ihre Aufgaben bei jedem noch so kleinen Bahnhof wahrnehmen müsste. Da in dieser Situation die lokale Politik regelmäßig ein Einschreiten polizeilicher Kräfte fordert, die Landespolizei und die Kommunen selbst aber nur eingeschränkte Rechte haben, liegt es nahe, dass die verschiedenen Kräfte zusammenarbeiten.

Im Berichtszeitraum sind mir verschiedene Planungen zur Videoüberwachung von Bahnhöfen vorgetragen worden, die allesamt die unterschiedlichen Befugnisse der Ordnungsbehörden nicht sauber voneinander getrennt haben. Insbesondere wurde häufig übersehen, dass im Bereich der Bahnhöfe und Gleisanlagen – anders als auf Bahnhofsvorplätzen – die Landespolizei und die kommunalen Ordnungsbehörden keine eigenen Überwachungsbefugnisse besitzen, sondern dass hier die Bundespolizei zuständig ist. Auch wurde häufig angenommen, dass es ausreichend sei, dass die Deutsche Bahn AG (DB AG) Rechte an die Kommunen oder die Polizei übertrage und damit eine Videoüberwachung durch diese Stellen vorgenommen werden könne.

Im gewidmeten Bereich der öffentlichen Bahnanlagen ist nur die Bundespolizei befugt, gem. § 27 BPolG i. V. m. § 23 Abs. 1 Nr. 4 BPolG, Bildaufnahmen und -aufzeichnungen

vorzunehmen. Für den Anwendungsbereich des § 14 Abs. 3 und 4 HSOG bleibt hier kein Raum.

Die Befugnisse der Bundespolizei können nicht von der DB AG an die Kommunen übertragen werden. Die DB AG selbst ist lediglich Inhaber des privaten Hausrechts der Bahnhöfe. Sie hat aber im Rahmen dieses privaten Hausrechts keine Befugnisse, die Überwachung des öffentlich gewidmeten Bereichs auf Dritte zu übertragen. Über Befugnisse der Bundespolizei kann sie nicht verfügen.

Ich habe deshalb in allen Fällen empfohlen, schon zu Beginn von Überlegungen im Bereich von Bahnhöfen Videoüberwachungen durchzuführen, immer die Bundespolizei als Beteiligte mit an den Planungstisch zu holen.

So hat jetzt in diversen Fällen die Bundespolizei ihre Befugnisse per öffentlich-rechtlichen Vertrag auf die Kommunen übertragen. Diese haben nunmehr das Recht, auch in Bahnhöfen, in Unterführungen und auf den Bahnsteigen Videoüberwachungsanlagen zu installieren. Eine solche Vereinbarung könnte auch zwischen Bundespolizei und Landespolizei getroffen werden.

Etwas anderes gilt für die Bahnhofsvorplätze mit Parkplätzen etc., die nicht mehr zum Bahngelände gehören. Dort kann bei Vorliegen der rechtlichen Voraussetzungen entweder die Landespolizei nach § 14 Abs. 3 HSOG oder die zuständige Ordnungsbehörde nach § 14 Abs. 4 HSOG eine Videoüberwachung vornehmen.

Sollen die verschiedenen Gefahrenabwehrbehörden die Datenbestände aus den Überwachungsmaßnahmen gemeinsam nutzen dürfen, so bedarf es neben der Prüfung, ob die rechtlichen Voraussetzungen für alle Beteiligten erfüllt sind auch einer Verfahrensbeschreibung gem. § 15 HDSG (gemeinsames Verfahren), aus der sich die Rechte und Pflichten der einzelnen Verfahrensbeteiligten klar ergeben. Bevor ein derartiges Verfahren eingeführt wird, ist immer meine Dienststelle im Vorhinein zu beteiligen. Insofern gilt für diese Überwachungsmaßnahmen etwas anderes als für Überwachungsmaßnahmen nur durch eine Stelle.

4.1.4
eArchiv

Mit dem Projekt eArchiv ist die Einführung des flächendeckenden Dokumentenmanagementsystems in der hessischen Landesverwaltung abgeschlossen. Ich habe das Projekt über Jahre datenschutzrechtlich begleitet.

Die eGovernment-Strategie des Landes Hessen benennt die Einführung eines Dokumentenmanagementsystems (HeDok) als eines ihrer wichtigen Ziele. Das Ziel wurde in drei abgeschlossenen Teil-Projekten umgesetzt: In den Jahren 2003 bis 2005 erfolgte die Umstellung der Poststellen und Registraturen (Phase 1), mit der ich mich ausführlich im 34. Tätigkeitsbericht (Ziff. 8.2) befasst habe. Als weiterer Baustein wurde im Jahr 2006 die Sachbearbeitung im Dokumentenmanagementsystem (Phase 2) eingeführt. Darüber habe ich im 35. Tätigkeitsbericht Ziff. 8.3 berichtet. Das Projekt eArchiv (Phase 3) stellt nun den Abschluss dieses Gesamt-Projektes dar.

4.1.4.1
Zielsetzung des Projektes eArchiv

Im Juni 2009 startete das eGovernment-Projekt eArchiv. Ziel des Projektes war eine landesweit einheitliche Lösung für die rechtssichere Aufbewahrung von elektronischen Verwaltungsinformationen in der Phase nach Abschluss der Bearbeitung bis zur Übergabe der digitalen Informationen zur historischen Archivierung an das Hessische Hauptstaatsarchiv bei archivwürdigem Material bzw. anderenfalls bis einschließlich der Löschung. In Kooperation zwischen der Abteilung VII des HMDIS und der HZD wurde eine standardisierte Lösung entwickelt. Das Projekt eArchiv befasst sich also nicht mit der eigentlichen Archivierung im Hessischen Hauptstaatsarchiv, sondern es geht um die Aufbewahrung elektronischer Informationen nach Abschluss der Bearbeitung innerhalb der festgelegten Aufbewahrungsfristen. Die Aufbewahrungsfristen können ganz unterschiedlich sein: Die Regelaufbewahrungsfrist beträgt fünf Jahre; je nach Bedeutung des Vorgangs differieren die Fristen von einem Jahr bis zur dauerhaften Aufbewahrung. Das macht deutlich, dass es auch um die langfristige elektronische Aufbewahrung von digitalen Informationen der Verwaltung ging. Hierdurch und durch den schnellen Zuwachs an digitalen Informationen, u. a. mit der Einführung der eAkte, entstanden neue Anforderungen an die Einrichtung von Langzeit-Aufbewahrungssystemen.

4.1.4.2

Arbeitsabläufe

Ist die Bearbeitungsphase für ein Dokument beendet, veranlasst der oder die Verantwortliche den Abschluss des Vorgangs oder der Akte in HeDok. Dies hat zur Folge, dass die Aufbewahrungsfrist zu laufen beginnt. Die Länge der Aufbewahrungsfrist richtet sich nach dem Erlass zur Aktenführung in den Dienststellen des Landes Hessen (Aktenführungserlass – AfE) vom 16. Mai 2007, StAnz. 2007 S. 1123 ff. Sie wird bereits bei der Anlage der Akte oder bei der Anlage des Vorgangs festgelegt.

Mit dem Abschluss der Akte oder des Vorgangs werden im System folgende Prozesse angestoßen:

- Sperren der Dokumente für die weitere Bearbeitung,
- Umwandlung der Dokumente in das Format PDF/A zur Erhaltung der langfristigen Lesbarkeit,
- Erstellen einer txt-Datei zur Erleichterung der späteren Volltext-Recherche nach Dokumenteninhalten,
- Verschieben der Dokumente im Originalformat und in den gewandelten Formaten in die Ablage des Archivspeichers und
- Fristbeginn der Aufbewahrungsfrist.

Das Verfügungsrecht über die im eArchiv abgelegten digitalen Dokumente bleibt weiterhin bei der aktenführenden Stelle. Sie behält, verwaltet und steuert weiterhin die Zugriffsrechte auf die archivierten Objekte.

Bei Suchanfragen werden in den Trefferlisten auch Akten, Vorgänge und Dokumente, die sich in der Aufbewahrungsphase befinden, angezeigt. Akten und Vorgänge, die zunächst abgeschlossen sind, können wieder in die Bearbeitung übernommen werden. Werden sie erneut abgeschlossen, beginnt die Aufbewahrungsfrist neu zu laufen.

4.1.4.3

Datenschutzrechtliche Bewertung

Die wesentlichen Datenschutzfragen stellten sich bereits bei der Einführung von HeDok, insbesondere hinsichtlich der Fragen, welche Dokumente nicht in HeDok überführt werden sollen (vgl. 34. Tätigkeitsbericht, Ziff. 8.2.4.1) und wie die Muster der Vorabkontrolle (vgl.

35. Tätigkeitsbericht Ziff. 8.3.1) oder das Rollen- und Berechtigungskonzept (vgl. 34. Tätigkeitsbericht, Ziff. 8.2.4.1) ausgestaltet ist.

Für die Behandlung der elektronischen Dokumente in der Aufbewahrungsphase stellen sich keine neuen datenschutzrechtlichen Fragen. Solange sich die Dokumente in der Aufbewahrungsphase befinden, gilt das gleiche Rollen- und Berechtigungskonzept wie während der Bearbeitungsphase. Bei der Archivierung handelt es sich lediglich um eine Funktionserweiterung von HeDok, weshalb die erstellten Muster lediglich ergänzt wurden. Gemeinsam mit den Projektverantwortlichen habe ich die „Ergänzung der Mustervorabkontrolle für DMS-Archivierung„ und das „Muster-Verfahrensverzeichnis DMS-Archivierung“ erarbeitet. Die genannten Dokumente stehen allen Ressorts in der Landesverwaltung zur Verfügung.

4.1.5
Löschung von Daten im SAP R/3 HR-System

Die Löschung von Daten im SAP R/3 HR-System ist bisher immer noch nicht erfolgt.

Sowohl in meinem 36. Tätigkeitsbericht (Ziff. 5.10.3.2) wie auch in meinem 38. Tätigkeitsbericht (Ziff. 4.8.3) habe ich über die nicht erfolgte Löschung von Daten im SAP R/3 HR-System berichtet.

Im Mai dieses Jahres hat die SAP AG den von ihr entwickelten Löschreport zur Vernichtung krankheits- und urlaubsbedingter Abwesenheitszeiten überarbeitet und zum weiteren Test freigegeben.

Die Landesregierung hat im August 2010 eine ressortübergreifende Arbeitsgruppe gebildet, die einen Test der inhaltlichen Funktionsfähigkeit dieses Reports durchführte und in der alle Ressorts außer dem HMWK, die HBS und der RP Kassel (Versorgung) mitarbeiten.

Seit Anfang Oktober testen die Mitarbeiterinnen und Mitarbeiter „vor Ort“ die gemeinsam besprochenen und von einer Unterarbeitsgruppe erarbeiteten Testfälle. Die Testanwender erstellen auf der Basis der ihnen zur Verfügung gestellten generischen Testskripte einen Testfallkatalog und melden die Ergebnisse an die Teilprojekte. Dabei waren komplexe Zusammenhänge wie z. B. Verbindungen zu den Entgeltzahlungsfunktionen (ist wegen

längerer Krankheit die Lohnfortzahlung entfallen und werden nun diese Krankheitszeiten gelöscht wird automatisch die Rückrechnungsfunktion ausgelöst) oder wegen klärungsbedürftiger Konkurrenz zu Aufbewahrungsfristen nach dem SGB oder dem HGB zu berücksichtigen.

Es ist geplant, die Tests bis zum Ende des Jahres abzuschließen und den Löschreport im ersten Quartal 2011 produktiv zu setzen.

Aus arbeitsökonomischen Gründen hat die Landesregierung bisher den Fokus nur auf die Löschung urlaubs- und krankheitsbedingter Abwesenheitsdaten verengt, da diese nach § 107f Abs. 2 HBG spätestens nach drei Jahren zu löschen sind.

§ 107f HBG

(1) Personalakten sind nach ihrem Abschluss von der personalaktenführenden Behörde fünf Jahre aufzubewahren. Personalakten sind abgeschlossen,

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

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

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

(4) Die Personalakten werden nach Ablauf der Aufbewahrungsfrist vernichtet, sofern sie nicht vom zuständigen Staatsarchiv übernommen werden.

Die weiteren zu löschenden Daten sollen in einem nächsten Arbeitsschritt, im Anschluss an das derzeitige Projekt, untersucht und gelöscht werden. Da auch diese Fristen abgelaufen sind bzw. in Kürze ablaufen, muss diese Aufgabe kurzfristig erledigt werden.

Ich war, wie in den vergangenen Jahren, in alle Arbeiten zum Thema „Löschung von Daten“ eingebunden und habe an den zu dieser Aufgabe stattgefundenen Sitzungen beratend teilgenommen.

4.1.6
Download-Berechtigungen

Die datenschutzrechtlich problematische Praxis bei der Vergabe von Download-Berechtigungen hat sich nicht geändert.

Schon in den beiden vergangenen Jahren (36. Tätigkeitsbericht, Ziff. 5.10.3.1; 37. Tätigkeitsbericht, Ziff. 4.8.4) habe ich über die Vergabe von Download-Berechtigungen im SAP-System berichtet.

Die Anzahl dieser Berechtigungen ist trotz meiner kritischen Hinweise nicht reduziert worden. Zwar wurde mir berichtet, dass es in den Ressorts Prüfungen auf die Notwendigkeit der Vergabe der Download-Berechtigungen gab, die allerdings nur in sehr wenigen Einzelfällen zum Entzug dieser Berechtigungen führte. Im Bereich des Hessischen Ministeriums der Finanzen wurde vielmehr für die Mitarbeiterinnen und Mitarbeiter der OFD, für die eine Berechtigung zum Download im Rechnungswesensystem vergeben war und die, weil sie auch eine Zugangsberechtigung für das HR-System über den Windows Terminal Server (WTS) hatten, damit automatisch auch die Daten des HR-System downloaden konnten, zusätzlich 72 entsprechende Berechtigungen im System eingetragen. Begründet wurden diese Berechtigungen in einem „Sammelauftrag“ damit, dass für die Erfüllung der Aufgaben im Querschnittsbereich der Oberfinanzdirektion bzw. in den Geschäftsstellen der Finanzämter die im Antrag aufgeführten Benutzer eine Download-Berechtigung benötigen. Nur durch eine Überführung der aus den SAP-Berichten gewonnenen Ergebnisse nach EXCEL sei es möglich, mit komplexen Filter- und Sortierfunktionen die Plausibilität und Richtigkeit der in HR

hinterlegten Daten zu prüfen und strategische Entscheidungen personeller und organisatorischer Art vorzubereiten.

Zur Vorbereitung dieser strategischen Entscheidungen und zur Prüfung der Datenqualität würden die erforderlichen Daten über vorhandene SAP-Berichte ermittelt. Dabei sei es oftmals erforderlich, die Ergebnisse verschiedener Berichte zu kombinieren und/oder miteinander zu vergleichen. Dies sei mit den vom Landesreferenzmodell HR angebotenen Funktionen nicht oder nur eingeschränkt möglich.

Diese Begründungen überzeugen mich nicht. Zum einen halte ich es nicht für glaubhaft, erforderlich und praktikabel, dass alle Mitarbeiterinnen und Mitarbeiter der OFD mit Zugangsrechten für das SAP-HR-System strategische Entscheidungen für den Personaleinsatz der nachgeordneten Dienststellen erstellen bzw. die Datenqualität überprüfen und hierzu eine Download-Berechtigung benötigen. Dies wird üblicherweise „Spezialisten“ überlassen. Zum anderen sollte das SAP-System in der Lage sein, die für die beschriebenen Aufgaben notwendigen Berichte zu erstellen, ohne dass weitere Verarbeitungsschritte außerhalb des Systems durch das Zusammenführen verschiedener Auswertungen in EXCEL notwendig sind.

Um das von mir gesehene Gefährdungspotenzial nochmals deutlich zu machen: Es handelt sich um sensible Personaldaten, die die persönliche und berufliche Lebenssituation im Einzelnen wiedergeben. Besonders sensibel und schützenswert sind beispielsweise die personenbezogenen Daten in den Bereichen des LfV, der Polizei, der Staatsanwaltschaften und des LKA. Dort kann schon die Tatsache, dass ein Bediensteter bei einer dieser Stellen beschäftigt ist, eine große Gefährdung darstellen. Dies gilt z. B. auch für Justizvollzugsbeamte, deren Privatadressen keinesfalls in „falsche Hände“ geraten dürfen.

Durch die Nutzung der Download-Funktion werden diese Personaldaten, die im SAP-System mit strengen Berechtigungshinterlegungen vor unberechtigten Zugriffen und Veränderungen geschützt sind, in völlig ungeschützte Bereiche geladen. Sie werden dort ohne jede Protokollierung zusammengeführt, weiterverarbeitet und gespeichert. Es können Subsysteme angelegt werden; die Daten können z. B. auf CD-ROM gespeichert, ausgedruckt und außerhalb jeder Zweckbindung weiterverwendet werden. Eine Kontrolle ist nicht möglich.

Ich prüfe zurzeit, ob es sich bei der Speicherung von personenbezogenen Daten, die mit der Download-Funktion aus SAP R/3 HR herausgezogen und in EXCEL gespeichert, zusammengeführt und weiterverarbeitet werden, um gesonderte Personaldatenverarbeitung

handelt. Sollte dies zutreffen, muss für jede der nach einem Download aus dem SAP R/3 HR-System mit dem EXCEL-Programm vorzunehmenden Datenverarbeitungen ein Verfahrensverzeichnis nach § 6 HDSG erstellt werden. In diesen Verzeichnissen ist jeweils insbesondere Zweck und Rechtsgrundlage der konkret zu verarbeitenden Daten aufzuführen und es sind die technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 HDSG zu beschreiben.

Nur wenn das EXCEL-Programm lediglich als „Standard-Werkzeug“ z. B. für nicht personenbezogene, statistische Tabellenkalkulationen usw. genutzt wird, ist ein Verfahrensverzeichnis entbehrlich.

§ 6 HDSG

(1) Wer für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten zuständig ist, hat in einem für den behördlichen Datenschutzbeauftragten bestimmten Verzeichnis festzulegen:

1. Name und Anschrift der Daten verarbeitenden Stelle,
2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. die technischen und organisatorischen Maßnahmen nach § 10,
8. die Technik des Verfahrens,
9. Fristen für die Löschung nach § 19 Abs. 3,
10. eine beabsichtigte Datenübermittlung nach § 17 Abs. 2,
11. das begründete Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3.

(2) Die Angaben des Verfahrensverzeichnisses können bei der Daten verarbeitenden Stelle von jeder Person eingesehen werden; dies gilt für die Angaben zu Nr. 7, 8 und 11 nur, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird.

Satz 1 gilt nicht für

1. Verfahren des Landesamtes für Verfassungsschutz,
2. Verfahren, die der Gefahrenabwehr oder der Strafverfolgung dienen,
3. Verfahren der Steuerfahndung,

soweit die Daten verarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

Gerade die Vorkommnisse bei der Deutschen Bahn AG und der Deutschen Telekom AG sollten deutlich machen, wie groß das Gefährdungspotenzial für einen möglichen Datenmissbrauch sein kann.

Ich halte weiterhin die große Anzahl der vergebenen Download-Berechtigungen für unverhältnismäßig und nicht für notwendig. Im Gegensatz zur Verarbeitung der Personaldaten im SAP R/3 HR-System kann ich nicht erkennen, dass die Vorgaben des § 10 Abs. 2 HDSG bei Download-Daten eingehalten werden.

§ 10 Abs. 2 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

1. Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten (Zutrittskontrolle),
2. Unbefugte an der Benutzung von Datenverarbeitungsanlagen und -verfahren gehindert werden (Benutzerkontrolle),
3. die zur Benutzung eines Datenverarbeitungsverfahrens Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
4. personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle),
5. es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind (Verantwortlichkeitskontrolle),
6. personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist (Dokumentationskontrolle),

8. die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

4.2 Justiz, Strafvollzug und Polizei

4.2.1
Strafvollzugsgesetze

Nach dem Jugendstrafvollzugsgesetz im Jahr 2007 hat der Hessische Gesetzgeber jetzt auch ein Hessisches Strafvollzugsgesetz sowie ein Untersuchungshaftvollzugsgesetz geschaffen. Im Wesentlichen entsprechen diese Gesetze den Anforderungen des Rechts auf informationelle Selbstbestimmung.

Hessen hat nunmehr abschließend von seinen durch die Föderalismusreform geschaffenen Kompetenzen im Bereich des Strafvollzuges Gebrauch gemacht. Am 1. November 2010 sind das Hessische Gesetz über den Vollzug der Freiheitsstrafe und der Sicherheitsverwahrung (HStVollzG) sowie das Hessische Untersuchungshaftvollzugsgesetz (HUVollzG) in Kraft getreten. Das Justizministerium hatte mich schon frühzeitig bei der Erarbeitung der Gesetzentwürfe beteiligt. Die Mehrzahl meiner Anregungen sind dann auch im weiteren Verfahren berücksichtigt worden.

Hervorzuheben ist, dass in allen Gesetzen weitgehend auf Verweisungen auf andere Regelungen verzichtet worden ist. Soweit nicht die besondere Haftart es erfordert, sind die Regelungen im Wesentlichen gleichlautend. In dieser Form sind die Gesetze aus sich selbst heraus, auch für die Betroffenen, verständlich und damit gerade auch für die Praxis gut handhabbar. Dies gilt auch für die Regelungen in den Titeln zum Datenschutz, soweit die Anwendbarkeit der Regelungen des HDSG betroffen ist. Im Folgenden beziehe ich mich deshalb als Beispiel jeweils auf die Regelungen des Strafvollzugsgesetztes.

Das Gesetz enthält eine Vielzahl von Regelungen, die auch einen datenschutzrechtlichen Bezug haben. Diese sind nicht nur in dem Titel mit der Überschrift Datenschutz enthalten. So ist etwa der Einsatz von Videotechnik sowohl im Kontext der Besuchsüberwachung, bei den allgemeinen Grundsätzen zur Sicherheit und Ordnung als auch beim Einsatz von besonderen Sicherungsmaßnahmen, hier bei der Unterbringung in besonders gesicherten Hafträumen, geregelt. Dass die optische Überwachung in dem jeweiligen Kontext gewollt ist, ist eine rechtspolitische Entscheidung des Gesetzgebers. Die im Gesetz festgelegten Rahmenbedingungen – bis hin zu der Aufbewahrungsfrist der Aufnahmen von maximal 72 Stunden – wahren die datenschutzrechtlich gesteckten Grenzen.

Allerdings gilt dies nicht für alle im Gesetz getroffenen Regelungen. Meine Kritik betrifft zunächst den Umfang der zulässigen erkennungsdienstlichen Maßnahmen gem. § 58 Abs. 2 HStVollzG.

§ 58 Abs. 2 HStVollzG

Zur Sicherung des Vollzugs, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt oder zur Identitätsfeststellung sind mit Kenntnis der Gefangenen zulässig:
1. die Abnahme von Finger- und Handflächenabdrücken,
2. die Aufnahme von Lichtbildern,
3. die Feststellung äußerlicher körperlicher Merkmale,
4. die elektronische Erfassung biometrischer Merkmale und
5. Körpermessungen.

Positiv ist dabei anzumerken, dass die noch in der Vorgängerregelung des § 86 StVollzG vorgesehene Verwahrung der erkennungsdienstlichen Daten aus den Vollzugsanstalten in den kriminalpolizeilichen Sammlungen nicht übernommen wurde. Erhebliche Bedenken habe ich allerdings bezüglich der Erweiterung der möglichen erkennungsdienstlichen Daten auf die elektronische Erfassung jeglicher biometrischer Merkmale im Gesetzgebungsverfahren geäußert. Zwar ist eine entsprechende Regelung auch im Jugendstrafvollzugsgesetz sowie in den Vollzugsgesetzen anderer Bundesländer enthalten. Aufgrund der Diskussion um den Einsatz biometrischer Merkmale – u. a. im Zusammenhang mit der Ausgestaltung von Reisepass und Personalausweis – halte ich eine andere Entscheidung für zwingend notwendig.

Die technische Weiterentwicklung in diesem Bereich ist derzeit seriös nicht abschätzbar. Bei der Verarbeitung weiterer biometrischer Merkmale – über Fingerabdrücke und Lichtbilder hinaus – ist nicht auszuschließen, dass damit Erkenntnisse gewinnbar sind, die über die Identifizierung einer Person hinausgehen. Da auch nicht ersichtlich ist, dass die derzeit genutzten Merkmale für den in der Norm genannten Zweck nicht ausreichen, sehe ich keine Notwendigkeit für eine solch breite Öffnung zur Nutzung biometrischer Merkmale. Eine Schaffung von zusätzlichen Eingriffsbefugnissen „auf Vorrat“ im Hinblick auf in der Zukunft liegende technische Entwicklungen halte ich für verfassungswidrig. Der Gesetzgeber ist diesen Argumenten jedoch nicht gefolgt.

Schließlich enthält das Gesetz in § 62 Abs. 4 HStVollzG eine Regelung, die einen länderübergreifenden Datenverbund ermöglichen soll.

§ 62 HStVollzG

(1) Zur Erfüllung ihrer Aufgaben kann die Aufsichtsbehörde Daten, die in der Anstalt gespeichert sind, abrufen.

(2) Daten über die persönlichen Verhältnisse der Gefangenen, Vollstreckungsdaten, Daten zum Vollzugsverlauf und sicherheitsrelevante Daten können in einer von der Aufsichtsbehörde eingerichteten und geführten gemeinsamen Datei gespeichert werden. Die Aufsichtsbehörde darf diese Daten, soweit erforderlich, verwenden zur übergeordneten Planung, zur Sicherung der Qualität des Vollzugs oder zur Durchführung von Einzelmaßnahmen. Für die Anstalten sind die Daten Teil der jeweiligen Gefangenenpersonalakte. Eingabe, Änderung und Löschung der Daten erfolgt jeweils durch die Anstalt, die für die Gefangene oder den Gefangenen zuständig ist. Die Übermittlung und der Abruf personenbezogener Daten aus dieser Datei zu den in § 60 Abs. 1 genannten Zwecken sind zulässig, soweit diese Form der Datenübermittlung oder des Datenabrufs unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Erfüllung des Zwecks der Übermittlung angemessen ist.

(3) Für die Ausgestaltung des Verfahrens nach Abs. 2 gilt § 15 des Hessischen Datenschutzgesetzes.

(4) Durch Staatsvertrag kann mit anderen Ländern und dem Bund ein automatisierter Datenverbund nach Maßgabe der Abs. 2 und 3 eingerichtet werden.

Die Erforderlichkeit, jederzeit zu allen Strafgefangenen im gesamten Bundesgebiet Daten abrufen zu können, erschließt sich nicht. Auch die Begründung des Gesetzentwurfes sagt dazu nichts aus.

Eine Datenübermittlung im Einzelfall etwa im Zusammenhang mit dem Wunsch eines Gefangenen in eine Anstalt in einem anderen Bundesland verlegt zu werden, ist auch auf der Grundlage geltenden Rechts möglich.

Soweit der Sinn der Regelung lediglich darin besteht, zukünftige Vorhaben dieser Art zu ermöglichen und klarzustellen, dass solche gemeinsamen Dateien auf Grundlage eines Staatsvertrages eingerichtet werden können, habe ich darauf hingewiesen, dass dies nicht davon entbindet, die Erforderlichkeit und den Zweck der Übermittlung der Daten aller Gefangenen bundesweit vor der Einrichtung eines Staatsvertrages zu begründen.

Die Praxis wird zeigen, ob mit diesen Gesetzen die Interessen der Betroffenen zur Wahrung ihres Rechts auf informationelle Selbstbestimmung auch unter den besonderen Bedingungen des Strafvollzuges bzw. der Untersuchungshaft gewahrt werden können.

Aufgabe des Gesetzgebers bleibt es allerdings, auch für den Maßregelvollzug eine ausreichende gesetzliche Grundlage zu schaffen. Diese muss für den Umgang mit den Daten der Betroffenen Regelungen treffen, die denen des Strafvollzugsgesetzes entsprechen. Abweichende Festlegungen sollten nur da erfolgen, wo es die Besonderheiten des Maßregelvollzuges erfordern. Das derzeit geltende Maßregelvollzuggesetz wird diesen Anforderungen nicht gerecht.

4.2.2
Hessisches Dolmetscher- und Übersetzergesetz

Nicht in allen Punkten ist es dem Gesetzgeber gelungen, eine normenklare Regelung für die Voraussetzungen zur Beeidigung und den daraus resultierenden Pflichten der Dolmetscher zu finden.

In einer Vielzahl von gerichtlichen Verfahren werden Dolmetscher benötigt. Dies gilt ebenso für die Übersetzung von Dokumenten. Bisher wurden Dolmetscher auf Grundlage einer Verwaltungsvorschrift von den Landgerichtspräsidenten vereidigt und in eine Liste aufgenommen. Nachdem das Bundesverwaltungsgericht am 16. Januar 2007 (6 C 15/06) festgestellt hatte, dass die berufsrechtlichen Voraussetzungen für die allgemeine Beeidigung von Dolmetschern und die Ermächtigung von Übersetzern durch eine Rechtsnorm geregelt sein müssen, hat auch der hessische Gesetzgeber eine entsprechende Regelung getroffen.

Im Laufe des Gesetzgebungsverfahrens hatte ich mehrfach Gelegenheit zur Stellungnahme. Das Gesetz ist nach ausführlichen Beratungen im Landtag im Juni des Jahres in Kraft getreten. In zwei Punkten halte ich das Gesetz in dieser Form jedoch für nicht umsetzbar wenn nicht sogar für verfassungsrechtlich nicht haltbar.

4.2.2.1
Beteiligung der Ausländerbehörden bei der Überprüfung der Zuverlässigkeit

Im Gesetz ist u. a. geregelt, dass ein Dolmetscher bestimmte Voraussetzungen erfüllen muss, um beeidigt zu werden. In § 2 des Gesetzes sind die Voraussetzungen der allgemeinen Beeidigung benannt. Dies gilt sowohl für die nähere Festlegung zur Sachkunde als auch für die Kriterien zur Beurteilung der Zuverlässigkeit. Auch die notwendigen Nachweise bzw. Unterlagen werden im Gesetz benannt.

§ 2 Hessisches Dolmetscher- und Übersetzergesetz

(1) Als Dolmetscherinnen und Dolmetscher sind auf Antrag Personen allgemein zu beeidigen, die

1. Staatsangehörige eines Mitgliedstaates der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum sind,
2. ihre fachliche Eignung nachgewiesen haben,
3. zuverlässig und
4. volljährig sind.

(2) Sonstige ausländische oder staatenlose Antragstellerinnen und Antragsteller, die ihren ständigen Wohnsitz oder ihre berufliche Niederlassung im Gebiet des Landes Hessen haben und die Voraussetzungen des Abs. 1 Nr. 2 bis 4 erfüllen, können als Dolmetscherin oder Dolmetscher allgemein beeidigt werden. Für die Überprüfung der Zuverlässigkeit ist eine Stellungnahme der zuständigen Ausländerbehörde einzuholen.

(3) Fachlich geeignet ist, wer eine staatliche Dolmetscherprüfung im Inland bestanden, einen inländischen Hochschul- oder Fachhochschulabschluss im Bereich Dolmetschen oder eine als gleichwertig anerkannte ausländische Dolmetscherprüfung abgelegt hat. Ist keine Stelle vorhanden, vor der eine staatliche Dolmetscherprüfung abgelegt werden kann, so ist der Nachweis der fachlichen Eignung durch eine Bescheinigung des Amtes für Lehrerbildung – Staatliche Prüfungen – in Darmstadt zu erbringen.

(4) Die Zuverlässigkeit besitzt insbesondere nicht, wer

1. in den letzten fünf Jahren vor Stellung des Antrags wegen eines Verbrechens oder eines Vergehens nach dem Neunten oder Fünfzehnten Abschnitt des Besonderen Teils des Strafgesetzbuches oder nach dem Strafgesetzbuch wegen Begünstigung nach § 257, Strafvereitelung nach § 258, Betruges nach § 263 oder Urkundenfälschung nach § 267 oder wegen einer oder mehrerer anderer vorsätzlicher Straftaten zu einer Freiheits- oder Jugendstrafe von mehr als einem Jahr rechtskräftig verurteilt worden ist,

2. in ungeordneten Vermögensverhältnissen lebt, insbesondere über wessen Vermögen das Insolvenzverfahren eröffnet worden oder wer in das Schuldnerverzeichnis eingetragen ist, oder
3. aus gesundheitlichen Gründen nicht nur vorübergehend unfähig ist, die Tätigkeit als Dolmetscherin oder Dolmetscher auszuüben.

(5) Die antragstellende Person hat ein Führungszeugnis nach § 30 Abs. 5 des Bundeszentralregistergesetzes in der Fassung vom 21. September 1984 (BGBl. I S. 1230, 1985 I S. 195), zuletzt geändert durch Gesetz vom 14. August 2009 (BGBl. I S. 2827), zur Vorlage bei der zuständigen Stelle nach § 10 Abs. 1 zu beantragen.

(6) Dem Antrag sind die für den Nachweis der fachlichen Eignung und Zuverlässigkeit erforderlichen Unterlagen, insbesondere eine Erklärung darüber, ob eine Verurteilung nach Abs. 4 Nr. 1 erfolgt ist, beizufügen.

Einen Anspruch auf die Beeidigung haben danach Deutsche sowie EU-Bürger. Nicht EU-Bürger können ebenfalls beeidigt werden, zusätzlich zu den allgemein geltenden Voraussetzungen sieht das Gesetz für deren Beeidigung im Rahmen der Überprüfung der Zuverlässigkeit zwingend die Einholung einer Stellungnahme der zuständigen Ausländerbehörde vor.

Allerdings enthält das Gesetz keinerlei Festlegungen wozu genau die Ausländerbehörde Stellung nehmen soll. Damit fehlt der Ausländerbehörde die Entscheidungsgrundlage für den Umfang ihrer Mitwirkungsverpflichtung. Sie kann dem datenschutzrechtlichen Grundsatz, Daten nur insoweit zu verarbeiten, wie dies für die Erfüllung einer Aufgabe erforderlich ist, nicht Rechnung tragen, weil sie nicht weiß, welche Daten für die Entscheidung wirklich erforderlich sind. Die Kriterien für die Zuverlässigkeit in § 2 Abs. 4 des Gesetzes geben hierzu keinen Aufschluss, da die Ausländerbehörde zu den dort konkret benannten Punkten über keine weitergehenden Informationen verfügt.

Eine Konkretisierung, welche (zusätzlichen) Informationen der Ausländerbehörde für die Entscheidung über die Zuverlässigkeit erforderlich sind, wäre daher zwingend notwendig. Nur so wären die Ausländerbehörden in der Lage festzustellen, welche Daten sie an die für die Feststellung der Zuverlässigkeit der Antragstellerinnen und Antragsteller zuständige Präsidentin oder den zuständigen Präsidenten des Landgerichts weiterleiten dürfen. Auf der

Grundlage der derzeitigen Regelung halte ich eine Übermittlung von Daten durch eine Ausländerbehörde in diesem Kontext für unzulässig.

4.2.2.2
Verschwiegenheitspflicht der Dolmetscher und Übersetzer

Dolmetscher und Übersetzer werden in gerichtlichen Verfahren mit einem Status beteiligt, der dem anderer Verfahrensbeteiligter etwa von Protokollführern vergleichbar ist. Alle Prozessbeteiligten können sich nur dann auf diese Personen verlassen, wenn sie darauf vertrauen können, dass sich Dolmetscher auch entsprechend verhalten. Deshalb bestimmt das Dolmetscher- und Übersetzergesetz auch in seinem § 4 die Rechte und Pflichten, die sich aus der allgemeinen Beeidigung ergeben. Dazu gehört u. a. die Pflicht zur Verschwiegenheit und zum sorgsamen Umgang mit anvertrauten Unterlagen. Allerdings macht das Gesetz hiervon eine Ausnahme. Die Verschwiegenheitspflicht soll nicht gelten, für alle Tatsachen, die Gegenstand öffentlicher Verhandlung waren.

§ 4 Abs. 2 Hessisches Dolmetscher- und Übersetzergesetz

Die Dolmetscherinnen und Dolmetscher sind verpflichtet,
1. ihre Aufgaben gewissenhaft und unparteiisch zu erfüllen,
2. Verschwiegenheit zu bewahren und Tatsachen, die ihnen bei der Ausübung ihrer Tätigkeit bekannt geworden sind und die nicht Gegenstand öffentlicher Verhandlung waren, weder zu verwerten noch Dritten zur Kenntnis zu geben,
3. die ihnen anvertrauten Dokumente sorgsam aufzubewahren und von deren Inhalt Unbefugten keine Kenntnis zu geben,

.....

Gegen diese Regelung gibt es aus Sicht des Datenschutzes erhebliche Bedenken. Sie ist weder normenklar noch überzeugt die Begründung für diese Ausnahme von der Verschwiegenheitsverpflichtung.

Offensichtlich wird laut der amtlichen Begründung davon ausgegangen, dass alle im Rahmen einer mündlichen Verhandlung geäußerten Informationen/Daten gleichzusetzen sind mit Informationen aus allgemein zugänglichen Quellen entsprechend der Regelung des § 3 Abs. 4 HDSG.

§ 3 Abs. 4 HDSG

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

In der Begründung zum Dolmetscher- und Übersetzergesetz heißt es: “Hiervon ausgenommen sind Umstände, die Gegenstand öffentlicher Verhandlung waren, da diese allgemein zugänglich sind und damit nicht der Verschwiegenheit unterliegen können“; (LTDrucks. 18/1620, S. 19). Diese Auffassung ist jedoch unzutreffend.

Die in der Regel öffentliche mündliche Verhandlung, in der jeder Anwesende die dort erörterten Informationen wahrnehmen kann, ist nicht gleichzusetzen mit der Veröffentlichung einer Information in der Presse oder in einer Publikation, die ausdrücklich zur Veröffentlichung bestimmt ist.

Die Öffentlichkeit der Verhandlungen dient der Transparenz der Gerichtsbarkeit im Gegensatz zu den Geheimprozessen früherer Zeiten. Auch wenn in der Regel die Rechtsprechung zu § 203 StGB davon ausgeht, dass das was Gegenstand öffentlicher Verhandlung war kein Geheimnis mehr ist, kann daraus nicht folgen, dass damit alle Informationen jederzeit für jeden zugänglich sind. Betroffen sein können eine Vielzahl von Daten von Angeklagten oder Zeugen, ebenso wie sensible Informationen aus dem wirtschaftlichen Bereich auch im Rahmen von Zivil- oder Verwaltungsprozessen. Das Recht auf informationelle Selbstbestimmung und damit der Grundrechtsschutz der Menschenwürde verlangen auch weiterhin einen angemessenen Umgang mit solchen Informationen. Selbst die Rechtsprechung der Strafgerichte schließt nicht aus, auch nach Erörterungen in der öffentlichen Verhandlung weiterhin Tatsachen als Geheimnis einzustufen (vgl. OLG Frankfurt, Beschluss vom 11. Januar 2005, Az. 3 Ws 1003/04). Zudem sind nicht alle Verhaltensweisen, die unzulässig in das Recht auf informationelle Selbstbestimmung eingreifen, gleichzeitig auch strafbewehrt.

Dass die im Prinzip jedermann offenstehende mündliche Verhandlung nicht gleichzusetzen ist mit einer Veröffentlichung dieser Daten, sieht man auch daran, dass es weiterhin unzulässig ist, während einer solchen Verhandlung Rundfunk- oder Fernsehaufnahmen zu machen. Auch dürfen die Urteile, die ja in öffentlicher Verhandlung zu verkünden sind, nur in anonymisierter Form veröffentlicht werden. Alles andere wäre ein unzulässiger Eingriff in das Recht auf

informationelle Selbstbestimmung, wie es erst kürzlich der Verwaltungsgerichtshof Baden-Württemberg festgestellt hat (Beschluss vom 23. Juli 2010, Az: 1 S 501/10).

Auch die anderen Personen, die in dienstlicher Funktion an einer solchen Verhandlung teilnehmen, (z. B. Richter, Protokollführer und Staatsanwälte) müssen ja weiterhin für das, was ihnen in ihrer amtlichen Eigenschaft bekannt geworden ist, die Verschwiegenheitsgrundsätze beachten. Dolmetscher/Übersetzer nehmen eine vergleichbare Funktion in der Verhandlung wahr.

Im Übrigen ist schließlich das datenschutzrechtliche Gebot der Zweckbindung zu beachten. Auch dieses schränkt die Möglichkeiten, Informationen in einem anderen Kontext zu verwenden, erheblich ein. Die am Verfahren Beteiligten müssen darauf vertrauen können, dass ein Dolmetscher genauso zuverlässig mit den Informationen umgeht wie Personen, die amtlich an diesem Verfahren beteiligt sind.

Die in anderen Bundesländern bis jetzt erlassenen entsprechenden Gesetze sehen eine solche Ausnahme von der Verschwiegenheitspflicht ebenfalls nicht vor.

4.2.3
Ergebnisse der Prüfung des Justizzentrums Wiesbaden

Das Hessische Justizministerium hat in Wiesbaden mehrere Gerichte und die Staatsanwaltschaft in einem Gebäude, dem Justizzentrum, untergebracht. Das Gebäude wurde in einem ppp-Projekt erstellt und durch die Justizverwaltung angemietet. Ich habe geprüft, ob bei den gemeinsam genutzten Ressourcen die datenschutzrechtlichen Vorgaben eingehalten sind.

4.2.3.1
Gründe ein Justizzentrum in Wiesbaden einzurichten

Die Justizverwaltung versucht, Einsparmöglichkeiten zu finden. Als eine Lösung wurde die Reduzierung von Gebäudekosten gesehen. Um die Möglichkeiten privater Bauherrn nutzen zu können, wurde ein ppp-Projekt (public private partnership) aufgesetzt, bei dem entsprechend den Anforderungen der Justiz ein privater Betreiber das Gebäude erstellt. Das Hessische

Immobilienmanagement (HI) ist während der Bauphase Ansprechpartner für den Betreiber. Die Justizverwaltung mietet das Gebäude dann später an.

In Wiesbaden sollten mehrere Gerichte und eine Staatsanwaltschaft – im Folgenden werde ich verkürzend von Behörden sprechen – in dem neuen Gebäude untergebracht werden. Dadurch sollte sich auch bei gemeinsam zu nutzenden Ressourcen ein Einsparpotenzial ergeben. Dem standen, wie sich herausstellte, komplexere Abstimmprozesse bei der Nutzung und damit verbunden höhere Kosten gegenüber. Ich habe dieses Jahr – einige Wochen nach dem Einzug im Justizzentrum – geprüft, ob die datenschutzrechtlichen Anforderungen bei den gemeinsam genutzten Ressourcen in ausreichendem Maße umgesetzt wurden.

4.2.3.2
Ergebnisse

Gemeinsam genutzte Ressourcen gab es bei der IT-Infrastruktur, einem IT-Verfahren, der Videoüberwachung und bei der Zutrittskontrolle. Von diesen Punkten möchte ich auf die IT-Infrastruktur und die Zutrittskontrolle detaillierter eingehen, da sie exemplarisch die aufgetretenen Probleme aufzeigen.

4.2.3.2.1
IT-Ressourcen

Das Grundproblem bestand darin, dass jede Behörde IT-Verfahren in eigener Verantwortung betreibt und andere Komponenten mit anderen Behörden teilt. Auch war die Zahl der Mitarbeiter mit vertieften IT-Kenntnissen so gering, dass die einzelne Behörde Schwierigkeiten hatte, einen ausreichenden Service zu garantieren. Es wurde daher eine Lösung gesucht, um mit den bei den Behörden vorhandenen Mitarbeitern die gemeinsam genutzten Komponenten in ausreichender Güte zu administrieren. Von allen Behörden sollten deshalb IT-Mitarbeiter in einer Gruppe zusammengefasst werden, die die Administration der gemeinsamen Ressourcen vornimmt. Dabei musste eine rechtliche Lösung dafür gefunden werden, dass der Mitarbeiter einer Behörde die Daten anderer Behörden zur Kenntnis nehmen darf.

Um die organisatorischen Anforderungen zu erfüllen, wurde in eingehenden Diskussionen eine Vereinbarung zwischen den Behörden erarbeitet, die die Administration der gemeinsamen IT-Ressourcen regelt. Dazu wurden Mitarbeiter der beteiligten Behörden mit

einem Teil ihrer Arbeitskraft der GIT (gemeinsame IT-Stelle der Hessischen Justiz) zugeordnet, die als verantwortliche Stelle die Aufgaben der Administration wahrnimmt.

Die Anforderung, die Systeme und Subnetze der einzelnen Behörden abzuschotten und nur bei gemeinsamen Ressourcen Zugriffe aus den Subnetzen im erlaubten Maße zuzulassen, wurde in einem gemeinsamen Sicherheitskonzept beschrieben und dann umgesetzt. Ein wesentlicher Punkt betraf die Tätigkeit Dritter, wie sie beispielsweise bei Fernwartungstätigkeiten vorkommen. Erst zu einem späten Zeitpunkt wurde erkannt, dass besondere Maßnahmen ergriffen werden mussten, um die Justiznetze gegen das eigentliche Hausnetz abzuschotten. Das Hausnetz ist unter Kontrolle der Hausverwaltung und vernetzt die Haustechnik wie Heizung, Aufzüge oder auch – einige – Türöffner, wodurch sich zwangsläufig Schnittstellen ergaben. Die Schnittstellen konnten noch rechtzeitig im Sicherheitskonzept berücksichtigt werden.

Während der Prüfung konnte ich u. a. am Beispiel einer Fernwartung feststellen, dass die Vorgaben des Sicherheitskonzepts umgesetzt waren. Wartungstätigkeiten an Netzkomponenten wurden erkannt. Unzulässige Zugriffe wurden ebenfalls erkannt und führten zu entsprechenden Aktivitäten.

Nur durch eine frühzeitige, konsequente Herangehensweise wurden insoweit für die IT-Infrastruktur rechtzeitig tragfähige Lösungen gefunden.

4.2.3.2.2
Zutrittskontrolle

Es gab strukturelle Probleme, die durch die geprüften Behörden selbst ursächlich nicht zu verantworten waren.

Die jetzt im Justizzentrum befindlichen Behörden waren bei der Bauplanung nicht bzw. nur unzureichend beteiligt. Dies zeigte sich beim Zutrittskontrollsystem. Es war den Behörden praktisch nicht bekannt, welche Technik installiert war, wer die Technik warum ausgewählt hat und, zum Teil, wie sie konkret eingesetzt wird. Zwar sollten zum Zeitpunkt der Prüfung noch Einweisungen erfolgen, aber diese hätten vor dem Einzug erfolgt sein müssen. Die Technik selbst war zum Zeitpunkt meiner Prüfung nicht mehr änderbar, was beispielsweise bei der Ausgestaltung der Zutrittskontrolle Konsequenzen hinsichtlich der Bildung von Gruppen für Zutrittsrechte hatte.

Eine Ursache dieses Mankos liegt nach meiner Einschätzung in der Beteiligung einer Vielzahl verschiedener Institutionen, die als Bauherr, als Vermieter, als „Facility Manager“, als Immobilien-Management und in anderen Funktionen bei der Planung, Errichtung und Ausstattung des Justizzentrums beteiligt waren. Dies führte zu unübersichtlichen Verantwortlichkeiten – man könnte in Abwandlung eines neuen Technik-Begriffs von „Cloud-Verantwortung“ sprechen –, so dass die Behörden, für die das Gebäude geplant und errichtet wurde, kaum noch Einfluss nehmen konnten.

Das Zutrittskontrollsystem wurde zusammen mit der Zeiterfassung durch den Hersteller installiert. In diesem Bereich waren zum Zeitpunkt meiner Prüfung noch Restarbeiten zu erledigen. Die endgültige Übergabe war für einen Zeitpunkt vorgesehen, zu dem die Behörden schon lange eingezogen waren.

Federführend verantwortlich für den Betrieb der Anlage war das Landgericht. Die konkrete Vergabe von Zutrittsrechten sollten die einzelnen Gerichte in ihrem Zuständigkeitsbereich vornehmen. Die Vergabe von Zutrittsrechten für den Bereich Haustechnik/Putzkräfte führte die Betreiber-Firma durch.

4.2.3.2.2.1
Zur Technik

Es gibt zwei Typen von Kartenlesern, mit denen Türen geöffnet werden.

Online-Leser
Die Online-Leser hatten eine permanente Verbindung zu dem Server der die Zutrittsrechte verwaltet. Sie wurden insbesondere für die Einlasskontrolle der Bediensteten (einschl. Zeiterfassung) verwendet. Die Berechtigungen des Ausweisinhabers wurden täglich beim Betreten des Gebäudes auf die Karte geschrieben und waren um 23:59 Uhr ungültig. Damit war eine zeitnahe Änderung von Berechtigungen problemlos möglich.

Offline-Leser
Offline-Leser wurden für die Zutrittskontrolle der Bürotüren verwendet. Sie wurden durch den Hersteller konfiguriert und hatten keine Verbindung zum Verwaltungsserver. Die Stromversorgung erfolgte über integrierte Batterien. Auf dem Offline-Leser wurden die

zutrittsberechtigten Gruppen gespeichert. Es konnten mehr als zwei sein. Während der Prüfung stand keine Technik zur Verfügung, mit der die in einem Offline-Leser gespeicherten Gruppen ausgelesen werden konnten.

Die Berechtigungen waren auf den Zutrittskarten hinterlegt. Durch Beschränkungen des Systems waren pro Karte nur zwei Gruppen hinterlegbar. Bedingt dadurch musste das Zutrittskonzept mit wenigen Gruppen arbeiten, die folglich viele Personen umfassten.

Es gab „Demontagekarten“. Über diese war sichergestellt, dass auch im Fehlerfall (z. B. leere Batterie) ein Zutritt zu den Räumen möglich ist.

Berechtigungen konnten zum Prüfzeitpunkt nur vom Hersteller eingesehen und geändert werden.

4.2.3.2.2.2
Mandantenzuordnung

Die Mandantenzuordnung (Gerichte/Staatsanwaltschaft und Hausverwaltung) wurde anhand des Belegungskonzeptes durch den Hersteller vorgenommen. Nur der Hersteller hatte die nötigen Zugriffsrechte auf dem Server, um Änderungen vorzunehmen. Es war zum Zeitpunkt der Prüfung noch nicht abschließend geklärt, wer diese Berechtigungen nach der Übergabe erhalten sollte.

4.2.3.2.2.3
Forderungen

Aus den Feststellungen ergaben sich datenschutzrechtliche Forderungen:

– Die Verantwortlichkeiten zwischen den Vertragspartnern müssen bei der Zutrittskontrolle klarer gefasst werden.

– Im Rahmen der Übergabe muss festgelegt werden (ggf. durch gerichtsübergreifende Abstimmung), wer die zentralen Aufgaben (Mandantenverwaltung) übernimmt.

– Insbesondere im Bereich der Offline-Leser muss eine Dokumentation erstellt werden, für welche Räume welche Berechtigungen existieren.

– Es muss für die Gerichte und die Staatsanwaltschaft die technische Möglichkeit geschaffen werden, die vorgenommene Programmierung eines Offline-Lesers zu überprüfen und ggf. zu berichtigen.

– Die Ausgestaltung der Berechtigungsvergabe muss überarbeitet werden.
Die zutrittsgewährende Stelle muss wissen, wer Zutrittsrechte zu den Räumen hat; dies gilt insbesondere für Personal der Hausverwaltung einschließlich Reinigungskräfte. Sie sollte in der Lage sein, Zutrittsrechte auch an einzelne Personen zu vergeben.

4.2.3.2.3
Fazit

Die Behörden mussten die Verantwortung für eine Datenverarbeitung übernehmen, die sie nicht beeinflussen konnten und deren Ausgestaltung ihnen in Teilen unbekannt war. Bei zukünftigen Projekten muss gewährleistet werden, dass die Daten verarbeitenden Stellen ihrer Verantwortung gerecht werden können. Dazu müssen sie frühzeitig eingebunden werden und diese Möglichkeit auch nutzen. Es ist nicht zielführend, bei der Bauplanung zwar festzulegen, wo sich Serverräume und andere Teile der technischen Infrastruktur befinden sollen sowie die Kabelführung für die einzelnen Räume festzulegen, aber dabei nicht ansatzweise zu überlegen, welche Datenverarbeitung – getrennt und/oder gemeinsam – von den einzelnen Nutzern im Gebäude mit dieser Infrastruktur bewältigt werden soll.

4.2.4
Telefonieren in der Justizvollzugsanstalt

Das Führen sog. „Weißlisten“ zur Minimalkontrolle von Telefonaten, die von Gefangenen aus der Haftanstalt hinaus geführt werden, ist zulässig. Allerdings ist dafür Sorge zu tragen, dass das von der Haftanstalt gewählte Verfahren zur Aufnahme einer Rufnummer in die „Weißliste“ datenschutzrechtlich unbedenklich ausgestaltet ist.

Immer wieder erreichen mich Eingaben von Gefangenen, die sich damit beschäftigen, inwieweit Maßnahmen der Haftanstalten, durch die die Telekommunikation von Gefangenen eingeschränkt wird, zulässig sind.

In diesem Jahr wurde in Eingaben mehrfach das Verfahren zur Erstellung sog. „Weißlisten“ thematisiert.

Meine Recherchen führten zu dem Ergebnis, dass Telefonate von Gefangenen aus Gründen der Sicherheit und Ordnung in der Regel mindestens insofern überwacht werden, als diese nur solche Teilnehmer anwählen können, die zuvor auf einer sog. „Weißliste“ freigeschaltet wurden. Bevor eine solche Freischaltung erfolgt, prüfen die Anstalten in der Regel, wem der Telefonanschluss zuzuordnen ist. Zur Ermittlung des Anschlussinhabers gehen die Justizvollzugsanstalten dabei höchst unterschiedlich vor. Teilweise werden Telefonrechnungen, Verträge oder sonstige Bescheinigungen zum Nachweis der Anschlussinhaberschaft verlangt, teilweise werden aber auch die Angaben des Gefangenen durch die Haftanstalt selbst überprüft und verifiziert, etwa durch Anrufe auf der Telefonnummer oder eine eigenständige Recherche über das Internet.

Hiergegen bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken, soweit die Betroffenen in diese Datenerhebung einwilligen.

Hiervon kann jedoch nicht in allen Fällen ausgegangen werden. Lässt sich die Justizvollzugsanstalt schriftliche Nachweise vorlegen, so werden damit insbesondere bei ungeschwärzten Telefonrechnungen mit Einzelverbindungsnachweis sehr weitreichend Daten völlig unbeteiligter Dritter erhoben.

Ich habe deshalb das HMDJIE gebeten, darauf hinzuwirken, dass im Zusammenhang mit der Führung der „Weißlisten“ eine einheitliche, den Erfordernissen des Datenschutzes gerecht werdende Handhabung in allen hessischen Justizvollzugsanstalten erfolgt. Dabei muss das Hauptaugenmerk darauf liegen, dass die Daten Dritter nur im unbedingt erforderlichen Umfang erhoben werden. Da die Klärung des Anschlussinhabers schon jetzt teilweise durch die Justizvollzugsanstalten so gehandhabt wird, dass zunächst eine Recherche in öffentlich zugänglichen Telefonbüchern oder ähnlichen Verzeichnissen erfolgt bzw. die gewünschte Rufnummer von einem Justizvollzugsbeamten direkt angewählt wird, um festzustellen, wem der Anschluss zuzuordnen ist, erscheint es mir im Regelfall nicht notwendig zu sein, die Vorlage von anderen Nachweisen wie Telefonrechnungen, Verträgen oder sonstigen Bescheinigungen zu verlangen. Sollte die Vorlage von derlei Unterlagen dennoch notwendig

sein, ist auch hier darauf zu achten, dass dem Grundsatz der Datensparsamkeit und der Datenvermeidung folgend nur die erforderlichen Daten erhoben werden. So ist z. B. zu gewährleisten, dass Telefonrechnungen auch teilweise geschwärzt eingereicht werden können.

Hinsichtlich der Dokumentation des Nachweises über die Anschlussinhaberschaft ist es ausreichend, wenn ein erbrachter Nachweis in den Akten mit einem Vermerk dokumentiert wird. Sofern zum Nachweis der Anschlussinhaberschaft ein schriftlicher Nachweis gefordert wurde, ist dieser im Original wieder zurückzureichen und auch nicht in Kopie zu den Akten zu nehmen.

Hierauf hat mir das HMDJIE mitgeteilt, dass die Anstaltsleiterinnen und Anstaltsleiter im Rahmen einer Dienstbesprechung angehalten wurden, dafür zu sorgen, dass die von mir gemachten datenschutzrechtlichen Vorgaben im Verfahren mit „Weißlisten“ in den Anstalten Rechnung getragen wird.

4.2.5
Beteiligung freier Träger im Strafvollzug

Eine hessische Justizvollzugsanstalt gab im Rahmen entlassungsvorbereitender Maßnahmen die Namen von Gefangenen, deren Entlassung aus dem geschlossenen Vollzug bevorstand, an einen Träger der freien Straffälligenhilfe weiter, ohne vorher die Einwilligung der Betroffenen hierzu einzuholen. Nach meiner Intervention wurden die Anstaltsleitungen sowie die Träger der freien Straffälligenhilfe per Erlass angehalten, für die Gestaltung eines datenschutzgerechten Informationsflusses zwischen den Vollzugsanstalten und den freien Trägern der Straffälligenhilfe zu sorgen.

Seit Beginn des Jahres 2007 besteht in den Hessischen Haftanstalten des Erwachsenenvollzuges ein Übergangsmanagement zur Vorbereitung der Entlassung. Das Übergangsmanagement – das Gesetz spricht von Entlassungsvorbereitung – ist im Hessischen Strafvollzugsgesetz in § 16 geregelt.

§ 16 Abs. 1 HStVollzG

Die Anstalt arbeitet frühzeitig, spätestens sechs Monate vor dem voraussichtlichen Entlassungszeitpunkt, darauf hin, dass die Gefangenen über eine geeignete Unterbringung und eine Arbeits- oder Ausbildungsstelle verfügen sowie bei Bedarf in nachsorgende Maßnahmen vermittelt werden. Hierbei arbeitet sie mit Dritten (§ 7), insbesondere der Bewährungshilfe, den Führungsaufsichtsstellen und der freien Straffälligenhilfe zum Zwecke der sozialen und beruflichen Eingliederung der Gefangenen zusammen.(…)

Anlässlich der Eingabe eines Gefangenen erhielt ich vertieften Einblick in die Praxis der Einbeziehung der freien Straffälligenhilfe in die Entlassungsvorbereitung:

In dem von dem Gefangenen an mich herangetragenen Fall wurden der freien Straffälligenhilfe die Namen der Häftlinge, für die eine Entlassungsvorbereitung eingeleitet werden soll, direkt übermittelt. Die freie Straffälligenhilfe hat sodann die Betroffenen in einer Informations- und Motivationsphase über das Übergangsmanagement und seine Möglichkeiten informiert. Im Anschluss an diese Phase konnten die Gefangenen entscheiden, ob sie mit der freien Straffälligenhilfe im Übergangsmanagement zusammenarbeiten wollten.

Diese Praxis entsprach jedoch nicht den datenschutzrechtlichen Anforderungen an eine zulässige Weitergabe von Daten an eine Stelle außerhalb der Haftanstalt.

Da weder das Hessische Strafvollzugsgesetz noch das Hessische Datenschutzgesetz eine Übermittlung der Daten von Gefangenen an die freie Straffälligenhilfe vorsieht, dürfen die Namen der infrage kommenden Gefangenen erst dann an die freie Straffälligenhilfe übermittelt werden, wenn die Betroffenen ohne jeden Zweifel in die Übermittlung eingewilligt haben.

Ich habe das HMDJIE deshalb aufgefordert, darauf hinzuwirken, dass die Haftanstalten immer nur dann entsprechende Daten übermitteln, wenn die Gefangenen ausdrücklich zugestimmt haben. Dem ist das Ministerium nachgekommen und hat in einem Erlass klargestellt, dass die Gefangenen zunächst durch den internen Sozialdienst vom Beratungsangebot der freien Straffälligenhilfe mit einem Formblatt in Kenntnis gesetzt werden. Die Gefangenen bestätigen mit einer Unterschrift, ob sie mit der Betreuung durch das Übergangsmanagement einverstanden sind oder nicht. Ist die oder der Gefangene mit der Betreuung einverstanden, erhält die Übergangsmanagerin oder der Übergangsmanager eine Kopie des unterschriebenen Formblattes. Ist die oder der Gefangene mit der Betreuung nicht einverstanden wird das Formblatt zur Gefangenenpersonalakte genommen und darf selbstverständlich nicht an die Übergangsmanagerin oder den Übergangsmanager weitergeleitet werden.

Durch diese Vorgaben sollte gewährleistet sein, dass es künftig nicht zu Datenübermittlungen von den Haftanstalten an die Träger der freien Straffälligenhilfe kommt, ohne dass die Gefangenen dieser Übermittlung vorher zugestimmt haben.

4.2.6
Übermittlung von Informationen der Polizei an Fahrerlaubnisbehörden

Die Polizei darf Erkenntnisse bereits dann an die Fahrerlaubnisbehörden übermitteln, wenn ein begründeter Verdacht besteht, dass eine Person aufgrund nicht nur vorübergehender Mängel zum Führen von Kraftfahrzeugen nicht befähigt ist. Ob tatsächlich ein derartiger Mangel besteht, muss zum Zeitpunkt der Übermittlung noch nicht feststehen.

Immer wieder erreichen mich Eingaben, bei denen die Frage im Raum steht, inwieweit die Polizei ihre Erkenntnisse anderen Verwaltungsbehörden mitteilen darf. Mehrfach ging es dabei in diesem Jahr um die Frage, inwieweit die Polizei Daten an die Fahrerlaubnisbehörden übermitteln darf.

In einem konkreten Fall hatte die Polizei nach einem Verkehrsunfall die Untersuchung von Blut- und Urinproben sowie einen Atemalkoholtest eines Unfallbeteiligten veranlasst. Die Untersuchungsergebnisse fielen zum Teil widersprüchlich aus. Während sich aus dem Atemalkoholtest und der Urinprobe keinerlei Hinweise auf den Konsum von Alkohol oder Drogen ergaben, zeigte die Blutprobe einen Konsum von Cannabis an. Das hierauf von der Staatsanwaltschaft betriebene Verfahren zur Entziehung der Fahrerlaubnis des Unfallbeteiligten wurde vom Gericht schließlich eingestellt.

Dennoch ordnete die Fahrerlaubnisbehörde eine medizinisch-psychologische Untersuchung (MPU) an. In der Begründung der Anordnung wurde auf das rechtsmedizinische Gutachten, welches noch vor Abschluss des gerichtlichen Verfahrens zur Einziehung der Fahrerlaubnis an die Fahrerlaubnisbehörde übermittelt wurde, verwiesen. Es war daher fraglich, ob die Polizei die medizinischen Daten des Verkehrsunfallbeteiligten an die Fahrerlaubnisbehörde weitergeben durfte noch bevor feststand, wie das Gericht mit den sich widersprechenden Befunden umgehen und das Verfahren um den Entzug der Fahrerlaubnis ausgehen würde.

Hierauf war dem Eingeber mitzuteilen, dass die Übermittlung der Daten durch die Polizei an die Fahrerlaubnisbehörde datenschutzrechtlich nicht zu beanstanden ist. Die Übermittlung findet ihre gesetzliche Grundlage in § 2 Abs. 12 StVG.

§ 2 Abs. 12 StVG

Die Polizei hat Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden zu übermitteln, soweit dies für die Überprüfung der Eignung oder Befähigung aus Sicht der übermittelnden Stelle erforderlich ist.

Mit einer entsprechenden Mitteilung an die Fahrerlaubnisbehörde muss die für die Gefahrenabwehr zuständige Polizei nicht abwarten, bis gerichtlich festgestellt ist, dass eine mangelnde Befähigung zum Führen von Kraftfahrzeugen tatsächlich besteht. Dies wird aus der gesetzlichen Formulierung, nach der bereits Informationen über Tatsachen, die auf entsprechende Mängel *schließen lassen*, von der Polizei an die Fahrerlaubnisbehörde zu übermitteln sind, deutlich.

Nachdem es in dem hier beschriebenen Fall zu einem Verkehrsunfall kam und das Ergebnis der Blutprobe einen Cannabiskonsum angezeigt hatte, halte ich die Übermittlung von der Polizei an die Fahrerlaubnisbehörde für zulässig.

4.3 Verfassungsschutz

4.3.1
Neues Datenverarbeitungssystem HARIS beim Hessischen Landesamt für Verfassungsschutz – weitere Entwicklungen

Das Hessiche Landesamt für Verfassungsschutz hat die Arbeiten an dem Datenverarbeitungssystem HARIS fortgesetzt. In die Planung und Umsetzung wurde ich einbezogen.

Im 38. Tätigkeitsbericht (Ziff. 4.3.1) hatte ich davon berichtet, dass das HLfV den Aufbau eines Hessischen Analyse- und Recherchesystems (HARIS) plant. HARIS soll als eigene Amtsdatei des HLfV neben das nachrichtendienstliche Informationssystem NADIS (s. a. Ziff. 3.1) treten, an dem sich das BfV und alle Landesämter für Verfassungsschutz beteiligen.

4.3.1.1
Sachstand

Dem Ziel, ein einheitliches Datenverarbeitungssystem zu nutzen, ist das HLfV im laufenden Jahr nähergekommen. Nach der Migration der Daten aus den alten Amtsdateien LARGO und CRIME nach HARIS werden die Daten in den alten Systemen nicht mehr aktiv genutzt. Informationen, die den Aufgabenbereich Sicherheitsüberprüfung betreffen, konnten bisher noch nicht migriert werden. Denn die Anpassung der Software, die auch die verschiedenen Nachberichtspflichten bei den Sicherheits- und Zuverlässigkeitsüberprüfungen organisieren soll, war im Berichtszeitraum noch nicht abgeschlossen. HARIS ist im Gegensatz zum alten NADIS als bloßes Aktenhinweissystem ein Wissensnetz; es können also die zu einer Person oder einem Objekt gehörenden Informationen direkt eingespeichert werden. Durch variable Verknüpfungsmöglichkeiten und insbesondere deren grafischer Darstellung werden die erforderlichen Auswertungen wesentlich effizienter. Da NADIS jetzt ebenfalls zu einem Wissensnetz als NADIS WN 1.0 (s. Ziff. 3.1) ausgebaut werden soll, wird dieser Unterschied künftig entfallen. Es wird sich dann aber die Frage nach dem Mehrwert stellen, d.h. welchen weiteren Nutzen das HLfV aus dem Betrieb von HARIS ziehen kann.

HARIS soll im Sommer 2011 mit Ausnahme des Moduls „Sicherheitsüberprüfung“ zum Einsatz kommen.

4.3.1.2
Rechtliche und technische Bewertung

Das HLfV hat die nötige Vorabkontrolle durchgeführt und mir die zur datenschutzrechtlichen Bewertung erforderlichen Informationen zur Verfügung gestellt.

Positiv zu bewerten ist, dass die Schwelle für eine Speicherung in HARIS den Anforderungen für eine Speicherung in NADIS im Wesentlichen entspricht. Grundsätzlich erfolgt für jeden Datensatz, der in HARIS gespeichert wird, auch eine NADIS-Speicherung. Ausnahmen bestehen für jene Fälle, in denen das Gesetz über das Landesamt für Verfassungsschutz (VerfSchG) eine Speicherung unter weitergehenden Voraussetzungen zulässt, also z. B. im Fall von Minderjährigen (14- bis 17-Jährigen) oder sog. unbeteiligte Personen. Unbeteiligte sind Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, dass sie selbst extremistische Bestrebungen oder Tätigkeiten im Sinne der Aufgabenerfüllung des Verfassungsschutzes nachgehen. Sie stehen allerdings bspw. mit Zielpersonen oder Objekten in zufälligem oder flüchtigem Kontakt und sind deshalb aus Sicht des HLfV für die Bewertung des Zielobjektes wichtig. Hier habe ich mich dafür eingesetzt, dass diese Personen nur sehr eingeschränkt erfasst bzw. dargestellt werden und in jedem Fall die Speicherung nach zwei Jahren auf ihre Erforderlichkeit hin geprüft werden muss.

Weitere Probleme gab es bei der Speicherung von Informationen über Verstorbene, die ausnahmsweise erfolgen soll, wenn ihre Speicherung für die Aufgabenerfüllung und das Verständnis für gespeicherte Informationen weiterhin erforderlich ist. Auch hier ist die Erforderlichkeit der Speicherung alle zwei Jahre zu prüfen.

Bei der im Laufe des Jahres 2011 geplanten Migration von Daten, die im Rahmen der Mitwirkung des HLfV bei der Sicherheitsüberprüfung u. a. von Personen im öffentlichen Dienst gespeichert werden, habe ich die Erforderlichkeit der strikten Abschottung dieser Daten von den anderen Informationen betont. Meine Forderungen hinsichtlich der Verarbeitung und der Abschottung der Daten wurden in den technischen Konzepten berücksichtigt.

Ich werde das Projekt weiter datenschutzrechtlich begleiten und mich im nächsten Jahr von der ordnungsgemäßen Umsetzung der technischen Konzepte überzeugen.

4.4 Ausländerwesen

4.4.1
Verpflichtungserklärung für die Einladung eines Ausländers

Die Ausländerbehörde ist verpflichtet, die Bonität der Person, die sich verpflichtet für den Unterhalt eines Ausländers während seines Aufenthalts in der Bundesrepublik Deutschland aufzukommen, zu überprüfen. Der Umfang der hierzu vorzulegenden Unterlagen richtet sich nach den Umständen im Einzelfall.

Um ein Visum für die Einreise in die Bundesrepublik Deutschland zu erhalten, muss ein Nachweis vorgelegt werden, dass die Kosten für den Lebensunterhalt des Einreisenden während seines Aufenthalts in Deutschland gedeckt sind. Verfügt der Visumsantragsteller selbst nicht über ausreichende finanzielle Mittel, kann die gesicherte Finanzierung seines Aufenthalts auch mittels einer Verpflichtungserklärung durch eine dritte Person nach § 68 AufenthG erbracht werden. Durch die Abgabe einer solchen Verpflichtungserklärung übernimmt der Aussteller die finanzielle Verantwortung für den Visumsantragsteller.

§ 68 Abs. 1 AufenthG

Wer sich der Ausländerbehörde oder einer Auslandsvertretung gegenüber verpflichtet hat, die Kosten für den Lebensunterhalt eines Ausländers zu tragen, hat sämtliche öffentliche Mittel zu erstatten, die für den Lebensunterhalt des Ausländers einschließlich der Versorgung mit Wohnraum und der Versorgung im Krankheitsfalle und bei Pflegebedürftigkeit aufgewendet werden, auch soweit die Aufwendungen auf einem gesetzlichen Anspruch des Ausländers beruhen. (…)

Diese Verpflichtungserklärung gilt jedoch erst dann als Nachweis darüber, dass ausreichende finanzielle Mittel vorhanden sind, wenn die Ausländerbehörde die Bonität des sich Verpflichtenden überprüft und bestätigt hat.

Durch eine Eingabe wurde ich auf die Homepage einer Ausländerbehörde aufmerksam, in der über die Verpflichtungserklärung informiert wurde. Neben einem Antragsformular und der Verpflichtungserklärung selbst wurde dort ein weiteres Dokument „Informationen zur Verpflichtungserklärung“ vorgehalten. Dieses erweckte den Eindruck, dass bei der Abgabe einer Verpflichtungserklärung standardmäßig umfangreichste Unterlagen vorzulegen wären. Dabei handelte es sich neben Einkommensnachweisen und einem Wohnraumnachweis auch

um Nachweise über monatliche Nebenkosten für Haus und Wohnung und Nachweise über laufende Verbindlichkeiten (Darlehen, Versicherungen, Unterhaltszahlungen, andere Verbindlichkeiten).

Meine Nachfrage hierzu bei der Ausländerbehörde ergab, dass dieses Dokument in keinem Fall so zu verstehen sei, dass derart weitreichende Nachweise standardmäßig verlangt würden; die erforderliche Bonitätsprüfung würde stets einzelfallbezogen durchgeführt. Dies war für den Bürger jedoch nicht ohne Weiteres erkennbar. Nur aus der Betrachtung der verschiedenen zu diesem Thema von der Ausländerbehörde bereitgehaltenen Informationen wurde erkennbar, dass nicht alle genannten Unterlagen in jedem Fall vorzulegen sind. Das missverständliche Dokument wurde deshalb von der Homepage der Ausländerbehörde entfernt. Ein entsprechend modifiziertes eindeutiges Dokument, das den datenschutzrechtlichen Vorgaben entspricht, soll nach interner Überarbeitung sodann wieder auf der Homepage eingestellt werden.

4.4.2
Akteneinsicht im Aufenthaltsgenehmigungsverfahren

Während des Verfahrens der Sicherheitsbefragung im Rahmen der Erteilung eines Aufenthaltstitels ist Einsicht in das über die Befragung angefertigte Protokoll zu gewähren.

Durch Eingaben eines Rechtsanwaltes wurden zwei gleich gelagerte Fälle an mich herangetragen, in denen eine Ausländerbehörde dem Rechtsanwalt Einsicht in die Protokolle zur Sicherheitsbefragung seiner Mandanten verwehrte. Diese Fälle veranlassten mich dazu, mich näher mit dem Verfahren zur Erteilung von Aufenthaltstiteln zu befassen.

Vor der Erteilung eines Aufenthaltstitels wie z. B. eines Visums oder einer Aufenthaltserlaubnis ist es etwa bei Angehörigen bestimmter Staaten erforderlich, dass die Ausländerbehörden feststellen, ob Gründe nach § 54 Nr. 5 bis 5b AufenthG vorliegen, die eine Versagung des Aufenthaltstitels nach sich ziehen.

§ 54 AufenthG

Ein Ausländer wird in der Regel ausgewiesen, wenn
…

5. Tatsachen die Schlussfolgerung rechtfertigen, dass er einer Vereinigung angehört oder angehört hat, die den Terrorismus unterstützt, oder eine derartige Vereinigung unterstützt oder unterstützt hat; …

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

5b. Tatsachen die Schlussfolgen rechtfertigen, dass er eine in § 98a Abs. 1 des Strafgesetzbuches bezeichnete schwere staatsgefährdende Gewalttat gemäß § 89a Abs. 2 des Strafgesetzbuches vorbereitet oder vorbereitet hat, …

Zur Prüfung dieser Frage richtet die Ausländerbehörde eine sog. Sicherheitsanfrage an das Landesamt für Verfassungsschutz und das Hessische Landeskriminalamt. Bieten die Antworten dieser Behörden Anlass dazu, wird eine Sicherheitsbefragung mit der Ausländerin bzw. dem Ausländer durchgeführt. Nach einem Erlass des HMDIS ist während des Verfahrens der Sicherheitsbefragung keine Akteneinsicht zu gewähren.

In den vom Rechtsanwalt an mich herangetragenen Fällen hatte die Ausländerbehörde dem Rechtsanwalt keine Einsicht in das Protokoll der Sicherheitsbefragung seines Mandanten gewährt.

Zur Begründung der Ablehnung des Akteneinsichtsgesuchs führte die Ausländerbehörde an, dass sie hierzu nach § 29 Abs. 2 HVwVfG nicht verpflichtet sei.

§ 29 Abs. 2 HVwVfG

Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit durch sie die ordnungsgemäße Erfüllung der Aufgaben der Behörde beeinträchtigt, das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen der Beteiligten oder dritter Personen, geheim gehalten werden müssen.

Soweit die in den Akten zur Sicherheitsbefragung befindlichen Unterlagen diese Kriterien erfüllen, indem sie etwa Erkenntnisse des Verfassungsschutzes enthalten, deren Bekanntwerden das Wohl des Landes Nachteile bereiten würde, ist einer Weigerung der

Ausländerbehörde, Akteneinsicht zu gewähren aus datenschutzrechtlicher Sicht nichts entgegenzusetzen.

Anders ist dies jedoch für das Protokoll der Sicherheitsbefragung zu bewerten. Da das Protokoll eine schriftliche Darstellung der mit der oder dem Betroffenen besprochenen Fragen ist, kann es keine Inhalte aufweisen, die der oder dem Betroffenen nicht bereits bekannt sind. § 29 Abs. 2 HVwVfG stand daher der begehrten Einsicht allein in das Protokoll der Befragung nicht entgegen.

Bei einem Gespräch mit dem HMDIS ergab sich, dass das Ministerium meine Auffassung teilte. Es hat mir gegenüber klargestellt, dass sich der Erlass und dessen Aussage bezüglich der Akteneinsicht im Verfahren der Sicherheitsbefragung nicht auf die Protokolle der Sicherheitsbefragung selbst bezogen. Das Ministerium veranlasste daher, dass die Ausländerbehörde dem Rechtsanwalt die begehrte Einsicht gewährte. Außerdem hat das Ministerium mir gegenüber zugesagt, dass der Erlass an der entsprechenden Stelle bei nächster Gelegenheit so umformuliert wird, dass derartige Irritationen nicht mehr entstehen können.

4.5 Schulen und Schulverwaltung

4.5.1
Änderung des Hessischen Schulgesetzes

Eine Novelle zum Hessischen Schulgesetz sieht u. a. einige wenige datenschutzrechtlich relevante Regelungen vor. Die geplanten Neuerungen unterstütze ich grundsätzlich.

Das Hessische Kultusministerium hat mich zu dem Vorhaben angehört, das Hessische Schulgesetz in der geänderten Fassung vom 14. Juli 2009 erneut zu ändern.

Der Gesetzentwurf verfolgt die Zielsetzung, die Eigenverantwortung und Selbständigkeit der Schulen zu stärken. Die Weiterentwicklung der Schulaufsicht, des Anspruchs auf sonderpädagogische Förderung und die Qualität der schulischen Bildung sind u. a. weitere Ziele der vorgesehenen Novelle. Zu wenigen Regelungen, die auch von datenschutzrechtlicher Relevanz sind, habe ich Stellung genommen:

§ 3 HSchG beschreibt die Grundsätze der Verwirklichung des allgemeinen schulischen Bildungs- und Erziehungsauftrages. Dort soll ein Absatz neu eingefügt werden:

§ 3 Abs. 10 HSchG (Entwurf)

Die Schule arbeitet mit den Jugendämtern zusammen. Sie soll das zuständige Jugendamt unterrichten, wenn tatsächliche Anhaltspunkte für eine Gefährdung oder Beeinträchtigung des Wohls einer Schülerin oder eines Schülers bekannt werden. Dies gilt auch für Schulen in freier Trägerschaft.

Dieser neue Absatz 10 beschreibt die Zusammenarbeit der Schule mit den Jugendämtern und die Rechtmäßigkeit von Datenübermittlungen "zum Wohle des Kindes". Näheres zum Verhältnis von Kindeswohl und Datenschutz s. mein 35. Tätigkeitsbericht, Ziff. 5.8.1. Die explizite Regelung im Schulgesetz wird von mir begrüßt.

§ 83 HSchG regelt die Erhebung und Verarbeitung von personenbezogenen Daten. Hier soll in Absatz 1 ein zweiter Satz eingefügt werden:

§ 83 Abs. 1 Satz 2 HSchG (Entwurf)

Über jede Schülerin und jeden Schüler wird eine Schülerakte geführt; sie ist vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Zur Schülerakte gehören alle Unterlagen einschließlich der in Dateien gespeicherten, die die Schülerin oder den Schüler betreffen, soweit sie mit dem Schulverhältnis in einem unmittelbaren Zusammenhang stehen (Schüleraktendaten).

Damit wäre der Begriff der Schülerakte erstmals ausdrücklich im Schulgesetz beschrieben. Die Beschreibung bezieht in den Begriff der Schülerakte ausdrücklich die in Dateien gespeicherten Daten der jeweiligen Schülerinnen und Schüler ein. Die Einführung einer Legaldefinition unterstütze ich. Das Fehlen einer Erheblichkeitsschwelle bei der Beschreibung, welche Unterlagen in der Schülerakte aufbewahrt werden sollen, kann aus datenschutzrechtlicher Sicht jedoch nicht zufriedenstellen. Ich habe deshalb empfohlen, dem Satz 2 die Passage "und für die weitere Entwicklung der Schülerin oder des Schülers wesentlich sind" anzufügen.

Daten die im Rahmen der Schulgesundheitspflege und der Tätigkeit von Schulpsychologinnen und Schulpsychologen verarbeitet werden, werden durch § 83 Abs. 6 HSchG besonders geschützt. Im Hinblick auf die letzten Fälle von Amokläufen an Schulen beabsichtigt die Landesregierung eine Ausnahme für solche Fälle zu schaffen, in denen die Untersuchungen Hinweise auf möglicherweise bevorstehende Handlungen von Schülerinnen oder Schülern ergeben haben, die mit einer erheblichen Selbst- oder Fremdgefährdung verbunden sein können. Der genaue Wortlaut der vorgesehenen Norm stand zum Redaktionsschluss dieses Berichtes noch nicht fest. Ich habe dem Kultusministerium signalisiert, gegen eine solche Norm keine grundsätzlichen Einwände zu erheben.

4.5.2
Schwarze Listen über Lehrer

Bei der Einführung des gemeinsamen Verfahrens „Informationsliste der Schulverwaltung zur Vermeidung der Wiedereinstellung ungeeigneter Lehrkräfte“ wurde ich nicht rechtzeitig beteiligt. Bei der anlassbezogenen Prüfung ergab sich erheblicher Nachbesserungsbedarf.

Kurz nach Redaktionsschluss meines letzten Tätigkeitsberichtes machte eine Schlagzeile Furore: "Schwarze Listen über Lehrer". Der dabei entstandene Eindruck, mit der Liste sollten unbeliebte oder politisch nicht linientreue Lehrer vom Schuldienst ausgeschlossen werden

oder es werde ein Berufsverbot konstatiert, bestätigte sich nicht. Allerdings gibt es eine Informationssammlung zu ungeeigneten Lehrkräften. Sie wird bei einer Organisationseinheit des Staatlichen Schulamtes Darmstadt, dem Zentralen Personal Management (ZPM), seit 1. April 2009 geführt. Die Presseberichte haben mich zu einer sofortigen Prüfung bei dieser Stelle veranlasst, bei der sich auch der in der Presse genannte Umfang der Datensammlung bestätigte. Ca. 60 Personen waren dort in einer automatisierten Datei erfasst. Die Bezeichnung der Liste lautet nicht "Schwarze Liste", sondern "Informationsliste der Schulverwaltung zur Vermeidung der Wiedereinstellung ungeeigneter Lehrkräfte". In allen Staatlichen Schulämtern des Landes haben jeweils zwei Bedienstete - in der Regel der Justiziar und ein Vertreter - lesenden Zugriff auf die Datei. Die Eintragungsbefugnis liegt ausschließlich beim ZPM.

Der Datensatz besteht aus folgenden Informationen:
– Name, Vorname und Telefonnummer der für die Eintragung verantwortlichen Person
– Name, Vorname, Geburtsdatum und Art der Lehramtsbefähigung der betroffenen Lehrkraft sowie Grund der Eintragung.

Bei der für die Eintragung verantwortlichen Person handelte es sich regelmäßig um den Justiziar des Staatlichen Schulamtes, welcher die Eintragung in der Liste veranlasst hat.

Für den Inhalt des Datenfeldes "Grund für die Eintragung" kann unter sechs fest vorgegeben Feldinhalten ausgewählt werden:
– Nichtaufnahme in die Rangliste aus Gründen in der Person
– Nichtaufnahme in die Rangliste aus fachlichen Gründen
– Entlassung aus fachlichen Gründen
– Entlassung aus Gründen in der Person
– Entlassung auf eigenen Antrag wegen drohender Entlassung
– Nichtbewährung in befristeten Verträgen.

Die Eintragung in der Liste komme nicht einem Berufsverbot gleich, so das ZPM. Wenn sich im Laufe der Zeit herausstelle, dass die Eignung wiederhergestellt sei, so erfolge die Löschung in der Datensammlung. Ein konkreter Einzelfall, in dem diese Prüfung gerade stattfand, wurde mir vorgelegt. Unmittelbar gezogene Stichproben führten in allen Fällen zu dem Ergebnis, dass die Bewertung, die betreffende Person sei für den Schuldienst ungeeignet, nachvollziehbar war. Teilweise gingen der Entlassung rechtskräftige strafrechtliche Verurteilungen voraus. In den meisten Fällen lagen auch abgeschlossene gerichtliche Auseinandersetzungen über die Beendigung des Arbeits- oder

Beamtenverhältnisses vor. Jedenfalls wurde deutlich, dass der mit der Informationssammlung verfolgte Zweck, die in einem Bezirk eines staatlichen Schulamtes gewonnene Information über die Nichteignung der betroffenen Person, auch allen anderen Schulamtsbezirken zugänglich zu machen, zum Schutze der Schüler hinreichend gerechtfertigt war.

Zweierlei war allerdings zu bemängeln:

4.5.2.1
Die mangelnde Transparenz

Zwar mag den meisten Betroffenen aufgrund der vorherigen Auseinandersetzung mit dem jeweiligen Dienstherren klar sein, dass sie als ungeeignet eingeschätzt werden und – zumindest vorläufig – nicht mit einer Wiedereinstellung rechnen können. Trotzdem ist ihnen nicht bekannt gewesen, dass dieser Sachverhalt automatisiert gespeichert und landesweit allen Staatlichen Schulämtern zur Verfügung steht. Der Regelung des § 107g Abs. 5 Satz 1 HBG, wonach bei erstmaliger Speicherung dem Betroffenen die Art der über ihn gespeicherten Daten mitzuteilen und er bei wesentlichen Änderungen zu benachrichtigen ist, wurde nicht hinreichend Rechnung getragen.

Das hessische Kultusministerium hat diesen Mangel unmittelbar nach dem Auftreten der öffentlichen Diskussion beseitigt. Es hat alle Personen, die auf der Liste verzeichnet waren, über die Datenspeicherung informiert. Außerdem wurde zugesichert, ab dem damaligen Zeitpunkt neu einzutragende Betroffene jeweils über den Eintrag zu benachrichtigen. Damit ist dem Verlangen nach Transparenz hinreichend Rechnung getragen worden.

4.5.2.2
Verfahrensrechtliche Mängel

Die Staatlichen Schulämter Hessens sind selbständige Daten verarbeitende Stellen. Die Datenverarbeitung in der Form, dass alle Staatlichen Schulämter gemeinsam einen Datenbestand unter der Federführung der ZPM verarbeiten, stellt ein gemeinsames Verfahren nach § 15 HDSG dar. Gemäß § 15 Abs. 1 HDSG bin ich vor der Einrichtung eines von mehreren Daten verarbeitenden Stellen genutzten gemeinsamen Verfahrens anzuhören. Mir sind dabei u. a. die Aufgaben der beteiligten Stellen, die getroffenen technischen und organisatorischen Datensicherheitsmaßnahmen, das Verfahrensverzeichnis nach § 6 Abs. 1

und das Ergebnis der Vorabkontrolle nach § 7 Abs. 6 Satz 3 HDSG vorzulegen. Diese Beteiligung war unterblieben.

§ 15 Abs. 1 HDSG

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

Das Staatliche Schulamt Darmstadt habe ich aufgefordert, die eigentlich vor Errichtung des gemeinsamen Verfahrens erforderliche Beteiligung unter Vorlage der in § 15 Abs. 1 HDSG bezeichneten Unterlagen, welche zum Zeitpunkt der damaligen Befassung nur zum Teil existent waren, nachzuholen.

Mittlerweile sind alle anzufertigenden Beschreibungen vorhanden. Mir ist ein Exemplar des Gesamtverzeichnisses für das gemeinsame Verfahren nach § 15 HDSG mit allen notwendigen Angaben präsentiert worden. Auch das Ergebnis der Vorabkontrolle nach § 7 Abs. 6 HDSG sowie ein IT-Sicherheitskonzept wurde mir vorgelegt. Die Verfahrensverzeichnisse nach § 6 sowie des Gesamtverzeichnis nach § 15 HDSG werden vom ZPM zur Einsicht für "jedermann" bereitgehalten. Zudem kann das Verzeichnis nach § 6 HDSG bei allen staatlichen Schulämtern eingesehen werden.

Der betroffene Personenkreis "ungeeigneter Lehrkräfte" wurde noch um ungeeignete "Sozialpädagogen und Erzieher" ergänzt, für die dieselben Transparenzregeln gelten. Auf dieser Basis habe ich das Verfahren nach der in § 15 Abs. 1 Satz 1 vorgeschriebenen Abwägung mit den schutzwürdigen Belangen der Betroffenen als angemessen angesehen. Die getroffenen Datensicherheitsmaßnahmen sind hinreichend.

Ich habe dem Staatlichen Schulamt Darmstadt mitgeteilt, dass ich nunmehr gegen das Führen des gemeinsamen Verfahrens keine Einwände mehr erhebe.

4.5.3
Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz von Lehrkräften

Hessische Lehrkräfte dürfen personenbezogene Daten auch an ihrem häuslichen Arbeitsplatz verarbeiten. Dies ist zulässig, wenn die Lehrkräfte den erlaubten Umfang und die Datensicherheitsmaßnahmen einhalten, mir für Kontrollen den Zugang zu diesem Arbeitsplatz gewähren und dies bei der erforderlichen Anzeige der häuslichen Datenverarbeitung bei der Schulleitung zusichern.

Aufgrund einer Ermächtigung im Hessischen Schulgesetz hat das Hessische Kultusministerium mit Verordnung vom 4. Februar 2009 (ABl. 3/2009 S. 131) geregelt, unter welchen Bedingungen personenbezogene Schüler- und Schuldaten durch Lehrkräfte auf privaten Datenverarbeitungseinrichtungen außerhalb der Schule verarbeitet werden dürfen. Gemeint ist der häusliche Arbeitsplatz von Lehrern. Es gibt u. a. eine Anzeigepflicht, einen fest umrissenen Datensatz, der verarbeitet werden darf und ein Löschgebot.

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

(1) Eine automatisierte Verarbeitung personenbezogener Schüler- und Schuldaten durch Lehrkräfte auf privaten Datenverarbeitungseinrichtungen außerhalb der Schule darf nur nach einer entsprechenden schriftlichen Anzeige bei der Schulleitung erfolgen.

Die Anzeige muss enthalten:

1. Eine Beschreibung der vorgesehenen Datenarten und Einsatzzwecke,
2. eine Verpflichtung, die Datensicherheitsmaßnahmen im Sinne des § 10 des Hessischen Datenschutzgesetzes einzuhalten,
3. die Erklärung der Lehrkraft, sich der Kontrolle des Hessischen Datenschutzbeauftragten zu unterwerfen sowie die Verpflichtung, dessen Beauftragten nach vorheriger Terminvereinbarung Zugang zu der häuslichen Arbeitsstätte zu gewähren, um die vorhandenen Datensicherungsmaßnahmen und die Einhaltung der Datensicherungsmaßnahmen zu überprüfen. Die Verpflichtung muss die Zusicherung enthalten, dass mögliche Mitinhaberinnen oder Mitinhaber der Wohnung mit dieser Zugangsregelung einverstanden sind.

(2) Auf den privaten Datenverarbeitungseinrichtungen der Lehrkräfte dürfen nur die in Abschnitt A 6 der Anlage 1 genannten personenbezogenen Daten verarbeitet werden, soweit dies zu der jeweiligen dienstlichen Aufgabenerfüllung erforderlich ist. Nach Ende des Datenverarbeitungsvorgangs sind alle für die Schüler- oder die Schulaktenführung relevanten Daten unverzüglich zu diesen Akten zu nehmen.

(3) Bei einer automatisierten Texterstellung für Zeugnisse, Mitteilungen, Benachrichtigungen und ähnliche Schriftstücke sind die hierzu erforderlichen personenbezogenen Daten nach Abschluss der Aufgabe unverzüglich zu löschen. Ausschließlich zu dem in Satz 1 genannten Zweck ist auch die Verarbeitung von Leistungs- und Verhaltensbewertungen zulässig, die andere Lehrkräfte getroffen haben.

(4) Bei der Verarbeitung personenbezogener Daten im Rahmen der Erstellung von sonderpädagogischen Gutachten sind besondere Maßnahmen zu treffen, um diese Daten gegen unberechtigten Zugriff zu schützen. Nach Erstellung der Gutachten sind diese auf Datenverarbeitungseinrichtungen der Schule auszudrucken und alle personenbezogenen Daten unverzüglich zu löschen.

(5) Bei der Verarbeitung der personenbezogenen Daten durch eine Lehrkraft bleibt die Schule die Daten verarbeitende Stelle im Sinne des Hessischen Datenschutzgesetzes und damit auch für die Datensicherheit verantwortlich.

(6) Die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungseinrichtungen kann einer Lehrkraft durch die Schulleiterin oder den Schulleiter untersagt werden, wenn ein Verstoß der Lehrkraft gegen eine Bestimmung dieser Verordnung oder des Hessischen Datenschutzgesetzes festgestellt wird.

Nähere Ausführungen mit konkreten technischen und organisatorischen Maßnahmen regelt ein Erlass des Kultusministeriums vom 21. August 2009 (ABl. 9/2009 S. 726). Damit ist der Schutz der personenbezogenen Daten am häuslichen Arbeitsplatz von Lehrkräften hinreichend sichergestellt. Es liegt in der Verantwortung der jeweiligen Lehrkraft, die verlangten Sicherheitsmaßnahmen auch tatsächlich einzuhalten. Nach außen hin, also gegenüber z. B. den betroffenen Schülern oder Eltern liegt die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung nicht bei der einzelnen Lehrkraft, sondern bei der Schule. Die Schule ist und bleibt Daten verarbeitende Stelle, auch wenn Daten am häuslichen Arbeitsplatz einer Lehrkraft verarbeitet werden (s. § 3 Abs. 5 der Verordnung).

Im Laufe des Berichtsjahres erreichten mich eine Reihe von Protestbriefen von Lehrkräften und von Lehrervertretungen. Stein des Anstoßes war die Erklärung in dem vom Ministerium vorgegebenen Formblatt zur Anmeldung des häuslichen Arbeitsplatzes. Die entsprechende Passage lautet:

Auszug aus dem Formblatt zur Anmeldung des häuslichen Arbeitsplatzes

Ich sichere zu, dem Hessischen Datenschutzbeauftragten die Wahrnehmung der Kontrollaufgaben in meinem häuslichen Bereich zu ermöglichen. Ich verpflichte mich, dem/der Beauftragten des HDSB nach vorheriger Terminvereinbarung Zugang zu der häuslichen Arbeitsstätte zu gewähren, um die Einhaltung der gebotenen Maßnahmen zur Gewährleistung der IT-Sicherheit und des Datenschutzes zu überprüfen. Diese Zusicherung gilt auch für alle erwachsenen Mitbewohner meines Haushaltes.

Der Text ist nahezu wortgleich mit dem Text in der Verordnung (§ 3 Abs. 1 Nr. 3). Die Lehrkräfte befürchteten, meine Mitarbeiter würden nun ihre Wohnungen durchsuchen oder die Datenverarbeitungsanlagen von Mitbewohnern oder Familienangehörigen kontrollieren.

Ich habe den Anfragenden mitgeteilt, dass sie verpflichtet sind, die Anzeige wie vorgesehen zu erstatten, wenn sie personenbezogene Schüler- und Schuldaten auf ihren privaten Datenverarbeitungsanlagen zu Hause verarbeiten möchten. Ansonsten müssen sie damit rechnen, dass die Schulleitung entsprechend § 3 Abs. 5 der Verordnung diese Verarbeitung der Daten am häuslichen Arbeitsplatz verbietet. Die geäußerten Befürchtungen sind unbegründet. Es ist weder vorgesehen, die Wohnung von Lehrern zu durchsuchen noch die Rechner ihrer Familienangehörigen zu sichten.

Nach § 29 Abs. 1 HDSG sind alle Daten verarbeitenden Stellen in Hessen verpflichtet, mich bei der Erfüllung meiner Aufgaben zu unterstützen. Mir ist dabei insbesondere Einsicht in alle Unterlagen und Zutritt zu allen Diensträumen zu gewähren. Das gilt für Rechenzentren, Polizeibehörden, Krankenhäuser und Justizvollzugsanstalten ebenso wie für alle Schulen. Es versteht sich von selbst, dass es sich um die Verarbeitung personenbezogener Daten für diese Stellen handeln muss. Dies ist ein unabdingbares Kontrollrecht, bei dem nicht derjenige der kontrolliert wird, sondern derjenige, der die Kontrolle vornimmt, den Kontrollgegenstand und -umfang definiert.

Lässt es eine Behörde zu, dass Daten außerhalb ihres Hoheitsbereichs verarbeitet werden, so muss sie sicherstellen, dass eine Datenschutzkontrolle faktisch möglich ist; z. B. muss sie bei

der Beauftragung privater Firmen diese verpflichten, sich meiner Kontrolle zu unterwerfen (§ 4 HDSG). Wegen des Grundrechts der Unverletzlichkeit der Wohnung entsteht ein rechtliches Problem, wenn ein Angehöriger der Dienststelle Daten nicht im räumlichen Bereich der Dienststelle, sondern in seiner privaten Wohnung verarbeitet. Soll dann eine Datenschutzkontrolle stattfinden, so ist es oft nicht zu vermeiden, auch die privaten Räume der Lehrkraft zu betreten. Deshalb muss vorher sichergestellt werden, dass der Bedienstete in diesem Fall dem Kontrolleur Einlass in die Wohnung gewährt. Das Grundrecht der Unverletzlichkeit der Wohnung kann also insoweit durch Einwilligung des Rechteinhabers Einschränkungen erfahren. Die Gewährung der Möglichkeit nicht nur in der Dienststelle, sondern auch zu Hause seinen Dienst zu verrichten, darf jedenfalls nicht dazu führen, dass ein kontrollfreier Bereich entsteht. Es geht – wie immer bei einer Kontrolle – um die Prüfung der Einhaltung gesetzlicher Erfordernisse; mit Misstrauen oder mangelndem Vertrauen hat dies nichts zu tun.

Die Erklärung ist ganz bewusst auf den Zweck beschränkt „die Einhaltung der gebotenen Maßnahmen zur Gewährleistung der IT-Sicherheit und des Datenschutzes zu überprüfen". Außerdem ist eine Terminabsprache zugesichert. Je nachdem, was kontrolliert werden soll, kann es im Einzelfall ausreichen, den PC in die Schule zu transportieren. Ist aber bspw. einem entsprechenden Vorhalt nachzugehen, der PC auf dem die Daten von Schülern verarbeitet werden, stünde im Gästezimmer der Wohnung des Lehrers auch Besuchern der Familie zur Verfügung, so muss auch vor Ort nachgesehen werden und so die Einhaltung der Datensicherheitsmaßnahmen in Augenschein genommen werden können. In diesem Falle darf die Kontrolle nicht an der Haustür der Lehrkraft enden. Da bei einer Kontrolle in der Wohnung auch das Grundrecht der Mitbewohner betroffen sein kann, bezieht die Erklärung auch diese ein. Sollte die Lehrkraft z. B. in einer Wohngemeinschaft oder zur Untermiete wohnen, soll die Kontrolle nicht deshalb "an der Haustür" abgebrochen werden müssen, weil ein Mitbewohner auf sein Grundrecht der Unverletzlichkeit der Wohnung pocht. Deshalb sind diese Fragen vor der Aufnahme der häuslichen Datenverarbeitung zu klären. Rechner von Haushaltsangehörigen oder private Zweitrechner der Lehrkraft sind nicht Gegenstand der Prüfung. Zwar könnte in die Formulierung der Erklärung auch dieses hineininterpretiert werden. Der Text einer solchen Erklärung kann aber ohnehin nicht alle denkbaren Eventualitäten abdecken. Um dem auch nur nahezukommen, müsste sie seitenlange Ausführungen umfassen. Darauf wurde bewusst verzichtet; die Formulierung orientiert sich stattdessen an der Erklärung für Telearbeitsplatzinhaber. Alle Telearbeitsplatzinhaber hessischer Behörden müssen zusichern, dass sie sowohl Vertreter der Dienststelle wie auch des Datenschutzbeauftragten in die Wohnung lassen. Es handelt sich hierbei keineswegs um eine hessische Besonderheit. Auch in anderen Bundesländern und auf Bundesebene wird

ähnlich verfahren. Das Grundrecht auf Unverletzlichkeit der Wohnung muss im Sinne einer praktischen Konkordanz, von der Person, welche die Datenschutzkontrolle vornimmt so weit als möglich geachtet werden. Die Entscheidung, wie weit dabei im Einzelfall genau gegangen wird, ist gerichtlich überprüfbar.

4.5.4
Beratung von Schulträgern bei der Einführung von Informationstechnik

Mit der Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen aus dem Jahr 2009 sind auch die Schulträger, die ihren Schulen zentrale Dienstleistungen im IT-Bereich erbringen, mit neuen Fragestellungen konfrontiert worden. Einige Schulträger haben mich deswegen bei der Neugestaltung ihrer technischen Konzepte um eine enge datenschutzrechtliche Beratung gebeten und Einzelheiten ihrer technischen und organisatorischen Lösungen sehr intensiv mit mir diskutiert. Dabei sind in Detailfragen zum Teil beachtliche Fortschritte erzielt worden.

4.5.4.1
Ausgangslage

Zu der Wirkung der Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen vom 4. Februar 2009 (ABl. 2009 S. 131) hatte ich bereits in meinem 38. Tätigkeitsbericht, Ziff. 4.5 und in der Broschüre „Datenschutz in Schulen“ detaillierte Ausführungen gemacht. Im Berichtszeitraum haben mich einige Schulträger um Beratung gebeten, damit sie bei der Entwicklung von Detailfragen ihrer Netzkonzepte alle datenschutzrechtlichen Fragestellungen schon frühzeitig berücksichtigen und Fehlentwicklungen vermeiden können.

Da die Ausgangslagen der Schulträger sowohl hinsichtlich der technischen Ausstattung als auch unter den Aspekten des möglichen Personal- und Sachmitteleinsatzes sehr verschieden sind und darüber hinaus sehr stark von der jeweiligen geografisch bestimmten Netzstruktur abhängen, entwickeln die Schulträger durchaus unterschiedliche Ansätze, um jeweils „ihre Lösung“ zu finden. Bei meiner Beurteilung und Begleitung der vorgelegten Lösungskonzepte habe ich unabhängig vom gewählten Weg feststellen können, dass die um Beratung nachsuchenden Schulträger sehr umfassend bemüht sind, die Umsetzung der neuen

Erlasslage, das Schulgesetz und die datenschutzrechtlichen Vorgaben in ihren Konzepten vollständig zu berücksichtigen.

Einige nach den vorliegenden Erkenntnissen besonders gelungene Lösungen will ich an dieser Stelle als positive Beispiele – gerade auch für die Schulträger, die ihre Konzepte noch entwickeln – skizzieren.

4.5.4.2
Vorbildliches Gesamtkonzept des Main-Kinzig-Kreises

Der Main-Kinzig-Kreis hat mir bereits im vergangenen Jahr ein Gesamtkonzept vorgelegt, dem ich nach nur einem Abstimmungsgespräch uneingeschränkt zustimmen konnte.
Die Umsetzung wurde im Jahr 2010 fast vollständig abgeschlossen und die Schulen des Kreises sind im Bereich der Verwaltung mit einheitlicher Technik ausgestattet.

Die in der Kreisverwaltung vorhandene Infrastruktur erlaubte es der zuständigen Fachverwaltung einen Lösungsansatz zu wählen, bei dem jede Schule über ein geschlossenes Netzwerksegment mit eigenem VLAN-Bereich an die Kreisverwaltung angeschlossen ist und am Standard-Arbeitsplatz weder ein Betriebssystem und die Anwendungssoftware noch die Daten vorgehalten werden müssen. Über die modernen Systeme ist es möglich, dass ein sog. Thin Client ohne eigene Festplatten sich das notwendige Betriebssystem aus dem Netz lädt. Die Anwendungen werden im Wesentlichen auf den Servern des Kreises betrieben und dem Benutzer über eine Terminalserver-Emulation zur Verfügung gestellt.

Je nach Schultyp und -größe wird zusätzlich mindestens ein vollwertiger Rechner mit verschlüsselten Festplatten als Datenaustauschstation und für bestimmte erweiterte Funktionen in den Schulen eingesetzt. Mit diesen Geräten können darüber hinaus bei einem Netzwerkausfall auch wichtige Aufgabenstellungen, wie z. B. die Vertretungsplanung, sichergestellt werden.

Insgesamt deckt das Konzept neben allen rechtlichen Vorgaben die Forderungen meines Eckpunktepapiers
„DV-Dienstleistungen für Schulen durch Schulträger und deren Auftragnehmer (Stand: 22. August 2008)“ ab:

– Trennung der Netze durch VLAN und den Einsatz von Firewalls,
– Schutz der Daten bei Gerätediebstahl durch eine zentrale Datenhaltung bzw. eine Verschlüsselung bei lokaler
  Speicherung,
– Umsetzung eines tagesaktuellen Virenschutzes,
– Kontrolle externer USB-Geräte durch den Einsatz einer entsprechenden Software,
– Einführung einer sicheren plattformbasierten Lösung für den häuslichen Arbeitsplatz (s. Ziff. 4.5.4.3),
– Zwischen dem Schulträger und den kreiseigenen Schulen wurden die Leistungen und wechselseitigen Verpflichtungen verbindlich geregelt.
– Der Schulträger hat ein Verfahren vorgesehen (s. Ziff. 4.5.4.4), das die notwendige Transparenz und Revisionssicherheit bei der Administration der Schulverwaltungsrechner bzw. Daten sicherstellt.

4.5.4.3
Plattformbasierte Zugriffe auf die Daten der Schulverwaltung am Heimarbeitsplatz

Die beschriebene Terminalserver-Lösung für die Verwaltungsarbeitsplätze macht sich der Schulträger auch bei der Gestaltung der Heimarbeitsplätze zunutze. Für die Einrichtung eines häuslichen Arbeitsplatzes ist nur die Installation eines Software-Clients auf dem Rechner erforderlich. Die Verbindung wird über einen verschlüsselten Zugriff (SSL) auf die Terminalserver-Plattform des Kreises hergestellt und zur Authentisierung der Benutzer wird zusätzlich zu dem verwendeten Passwort ein Token nach dem OTP-Standard eingesetzt. Da eine Anmeldung an den Servern der Kreisverwaltung über das Internet ohne das durch den Token generierte Einmal-Passwort nicht möglich ist, sind unbefugte Zugriffe auf diesem Weg sicher ausgeschlossen. Dennoch besteht auch bei dieser Konstellation für den Benutzer des Heimarbeitsplatzes die Verpflichtung, durch einen aktuellen Virenschutz sein System gegen Angriffe zu schützen und die anderen Vorgaben zum häuslichen Arbeitsplatz (s. Ziff. 4.5.3) zu erfüllen.

Eine Übertragung der Daten auf das lokale System am Heimarbeitsplatz wird durch entsprechende Einstellungen an den zentralen Systemen ausgeschlossen. Damit wird eines meiner wesentlichen Anliegen erfüllt, dass die Daten, die im Rahmen des § 3 Abs. 2 der Verordnung und deren Anlage 1, Ziff. 6 am häuslichen Arbeitsplatz verarbeitet werden, nicht durch technische Fehler oder ein Versehen des Benutzers auf das lokale System übertragen

werden und dort zu einem späteren Zeitpunkt unbefugten Personen zugänglich sind. Auch der Ausdruck von Unterlagen ist nur an den zugewiesenen Druckern in der Schule möglich, die entweder in nicht allgemein zugänglichen Bereichen der Schulverwaltung stehen müssen oder bei denen die Funktion „vertrauliches Drucken“ – der Druck kann dadurch an den Geräten erst nach Eingabe einer PIN erfolgen – genutzt wird. Im Ergebnis ist in jedem Fall sichergestellt, dass die Ausdrucke nicht in unbefugte Hände gelangen.

Anlage 1 Ziff. 6.1 bis 6.13 Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen

6. Datensatz bei der Verarbeitung personenbezogener Schülerdaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte

6.1 Name einschließlich Geburtsname,
6.2 Vorname,
6.3 Geschlecht,
6.4 Geburtsdatum,
6.5 Klasse/Jahrgangsstufe, Kurs,
6.6 Schüleraktenzeichen und Gesamtschülerverzeichnis,
6.7 LUSD-ID der Schülerin oder des Schülers,
6.8 Unterrichtsfächer,
6.9 Bildungsgang, Ausbildungsrichtung/Ausbildungsberuf, gegebenenfalls Schwerpunkt,
6.10 Fächer, in denen die Lehrkraft Schülerinnen und Schüler unterrichtet,
6.11 selbst erteilte Zeugnisnoten und Ergebnisse und Teilergebnisse schriftlicher, mündlicher und praktischer Leistungsüberprüfungen sowie Verhaltensbewertungen in dem von der Lehrkraft erteilten Unterricht sowie Art und Datum der Leistungserhebung beziehungsweise der Bewertung,
6.12 Zeiten des Fernbleibens vom Unterricht in den Fächern, in denen die Lehrkraft die Schülerinnen und Schüler unterrichtet,
6.13 Mitglieder der Schulleitung, gegebenenfalls weitere mit Leitungsaufgaben betraute Lehrkräfte und Klassenlehrer dürfen soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, darüber hinaus die folgenden Schülerdaten verarbeiten:
6.13.1 Halbjahresnoten in allen Fächern der betreffenden Schülerinnen und Schüler,
6.13.2 alle zeugnisrelevanten Leistungsangaben,
6.13.3 zeugnisübliche Bemerkungen,
6.13.4 Telefonnummer, Telefaxnummer und E-Mail-Adresse der Schülerinnen und Schüler sowie deren Eltern, sofern der Erhebung nicht widersprochen wird

In einem weiteren Schritt beabsichtigt der Main-Kinzig-Kreis eine geeignete, für die Verarbeitung der sonderpädagogischen Gutachten unerlässliche Verschlüsselung einzuführen. Wenn sich hier eine geeignete Lösung findet, lassen sich auch diese besonders zu schützenden Daten im Rahmen der rechtlichen Vorgaben an den häuslichen Arbeitsplätzen verarbeiten.

Anlage 1 Ziff. 6.14 Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen in Schulen

6. Datensatz bei der Verarbeitung personenbezogener Schülerdaten auf privaten Datenverarbeitungseinrichtungen der Lehrkräfte

...

6.14 Förderschullehrkräfte und Berufsschullehrkräfte mit sonderpädagogischer Zusatzausbildung dürfen zur Erstellung von sonderpädagogischen Gutachten außerdem folgende personenbezogene Daten verarbeiten:

6.14.1 zur Anamnese der Schülerin oder des Schülers in ihrer oder seiner Familie,

6.14.2 zu den Entwicklungsbedingungen der Lernumwelt,

6.14.3 zu Faktoren und Merkmalen hinsichtlich der Vorgeschichte,

6.14.4 zu Lernvoraussetzungen und den individuellen Fähigkeiten in ihrem Zusammenhang mit der aktuellen Lernsituation,

6.14.5 zum Lernverhalten,

6.14.6 zur sprachlichen Entwicklung,

6.14.7 zur körperlichen und motorischen Entwicklung,

6.14.8 zum emotionalen und sozialen Verhalten,

6.14.9 zur kognitiven Entwicklung,

6.14.10 zur Handlungsfähigkeit in Situationen der täglichen Erfahrung,

6.14.11 zu zusammenfassenden Beurteilungen,

6.14.12 zu Förderempfehlungen und zu Hinweisen für den zu entwickelnden Förderplan.

4.5.4.4
Revisionssichere Protokollierung

Die vollständige Protokollierung beim Betrieb von IT-Systemen umfasst unter dem datenschutzrechtlichen Blickwinkel alle automatisierten und ggf. manuellen Aufzeichnungen, die dazu geeignet sind festzustellen, wer wann mit welchen Mitteln auf Daten zugegriffen hat.

Ergänzend dazu kann mit den Protokollen und Dokumentationen nachvollzogen werden, wer wann über welche Berechtigung in den Systemen verfügte und ob diese Berechtigungen den in diesen Zeiträumen vorgegebenen Aufgabenstellungen entsprachen. Leider werden die automatisierten Protokolle in Standardsystemen oft nicht manipulationssicher erzeugt und abgelegt. Ein höheres Maß an Revisionssicherheit ist nur durch den Einsatz von speziellen Software-Paketen zu erreichen, die die anfallenden Protokolle schützen und sicher ablegen sowie alle dazu notwendigen Prozesse überwachen (s. 38. Tätigkeitsbericht, Ziff. 10.1).

In der Prüf- und Beratungspraxis der vergangenen Jahre wurde ich vereinzelt gebeten, den Inhalt und die Integrität von Protokolldaten zu bewerten. In aller Regel waren im Vorfeld in einer Daten verarbeitenden Stelle vertrauliche Informationen aus Schriftstücken, Patientendatensätzen oder nicht öffentlichen Sitzungen bzw. deren Protokollen, bekannt geworden und es galt festzustellen, ob mit den Zugriffsprotokollen der IT-Systeme unbefugte Zugriffe nachzuweisen wären.

Leider war in fast allen Fällen ein sicherer, möglicherweise gerichtlich verwertbarer Nachweis nicht zu führen, da die Protokollierung einerseits oft nur unvollständig aktiviert war und andererseits die anfallenden Protokolle nicht hinreichend gegen Veränderungen geschützt wurden. Auch um die in solchen Situationen automatisch in den Kreis der Verdächtigen geratenen Administratoren zu schützen, ist es notwendig, mit speziellen Systemen die anfallenden Protokolle und die beteiligten Prozesse zu schützen bzw. zu überwachen.

Für den Main-Kinzig-Kreis war es neben diesen grundsätzlichen Überlegungen wichtig, die Administrationsarbeiten für die kreiseigenen Schulen revisionssicher und mit einer verbesserten Auswertbarkeit nachweisen zu können. Daher hat der Kreis ein Projekt auf den Weg gebracht, bei dem durch den Einsatz eines entsprechenden Systems alle sicherheitsrelevanten Vorgänge in der IT der Kreisverwaltung auf separaten Servern abgelegt werden.

Das nahezu fertig entwickelte Konzept steht vor seiner Umsetzung. Allerdings müssen die Fragen der Rollenverteilung bei der Überwachung der kritischen Prozesse noch mit der Personalvertretung abgestimmt und durch die zuständigen Gremien der Kreisverwaltung beschlossen werden. Wegen der übergreifenden Bedeutung für alle IT-Bereiche der Kommunal- und Landesverwaltung werde ich die Projektumsetzung im Laufe des Jahres 2011 weiter begleiten und erneut dazu berichten.

4.5.4.5
Mustersicherheitskonzept für die Schulen im Kreis Groß-Gerau

Im Wege der Beratungsgespräche zu den Konzepten des Kreises Groß-Gerau hat die zuständige Fachverwaltung besonderen Wert darauf gelegt, dass die Umsetzung in den Schulen die notwendige Akzeptanz erfährt und entsprechend mitgetragen wird. In diesem Zusammenhang wurde im Lauf des Jahres neben einer Sicherheitsrichtlinie zur IT-Nutzung, in der verbindliche Rahmenbedingungen zwischen Schulträger und Schulen verabredet werden, auch der Entwurf eines Mustersicherheitskonzeptes für die Schulen erarbeitet.

Alle staatlichen Schulen in Hessen sind durch den Erlass über IT-Sicherheit und Datenschutz in Schulverwaltungen des Hessischen Kultusministeriums vom 27. November 2009 (ABl. 2010 S. 11) im Zusammenhang mit § 10 HDSG dazu verpflichtet, ein Sicherheitskonzept zu erstellen, sehen sich aber dabei in aller Regel vor einer Aufgabe, die sie ohne die Unterstützung ihres Schulträgers nicht bewältigen können. Ich unterstütze daher alle Ansätze, bei denen der Schulträger mit seinen kreiseigenen bzw. städtischen Schulen ein Musterkonzept entwickelt und dabei alle Punkte abdeckt, für die er, als der zentrale „Dienstleister“, die fachliche Verantwortung trägt.

Im jüngsten, mir vorliegenden Entwurf des IT-Sicherheitskonzeptes des Kreises Groß-Gerau sind neben zentralen Vorgaben zur allgemeinen Systemnutzung und zum Grundschutz auch solche zum Netzmanagement, zur Datenhaltung/Sicherung, zum Virenschutz usw. enthalten. Die Schulen müssen dann bspw. noch die folgenden schulspezifischen Details ergänzen:

- Zutrittskontrolle zu Gebäuden und Räumen
- Schlüsselvergabe
- Aufbewahrung/Lagerung von Schülerakten
- Aufbewahrung externer Datenträger
- Datensicherung lokaler Systeme
- lokale Entsorgung von Akten und Datenträgern

Der Kreis Groß-Gerau hat damit die Voraussetzungen geschaffen, dass die kreiseigenen Schulen im Laufe des nächsten Jahres flächendeckend ihre Sicherheitskonzepte erstellen können. Zusätzlich beabsichtigt die zuständige Fachverwaltung ein erweitertes Sicherheitskonzept für die eigenen Zwecke zu erstellen, das den Schulleitungen zur Klärung von Detailfragen zur Einsicht vorgelegt werden kann. Sicherheitsrelevante Einzelheiten sind

den Verantwortlichen in den Schulen auf diese Weise zugänglich, müssen aber nicht in die Konzepte der einzelnen Schulen übernommen werden.

4.6 Wissenschaft und Forschung

4.6.1
Datenschutzkonzept für die Nationale Kohorte

Verschiedene Universitäten und andere nationale Forschungseinrichtungen wollen im Rahmen einer großen Langzeitstudie die Ursachen von chronischen Krankheiten erforschen. Geplant ist eine Nationale Kohorte mit 200.000 Studienteilnehmern aus verschiedenen Regionen Deutschlands. Unter dem Vorsitz meiner Dienststelle ist im Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder mit Vertretern des Epidemiologischen Planungskomitees das Datenschutzkonzept für die Studie diskutiert worden. Ein endgültiges Datenschutzkonzept liegt noch nicht vor.

4.6.1.1
Inhalt der Langzeitstudie

Vor dem Hintergrund zunehmender chronischer Krankheiten werden neue Strategien für die Risikoerfassung, Früherkennung und Vorsorge wichtiger und weitverbreiteter Erkrankungen wie z. B. Diabetes, Herz-Kreislauf-Erkrankungen, Infektionen und Krebs, angestrebt. Dieses Vorhaben wird nun zusammen mit Universitäten und anderen nationalen Forschungseinrichtungen entwickelt. Geplant ist, eine Nationale Kohorte mit 200.000 Studienteilnehmern – Männern und Frauen im Alter von 20 bis 69 Jahren aus verschiedenen Regionen Deutschlands – aufzubauen. Die Studienteilnehmer werden mit Hilfe eines Zufallverfahrens aus dem Einwohnermeldewesen ausgewählt und um ihre Teilnahme gebeten.

Von allen Studienteilnehmern sollen mittels Fragebögen umfangreiche Informationen zu ihrer Krankengeschichte, der Krankengeschichte ihrer Familie, zu psychosozialen Faktoren und zum Lebensstil (z. B. körperlicher Aktivität, Ernährung und Rauchen) erhoben werden. Darüber hinaus ist beabsichtigt, bei allen Studienteilnehmern verschiedene medizinische Untersuchungen durchzuführen (z. B. Messung von Größe, Gewicht, Blutdruck) und Blut-, Speichel- und Urinproben zu sammeln. Diese Proben sollen für spätere Forschungsprojekte in einem zentralen Bioprobenlager am Helmholtzzentrum München aufbewahrt werden. Für eine große Untergruppe innerhalb der Kohorte von ca. 40.000 Männern und Frauen ist eine detailliertere Datenerhebung vorgesehen, die auch medizinische Untersuchungen umfassen wird. Nach dem derzeitigen Zeitplan soll ab 2012 für fünf Jahre die Rekrutierung der

Teilnehmer an der Nationalen Kohorte stattfinden. Alle erhobenen Daten sollen pseudonymisiert in einer zentralen Datenbank gespeichert werden. In regelmäßigen Abständen sind erneute schriftliche Befragungen bzw. Untersuchungen der Studienteilnehmer geplant. Darüber hinaus sollen weitere Informationen über die Studienteilnehmer aus bereits vorhandenen Krankenakten, medizinischen Registern (z. B. Krebsregistern) sowie Renten- und Sozialversicherungsakten in die Langzeitstudie einbezogen werden. Die Daten und Proben sollen zu Zwecken der medizinischen Forschung langfristig gespeichert und gelagert werden. Auch genetische Analysen sind geplant, um erbliche Risikofaktoren auf chronische Erkrankungen zu ermitteln.

4.6.1.2
Datenschutzrechtliche Diskussionspunkte

Mit den Vertretern des Planungskomitees wurden im Arbeitskreis Wissenschaft eine Reihe datenschutzrechtlicher Gesichtspunkte diskutiert, die künftig bei einer Konkretisierung des Datenschutzkonzepts berücksichtigt werden sollten:

4.6.1.2.1
Aufteilung der Aufgaben/Verantwortlichkeiten

An der Langzeitstudie sind zahlreiche Stellen beteiligt, insbesondere
- ca. 19 Rekrutierungszentren,
- zwei Integrationszentren, die die zentrale Datenbank vorhalten (aus Sicherheitsgründen wird die zentrale Datenbank sowohl beim DKFZ Heidelberg wie auch bei der Universität Greifswald gespeichert),
- verschiedene fachspezifische Kompetenzzentren (z. B. für die Befundung von Bildserien),
- eine Treuhandstelle, die u. a. die personenbezogenen Daten und die ihnen zugeordneten Pseudonyme speichert,
- ein Transferzentrum, über das auf Antrag pseudonymisierte Daten an externe Forschungseinrichtungen weitergegeben werden, sowie
- eine zentrale Biobank

Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, dass die Aufteilung der Verantwortlichkeit für die Verarbeitung der Daten klar festgelegt ist. Insbesondere muss geklärt sein, welche Stelle in eigener Verantwortung Daten verarbeitet, und welche Stelle im

Auftrag von einer anderen Stelle Daten verarbeitet, ferner, wer für welche technisch-organisatorischen Datensicherheitsmaßnahmen im Rahmen der Studie verantwortlich ist. Darüber hinaus muss klar vereinbart sein, wer Eigentümer der Bioproben ist und zu welchen Zwecken die Proben insgesamt verwendet werden dürfen.

4.6.1.2.2
Pseudonymisierungsverfahren

Im Rahmen der Studie sollen die Daten der Studienteilnehmer überwiegend pseudonymisiert verarbeitet werden, insbesondere auch in der zentralen Datenbank und der zentralen Bioprobenbank. Ein zentraler Punkt ist die Frage, wie ein Reidentifizierungsrisiko für die Teilnehmer weitestgehend verhindert werden kann. Ein solches Risiko kann sich zum einen aus dem Verfahren der Pseudonymbildung ergeben, zum anderen aus dem Inhalt/ Umfang des unter dem Pseudonym gespeicherten Datensatzes (hier z. B. aus der Geolokalisierung von Wohn- und Arbeitsstätte und seltenen Erkrankungen oder Krankheitsverläufen).

Wenn die o. a. Gesichtspunkte im Konzept konkretisiert sind, müssen die Verantwortlichkeiten und Verfahrensweisen in den Text der Teilnehmerinformation und der Teilnehmereinwilligung aufgenommen werden. Da die Studie über einen sehr langen Zeitraum laufen soll, ist es auch wichtig, die Konsequenzen des Widerrufs eines Teilnehmers im Detail festzulegen.

Die Vertreter des Planungskomitees sagten zu, die diskutierten datenschutzrechtlichen Gesichtspunkte in der aktualisierten Fassung des Konzepts zu berücksichtigen.

4.6.2
Zentrale Datenbank für die Erforschung von Lungenerkrankungen

Im Rahmen des Kompetenznetzes Asthma und COPD (chronisch-obstruktive Lungenerkrankung) haben sich führende Lungenfachzentren in Deutschland zu dem Verbund COSYCONET zusammengeschlossen, um eine zentrale Patientendatenbank aufzubauen und den Verlauf der COPD genauer zu erforschen. Es wurde ein Datenschutzkonzept für das Projekt 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 Bestandteil der Patienteninformationen.

4.6.2.1
Ziele des Kompetenznetzes Asthma und COPD und des Verbundes COSYCONET

Das vom Bundesministerium für Bildung und Forschung geförderte Kompetenznetz Asthma und COPD ist ein Zusammenschluss verschiedener Forschungseinrichtungen, Universitätskliniken und Studienzentren, die sich zum Ziel gesetzt haben, Fortschritte bzgl. der Prävention, Diagnostik und Therapie zu erzielen (http://www.gesundheitsforschung-bmbf.de/de/2170.php). Um diese Ziele zu erreichen, werden im Rahmen des Kompetenznetzes verschiedene Projekte durchgeführt. Die COSYCONET-Kohorten-Studie ist ein Teilprojekt des Kompetenznetzes. Es ist „ein nationales Netzwerk zur Untersuchung systemischer Manifestationen und Komorbiditäten bei Patienten mit COPD“. Die Studienleitung hat das Universitätsklinikum Gießen und Marburg, Standort Marburg. Bundesweit sollen von Fachärzten bzw. Studienzentren Patientendaten, -bilder und -proben auf der Basis einer Einwilligung des Patienten erhoben und zentral bei verschiedenen Kooperationspartnern gespeichert werden; d. h. Bestandteil der Studie ist

– eine zentrale Datenbank, die an der Medizinischen Hochschule Hannover aufgebaut wird,
– eine zentrale Biobank, die an der Universität des Saarlandes aufgebaut wird, sowie
– eine Bildbank, die an der Universität Heidelberg aufgebaut wird.

4.6.2.2
Datenschutzkonzept für den Verbund COSYCONET

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, www.tmf-ev.de). Die Daten werden in den Studienzentren personenbezogen erhoben und gespeichert. Außerhalb des Bereichs der Studienzentren werden nahezu ausschließlich pseudonymisierte Patientendaten verarbeitet. Lediglich für die 1. Generierung des Pseudonyms eines neuen Patienten durch den Pseudonymisierungsdienstbetreiber werden die personenbezogenen Daten kurzfristig verwendet, sie werden jedoch nicht gespeichert. Sowohl in der Datenbank in Hannover als auch in der Biomaterialbank in Saarbrücken und in der Bilddatenbank in Heidelberg wird ausschließlich mit pseudonymisierten Daten gearbeitet. Die Ergebnisse der in Saarbrücken durchgeführten Blutanalysen und der in Heidelberg

durchgeführten Bildanalysen werden an die zentrale Datenbank in Hannover gesendet und dort anhand des Pseudonyms zugeordnet. Der Pseudonymisierungsdienst wird von einer von der Medizinischen Hochschule Hannover unabhängigen selbstständigen weiteren Stelle betrieben. Über die Weitergabe von Daten oder Proben an Wissenschaftler innerhalb und außerhalb des Kompetenznetzes Asthma und COPD entscheidet der Führungskreis des Kompetenznetzes. Die Medizinische Hochschule Hannover ist dafür verantwortlich, dass die Daten nur entsprechend der Genehmigung durch den Führungskreis an die antragstellenden Wissenschaftler herausgegeben werden. Für die Bioproben gilt dies entsprechend. Bestandteil des Genehmigungsverfahrens ist u. a. die Sicherstellung, dass durch die Weitergabe der vom Forscher beantragten Daten kein Reidentifizierungsrisiko für die betroffenen Patienten entsteht. Soweit notwendig muss der Datensatz eingeschränkt oder verändert werden.

Die Patienten erhalten bei der Rekrutierung beim niedergelassenen Pneumologen eine erste Patienteninformation über die Studie. Die eigentliche Aufklärung findet im Studienzentrum statt. Dort erhält der Patient eine ausführliche Patienteninformation sowie eine Einwilligungserklärung zur Teilnahme an der Studie. Die Nutzungs- und Eigentumsrechte der Bioproben werden in einem Probenentnahmevertrag zwischen dem Patienten und der Biomaterialbank geregelt. Da es sich bei genetischen Analysen um besonders sensible Daten handelt, erhalten die Patienten für die genetische Analyse eine gesonderte Patienteninformation und Einwilligungserklärung.

4.6.2.3
Diskutierte datenschutzrechtliche Aspekte

Da an COSYCONET verschiedene selbstständige Kooperationspartner in verschiedenen Bundesländern beteiligt sind, habe ich die datenschutzrechtliche Beratung mit allen für die Studie zuständigen Landesdatenschutzbeauftragten koordiniert. Das vom Verbund vorgelegte Datenschutzkonzept hat sich an den datenschutzgerechten Modellen der TMF orientiert. Es waren noch Details klärungsbedürftig:

– **Aufteilung der Verantwortlichkeiten zwischen den Kooperationspartnern**
  Nicht eindeutig geklärt war zu Beginn der Gespräche, welche Stelle in welchem Umfang für die Gewährleistung von Datenschutz und Datensicherheit verantwortlich ist und wie Entscheidungen des Verbundes verbindlich werden.
  Geklärt ist nunmehr, dass der Führungskreis des Kompetenznetzes Asthma und COPD verantwortlich ist für das Netzübergreifende IT-Sicherheitskonzept und er auch über

Maßnahmen entscheidet, die ergriffen werden sollen. Die Kooperationspartner verpflichten sich schriftlich, die Entscheidungen des Führungskreises umzusetzen. Der Führungskreis bestimmt ebenfalls – auf Antrag von Wissenschaftlern – welche Daten und Proben in welcher Form herausgegeben werden und leitet dies in die Wege. Auch in diesem Punkt verpflichten sich die Kooperationspartner schriftlich, Daten und Proben nur nach den Vorgaben des Führungskreises herauszugeben. Entsprechendes gilt für alle weiteren alle Kooperationspartner betreffenden Fragen wie z. B. den Text der Patienteninformation und -einwilligung. Im Rahmen der Kooperation werden die Teilprojekte mit der Durchführung und Entwicklung von Konzepten zur Datenspeicherung und -sicherung beauftragt, die mit dem Führungskreis abgestimmt werden. Im Übrigen sind die Kooperationspartner für die Einhaltung der datenschutzrechtlichen Bestimmungen selbst verantwortlich.

– **Anlässe und Voraussetzungen für eine Depseudonymisierung der Patientendaten**
Die Studienzentren haben sowohl die personenbezogenen Daten der Patienten wie auch die Pseudonyme ihrer Patienten. Nur die Studienzentralen sind daher in der Lage, von einem Pseudonym wieder auf einen Patienten zu schließen. Klärungsbedürftig war, in welchen Fällen eine solche Depseudonymisierung von den Studienärzten vorgenommen werden darf und soll. Es bestand die Forderung der Datenschutzbeauftragten, diese Fälle konkret und abschließend verbindlich für den Verbund festzulegen und die Patienten hierüber auch in der Patienteninformation zu informieren. Dies ist inzwischen erfolgt. Eine Depseudonymisieierung erfolgt nur, wenn Patienten z. B. aufgrund bestimmter Merkmale zu einer weiteren Studie eingeladen werden sollen. Der Führungskreis entscheidet dies und lässt die Information den Patienten über den Studienarzt zukommen, denn nur dieser kann eine Depseudonymisierung vornehmen. Diese Patienten werden dann angeschrieben und um Einwilligung in die Teilnahme an der neuen Studie gebeten.

– **Klare Trennung zwischen Betrieb der Datenbank und Betrieb des Pseudonymisierungsdienstes**
Das IT-Sicherheitskonzept muss gewährleisten, dass nicht unberechtigt auf das Register zugegriffen werden kann. Geklärt sind nunmehr die folgenden Punkte:
  – Betreiber des Pseudonymisierungsdienstes und Betreiber der Datenbank sind voneinander unabhängige Stellen.
  – Nur der Pseudonymisierungsdienstleister verwahrt das Geheimnis, mit dem die Pseudonyme generiert werden. Es gibt keinen Grund, das Geheimnis anderen Stellen zugänglich zu machen. Der Betreiber des Pseudonymisierungsdienstes muss sich vertraglich verpflichten, das zur Generierung der Pseudonyme

verwendete „Geheimnis“ nicht an Dritte innerhalb oder außerhalb des Verbundes weiterzugeben. Er muss sich vertraglich verpflichten, das Geheimnis bei evtl. Vertragsende an seinen Vertragsnachfolger weiterzugeben.

– Die Pseudonymvergabe läuft im Prinzip wie folgt ab. Ein berechtigter Studienarzt beabsichtigt einen neuen Patienten in die Studie einzuschließen, wozu die Erstellung eines Pseudonyms erforderlich ist. Er meldet sich am Studienserver an und betätigt einen Button „Neues Pseudonym erstellen“ im Studienportal. Daraufhin baut der Browser eine neue, unabhängige Verbindung zum Pseudonymisierungs-Server auf mit der Anfrage, das notwendige Formular für die Eingabe von identifizierenden Daten bereitzustellen. Der Pseudonymisierungs-Server prüft über gesicherte Verbindungen beim Studienserver, ob der Studienarzt Patienten anlegen darf. Das Formular zur Eingabe der identifizierenden Daten wird bereitgestellt und der Studienarzt gibt die Daten ein. Die Daten werden SSL-verschlüsselt an den Pseudonymisierungs-Server geschickt. Dort wird das Pseudonym erstellt und vom Pseudonymisierungs-Server zusammen mit den identifizierenden Daten dem Studienarzt angezeigt. Der Studienarzt erhält die Möglichkeit, die Kombination von Pseudonym und identifizierenden Daten auszudrucken und zu der Patientenakte zu nehmen.

  An den Studienserver werden keinerlei Daten übertragen. Die identifizierenden Daten werden nur temporär zur Pseudonymerstellung auf dem Pseudonymisierungs-Server verwendet. Sie sind nach Beendigung des Prozesses gelöscht und sind außer im Ausdruck des Studienarztes nirgendwo gespeichert.

  Die zur Pseudonymbildung herangezogenen Daten sind teilweise gekürzt. Sie sind ausreichend trennscharf in Anbetracht der Zahl potenzieller Patienten, sind aber nicht dazu geeignet, eine Liste von Patienten zu erstellen.

– Es ist ausgeschlossen, dass der Betreiber der Datenbank – sei es auch nur kurzfristig – die personenbezogenen Daten der Patienten zur Kenntnis nehmen kann.

– **Zentrale Biomaterialbank**

  Verantwortliche Stelle ist das Universitätsklinikum Saarland. Die Probenentnahmeverträge werden in den Studienzentren unterschrieben und verbleiben dort. Das Universitätsklinikum Saarland hat ausschließlich pseudonymisierte Daten und Proben (spezielles Labor-Pseudonym).

– **Zentrale Bilddatenbank**

In der zentralen Bilddatenbank werden nur pseudonymisierte Daten verarbeitet. Die CT-Bilder werden nicht an Dritte versandt. Lediglich die Ergebnisse werden an die zentrale Datenbank übermittelt.

– **Weitere Datensicherheitsmaßnahmen**

Auf jedem der Server werden den Benutzern nur die erforderlichen Zugriffsrechte vergeben. Benutzerkennungen können nur Ärzte und Mitarbeiter von Institutionen erhalten, die an COSYCONET beteiligt sind. Ferner wird darauf geachtet, dass die Server technisch, räumlich und administrativ getrennt sind, d. h. es gibt insbesondere bei der Administration keine personellen Überschneidungen.

Als weitere Sicherheitsmaßnahmen werden alle Datenübertragungen verschlüsselt und die Server werden regelmäßig auf Sicherheitslücken überprüft, was Eindringversuche umfasst.

– **Wenn Daten an Forscher herausgegeben werden**, erfolgt dies in der Regel ohne Pseudonym. Falls ein Pseudonym benötigt wird, handelt es sich nicht um das in der zentralen Datenbank vorhandene Pseudonym, dieses wird durch ein „Exportpseudonym“ (z. B. eine Zufallszahl) ersetzt. Zur Vermeidung von Reidentifizierungsrisiken wird der Datensatz auch dahingehend überprüft, welche Daten tatsächlich für den Forschungszweck benötigt werden. Der herauszugebende Datensatz soll auf die für die Forschungsfrage notwendigen Variablen reduziert werden, ohne dass es zu einem Informationsverlust für die Forschungsfrage kommt. Insbesondere die demografischen Variablen werden daraufhin überprüft, ob sie zur Beantwortung der Fragestellung notwendig sind.

– **Löschung bzw. Anonymisierung von Daten und Proben**

Für die Speicherung und Aufbewahrung von Daten und Proben ist bisher keine Frist festgelegt, da das Kompetenznetz noch nicht weiß, wann die Studie beendet sein wird. Wenn ein Datensatz abgeschlossen ist, wird dieser aber anonymisiert. Nach einem Widerruf der Einwilligung können die Daten von teilnehmenden Patienten auf deren expliziten Wunsch hin aus der Datenbank gelöscht werden. Stimmt ein Patient zu, dass seine Daten noch für Forschungszwecke verwendet werden können, so werden seine Daten im gesamten Verbund anonymisiert. Darüber hinaus werden alle Patientendaten nach Abschluss der Studie anonymisiert. Die Anonymisierung wird wie folgt durchgeführt:

Jedes Pseudonym wird mit einer Zufallszahl überschrieben. Wenn dann noch Reidentifizierungsrisiken bestehen, müssen aus dem Datensatz diejenigen Daten entfernt werden, mittels derer die Möglichkeit einer Reidentifizierung der Patienten nicht ausgeschlossen scheint.

Alle hier aufgeführten Diskussionsergebnisse wurden von den Kooperationspartnern in einem Amendement zur Kooperationsvereinbarung und/oder in den Text der Patienteninformation und -einwilligung und den Probenentnahmevertrag aufgenommen.

4.6.3
Konzept für ein Nationales Mortalitätsregister

2009 hat der Rat für Sozial- und Wirtschaftsdaten eine Arbeitsgruppe einberufen, die ein Nationales Mortalitätsregister vorbereiten soll. Der aktuelle Stand der Überlegungen wurde von dieser Arbeitsgruppe unter dem Vorsitz meiner Dienststelle in dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erläutert und unter datenschutzrechtlichen Aspekten diskutiert. Der Dialog soll fortgesetzt werden.

4.6.3.1
Ziele eines Nationalen Mortalitätsregisters

Der Rat für Sozial- und Wirtschaftsdaten, ein unabhängiges Gremium von empirisch arbeitenden Wissenschaftlern aus Universitäten, Hochschulen und anderen Einrichtungen unabhängiger wissenschaftlicher Forschung sowie von Vertretern der wichtigsten öffentlichen Einrichtungen zur Datenerhebung (www.ratswd.de), hat eine Arbeitsgruppe „Mortalitätsregister“ eingesetzt, die ein Mortalitätsregister für Deutschland vorbereiten soll (http:// www.ratswd.de/Mortalitätsregister/index.php).

Gegenwärtig wird die vom Arzt ausgestellte Todesbescheinigung, die im „Vertraulichen Teil“ die Todesursache enthält, bei den Gesundheitsämtern gespeichert. Die Gesundheitsämter übermitteln die codierten Todesursachen an das Statistische Landesamt. Über die Statistischen Landesämter werden diese Daten Forschern in aggregierter Form zur Verfügung gestellt. Diese Forschungsmöglichkeiten werden von der Arbeitsgruppe Mortalitätsdaten als

nicht hinreichend bewertet. Sie sieht es vielmehr als Aufgabe des Nationalen Mortalitätsregisters an, personenbezogene Mortalitätsdaten für alle in Deutschland geborenen oder verstorbenen Personen zu erheben, für Forschungszwecke aufzubereiten und – soweit notwendig – für konkrete Forschungsvorhaben auch mit den Datenbeständen anderer Stellen (z. B. Rentenversicherungsträger, Krebsregister) abzugleichen.

Für ein Nationales Mortalitätsregister werden von der Arbeitsgruppe für alle in Deutschland geborenen oder verstorbenen Personen nach ihrem Tod mindestens folgende Informationen als notwendig angesehen:

– Name, Vornamen, (frühere Namen), Titel und Namenszusätze, letzte Adresse, Wohnort, PLZ;
– Geschlecht;
– Nationalität;
– Name und Nr. des beurkundenden Standesamtes, Sterbebuchnummer;
– Geburtsort;
– Geburtsdatum;
– Todesursachen (Grundleiden, Kausalkette, Nebendiagnosen) im Klartext und vercodet nach ICD;
– Datum der Leichenschau;
– Obduktion Datum, Ergebnisse als Klartext und als ICD-Codes;
– Angaben zu bestehender Schwangerschaft;
– Angaben für Kinder <1 Jahr oder Totgeborene;
– Angaben zu Unfällen;
– Elektronische Kopie des Originals der Todesbescheinigung.

Die Daten sollen nach Vorstellung der Arbeitsgruppe bundesweit zusammengeführt und dann auch bei Bedarf mit anderen Datenbeständen zu Forschungszwecken abgeglichen werden können. Die bisher schon etablierten Datenflüsse (insbesondere von den Gesundheitsämtern an die Statistischen Landesämter) sollen beibehalten und erweitert werden.

4.6.3.2
Datenschutzrechtliche Anforderungen

Wesentliche Fragen der möglichen Strukturen und Abläufe in einem evtl. Nationalen Mortalitätsregister sind noch klärungsbedürftig. Insbesondere auch wer speichernde Stelle ist,

welche Stellen die o. a. Daten an das Register melden und welche Stellen unter welchen Voraussetzungen personenbezogene/pseudonymisierte und/oder anonymisierte Daten über die Verstorbenen für Forschungszwecke erhalten. In der Sitzung des Arbeitskreises Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde mit Vertretern der Arbeitsgruppe über die Frage der Erforderlichkeit eines Nationalen Mortalitätsregisters und evtl. datenschutzgerechte Ausgestaltungsmöglichkeiten diskutiert. Wenn die derzeitigen Forschungsmöglichkeiten – insbesondere mit den Daten der Gesundheitsämter und der statistischen Landesämter – nicht ausreichen, wird es aus datenschutzrechtlicher Sicht darauf ankommen, dass

– die Aufteilung der Verantwortlichkeiten zwischen den verschiedenen am Nationalen Mortalitätsregister beteiligten Stellen klar abgegrenzt und
– die Voraussetzungen des Abgleichs mit und des Zugangs zu den Daten über die Verstorbenen

klar festgelegt sind.

Eine weitere zu diskutierende Frage ist hierbei, ob und in welchem Umfang Forscher einen Zugang zu personenbezogenen Daten benötigen.

Thematisiert wurde im Arbeitskreis auch die Möglichkeit, die Aufgaben der Forschungsdatenzentren der amtlichen Statistik (vgl. www.Forschungsdatenzentren.de) im Bundesstatistikgesetz dahingehend zu erweitern, dass über sie als Servicestellen Forschern Daten des Nationalen Mortalitätsregisters aufbereitet zur Verfügung gestellt werden.

Die Vertreter der Arbeitsgruppe „Mortalitätsregister“ werden ihr Konzept unter Berücksichtigung der im Arbeitskreis Wissenschaft geführten ersten Diskussion intern weiterentwickeln. Der Dialog wird im Jahr 2011 fortgesetzt. Letztendlich wird es eine Entscheidung des Bundesgesetzgebers sein, ob in Deutschland ein Nationales Mortalitätsregister aufgebaut werden soll.

4.7 Gesundheitswesen

4.7.1
Weiterhin in der Diskussion:
Die Ausgestaltung der Zugriffe auf Krankenhausinformationssysteme

Die Umsetzung der datenschutzrechtlichen Anforderungen an die Zugriffsausgestaltung bei Krankenhausinformationssystemen wirft nach wie vor sowohl in Hessen wie auch bundesweit Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben 2010 einen detaillierten Anforderungskatalog erarbeitet, der im Frühjahr 2011 veröffentlicht werden soll und eine Orientierung insbesondere für Krankenhausträger, Anwender, Hersteller und interne Datenschutzbeauftragte der Kliniken bietet.

4.7.1.1
Ausgangspunkt der Diskussion 2009

Krankenhausinformationssysteme (KIS) sind zu unverzichtbaren Hilfsmitteln der Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist technisch jederzeit ortsungebunden und zeitgleich 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. Ein Patient bzw. eine Patientin eines Klinikums rechnet nicht damit und muss auch nicht damit rechnen, dass die – u. U. mehreren tausend – Mitarbeiterinnen und Mitarbeiter des Klinikums seine sensitiven detaillierten medizinischen Daten während seiner Behandlung – vielleicht sogar noch Jahre danach – zur Kenntnis nehmen können. Vor dem Hintergrund, dass in den letzten Jahren immer wieder Fälle bekannt wurden, in denen zu weit gehende Zugriffsrechte dazu geführt haben, dass Klinikbeschäftigte Behandlungsdaten von Bekannten, Kollegen oder Prominenten unzulässig eingesehen und weitergegeben haben, bedarf dies Thema verstärkter Aufmerksamkeit. In meinem letzten Tätigkeitsbericht habe ich detailliert die rechtlichen Vorgaben des Hessischen Krankenhausgesetzes, der EU-Datenschutzrichtlinie sowie des Europäischen Gerichtshofs für Menschenrechte für die Ausgestaltung der Zugriffsmöglichkeiten auf Krankenhausinformationssysteme dargelegt (38. Tätigkeitsbericht, Ziff. 4.6.2.1.1 bis 4.6.2.1.4). Im Berichtszeitraum sind weiterhin sowohl in Hessen wie auch bundesweit intensive Diskussionen geführt worden.

4.7.1.2
Weitere Diskussion der von mir 2009 bei einer Prüfung festgestellten Defizite

2009 hatte ich eine Beschwerde zum Anlass genommen, die Ausgestaltung der Zugriffsberechtigungen auf das KIS einer Klinik vor Ort zu überprüfen. Im Rahmen der Prüfung hatte ich erhebliche Defizite bei der Ausgestaltung der Entscheidungsstrukturen, der Zugriffsberechtigungen und Abläufe festgestellt (s. hierzu auch 38. Tätigkeitsbericht, Ziff. 4.6.2.2.1). Eine Reihe von Defiziten wurde sofort oder zeitnah beseitigt (s. hierzu auch 38. Tätigkeitsbericht, Ziff. 4.6.2.2.1). Die internen Zugriffsmöglichkeiten auf personenbezogene Patientendaten wurden inzwischen im Hinblick auf die Erforderlichkeit überprüft und wesentlich reduziert. Ferner wurde die Protokollierung der Zugriffe auf personenbezogene Patientendaten erweitert.

Ein grundsätzlicher Kritikpunkt war die rechtliche und technische Ausgestaltung des Verhältnisses zwischen dem Klinikum und der Holding, der das Klinikum angehört. Das Klinikum ist eine Tochtergesellschaft der Gesundheit Nordhessen Holding AG (GNH). Der gesamte Bereich der Informationstechnologie (Hardware, Software, Kommunikationsinfrastruktur, Datenspeicher etc.) wurde vom Klinikum an die Holding ausgelagert. Damit konnten Mitarbeiter der Holding alle personenbezogenen Patientendaten des Klinikums zur Kenntnis nehmen. Es gab jedoch lediglich fragmentarische Regelungen in dem zwischen Klinikum und Holding geschlossenen Geschäftsbesorgungsvertrag, die keine Rechtsgrundlage für die Verarbeitung der Patientendaten durch die Holding sein können. Es lag auch kein Vertrag über Datenverarbeitung im Auftrag durch die Holding vor. Insbesondere konnte das Klinikum der Holding keine Weisungen erteilen. Aus dem Geschäftsbesorgungsvertrag ergab sich umgekehrt vielmehr die Weisungsgebundenheit des Klinikums.

Ein weiterer zentraler Kritikpunkt war die gemeinsame Stammdatenhaltung von dem Klinikum Kassel und dem Zentrum für medizinische Versorgung, einem vom Klinikum gegründeten Medizinischen Versorgungszentrum für die ambulante Krankenversorgung (MVZ). Beide Stellen sind rechtlich selbständige Daten verarbeitende Stellen im Sinne der Datenschutzgesetze. Infolge der gemeinsamen Stammdatenhaltung konnten sowohl die Mitarbeiter des Klinikums als auch die Mitarbeiter des MVZ auf sämtliche Stammdaten aller Patienten von Klinikum und MVZ zugreifen, obwohl die Patienten teilweise nur jeweils in einer der Einrichtungen behandelt wurden. Die Kenntnisnahme der Stammdaten der jeweils anderen Einrichtung erfolgte ohne Rechtsgrundlage.

Die Holding hat zunächst keine Änderungen vorgenommen und stattdessen ein Rechtsgutachten in Auftrag gegeben, in dem zu den von mir vertretenen rechtlichen Bewertungen Stellung genommen werden sollte. Dieses Rechtsgutachten „Stellungnahme und Gestaltungsvorschläge zu datenschutzrelevanten Einzelthemen in der Gesundheit Nordhessen Holding AG“ (Prof. Roßnagel et al.) wurde mir im November zur Kenntnis gegeben. Es stimmt in den zentralen Punkten mit den von mir vertretenen rechtlichen Bewertungen überein. Die zuvor mit dem Klinikum und der Holding geführten Kontroversen sind von grundsätzlicher Bedeutung auch für andere Kliniken, sodass hier im Folgenden die grundsätzlichen Punkte aufgeführt werden:

– Auslagerung des gesamten Bereichs der Informationstechnologie an die Holding

  Fragmentarische Regelungen in einem zwischen Klinikum und Holding geschlossenen Geschäftsbesorgungsvertrag sind keine Rechtsgrundlage für die Verarbeitung der Patientendaten des Klinikums durch die Holding. Wenn ein Klinikum der Holding keine Weisungen erteilen kann, sondern sich vielmehr aus dem Geschäftsbesorgungsvertrag eine Weisungsgebundenheit des Klinikums ergibt, liegt auch kein Vertrag über Datenverarbeitung im Auftrag als Rechtsgrundlage für die Verarbeitung der Patientendaten durch die Holding vor. Eine andere Rechtsgrundlage für die Übermittlung der Patientendaten an die Holding, z. B. im Landeskrankenhausgesetz, ist nicht vorhanden.

  Eine Verarbeitung der Patientendaten des Klinikums durch die Holding kann künftig rechtmäßig erfolgen, wenn ein Vertrag über Datenverarbeitung im Auftrag mit dem durch § 12 HKHG i. V. m. § 4 HDSG vorgegebenem Inhalt (s. hierzu auch den von mir unter http://www.datenschutz.hessen.de/mustervertragvia1.htm#entry2241 veröffentlichten Mustervertrag) zwischen dem Klinikum und der Holding abgeschlossen wird. Das bedeutet insbesondere, dass die Weisungsbefugnis des Klinikums gegenüber der Holding gewährleistet sein muss.

– Speicherung gemeinsamer Stammdatensätze der Patienten des Klinikums und des Medizinischen Versorgungszentrums (MVZ) durch die Holding

  Sowohl das Klinikum als auch das MVZ (das Zentrum für medizinische Versorgung GmbH, eine Tochtergesellschaft des Klinikums) sind jeweils eine rechtlich selbständige Daten verarbeitende Stelle. Derzeit werden von der Holding gemeinsame Stammdatensätze der Patienten beider Stellen gespeichert und zum Abruf bereitgehalten.

Auf diese gemeinsamen Stammdatensätze können sowohl Mitarbeiter des Klinikums als auch Mitarbeiter des MVZ umfassend zugreifen, d. h. auch dann, wenn ein Patient ausschließlich im Klinikum oder ausschließlich im MVZ behandelt wird. Dies ist unzulässig, und zwar auch dann, wenn die Holding einen wirksamen Vertrag über Datenverarbeitung im Auftrag sowohl mit dem Klinikum als auch mit dem MVZ abschließt. Die Holding muss in jedem Fall technisch-organisatorische Vorkehrungen treffen, damit gewährleistet ist, dass das Klinikum und das MVZ jeweils nur auf die Stammdatensätze ihrer eigenen Patienten zugreifen.

Die o. a. Zugriffsausgestaltung kann nicht durch eine Einwilligung der Patienten legitimiert werden. Bei formularmäßigen Klauseln muss eine zumutbare Möglichkeit zur Kenntnisnahme bestehen und die Erklärung die beabsichtigte Datenverwendung für den Betroffenen konkret und unmissverständlich erkennbar machen. Darüber hinaus gibt es rechtliche Grenzen im Hinblick darauf, was zum Inhalt einer Einwilligungserklärung gemacht werden kann: Der Umgang mit Patientendaten, die für die Behandlung unmittelbar erforderlich sind, wird durch die gesetzlichen Vorschriften abgedeckt, sodass keine Einwilligung benötigt wird. Es ist nicht zulässig, eine für die Behandlung nicht benötigte Verarbeitung personenbezogener Daten über eine eingeholte Einwilligung zu legitimieren. Ebenso wenig ist es zulässig, die in den Datenschutzgesetzen vorgeschriebenen technischen und organisatorischen Maßnahmen mit dem Hinweis auf eine datenschutzrechtliche Einwilligung der Betroffenen nicht umzusetzen. Unabhängig davon muss die Einwilligung eine freiwillige Entscheidung sein. Das bedeutet, dass für den Fall einer Ablehnung der Einwilligung oder den späteren Widerruf einer Einwilligung alternative Verfahrensweisen zur Verfügung stehen müssen.

Im Dezember 2010 hat mir das Klinikum mitgeteilt, dass es künftig die notwendigen vertraglichen Vereinbarungen über Datenverarbeitung im Auftrag durch die Holding in der von mir geforderten Form treffen wird. Hinsichtlich der gemeinsamen Stammdatenhaltung von Klinikum und MVZ liegen bisher noch keine hinreichenden Lösungsvorschläge vor.

4.7.1.3
Bundesweite Aktivitäten

Die Datenschutzbeauftragten des Bundes und der Länder sehen Handlungsbedarf hinsichtlich der Ausgestaltung und des Betriebs der Krankenhausinformationssysteme bundesweit. Auf ihrer Konferenz im Oktober 2009 haben sie eine Entschließung verabschiedet mit dem Thema

„Krankenhausinformationssysteme datenschutzgerecht gestalten!“ (s. 38. Tätigkeitsbericht, Ziff. 9.12). Darüber hinaus haben die Datenschutzbeauftragten des Bundes und der Länder 2009 eine gemeinsame Arbeitsgruppe eingerichtet, die auf eine generelle Verbesserung des Datenschutzes in den Krankenhäusern abzielt. Auch meine Dienststelle beteiligt sich an der Arbeitsgruppe. Der Düsseldorfer Kreis als Koordinierungsgremium der Aufsichtsbehörden über den privaten Bereich wurde über die Tätigkeit der Arbeitsgruppe informiert und er wurde eingeladen, sich an der Arbeitsgruppe zu beteiligen. Entsprechendes gilt für die Datenschutzbeauftragten der Kirchen. Die Arbeitsgruppe hat 2010 unter Einbeziehung von Experten aus den verschiedensten Bereichen und einer Anhörung von Anwendern und KIS-Herstellern eine detaillierte „Orientierungshilfe Krankenhausinformationssysteme“ erarbeitet.

Die Orientierungshilfe besteht aus zwei Teilen:

Teil I: Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus

Teil II: Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen.

Teil I beinhaltet rechtliche Anforderungen an die Zugriffsausgestaltung in Zusammenhang mit der Aufnahme des Patienten sowie während und nach Abschluss der Behandlung, u. a. auch an fachübergreifende Zugriffe und Zugriffe durch die Administration, ferner Fragen der Verarbeitung von Daten besonders schutzwürdiger Patientengruppen (z. B. Mitarbeiter des Krankenhauses und bekannte Persönlichkeiten), der Zugriffsprotokollierung und Datenschutzkontrolle sowie der Auskunftsrechte der Patienten.

Mit dem Teil II sollen die normativen Eckpunkte in technische Anforderungen umgesetzt werden. Er richtet sich an die Hersteller von Klinikinformationssystemen und an die Betreiber. An dieser Stelle möchte ich nur einige Beispiele von Forderungen und Themen nennen, die in dem Papier behandelt werden.

- Auf das Datenmodell wird in einem eigenen Kapitel eingegangen. So muss es die Mandantenfähigkeit umsetzen, die in der Praxis eine wichtige Rolle spielt. Es muss auch die sich aus dem Berechtigungskonzept ergebenden Forderungen optimal unterstützen. Dies betrifft bspw. Personen, die besonderen Gefährdungen ausgesetzt sind und auf deren Daten nicht nach den üblichen Regeln zugegriffen werden darf.
- In dem Abschnitt zum Berechtigungskonzept werden insbesondere die Anforderungen an die Patientenaufnahme, eine Mitbehandlung, ein Konzil, den Bereitschaftsdienst sowie Notfallzugriffe hinsichtlich der technischen Umsetzung konkretisiert.

– Fragen der Protokollierung werden ebenfalls detailliert behandelt. Hierbei geht es nicht zuletzt um lesende Zugriffe oder die Funktion der Protokollierung als Teil der Verfahrensdokumentation.
– Ein weiteres Thema ist das Zusammenspiel zwischen IT-technischer Auslagerung, Sperrung, Löschung und Archivierung.
– In einem separaten Kapitel wird auf den technischen Betrieb und die Administration eingegangen.

Als ein Gebiet, auf dem sich Schwierigkeiten abzeichnen, hat sich das Zusammenspiel verschiedener Komponenten der IT in einer Klinik ergeben. Neben dem eigentlichen KIS werden Röntgensysteme, Laborsysteme und andere Geräte genutzt, auf denen Daten der Patienten verarbeitet werden. So ist es noch nicht klar, wie Zugriffsberechtigungen zwischen diesen Komponenten so ausgetauscht werden können, dass sie das Berechtigungskonzept umfassend und einheitlich umsetzen. Das gilt vor allem, wenn die Komponenten von verschiedenen Herstellern stammen.

Nach weiteren Gesprächen mit Experten und einer abschließenden redaktionellen Bearbeitung soll die Orientierungshilfe im Frühjahr 2011 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedet und dann veröffentlicht werden.

4.7.2
Auftragsdatenverarbeitung durch den MDK Sachsen-Anhalt für den MDK Hessen – Fortsetzung der Prüfung

Auch im Berichtsjahr habe ich die Auftragsdatenverarbeitung beim Medizinischen Dienst der Krankenversicherung Sachsen-Anhalt geprüft. Ein neues Projekt ist die elektronische Erfassung von Daten nach § 301 SGB V sowie deren Verschlagwortung. Bei der Überprüfung der Verfahrensabläufe gab es keine gravierenden Defizite. Die fehlende Protokollierung der Zugriffe von sachsen-anhaltinischen MDK-Mitarbeitern auf die dafür bestimmte Datenbank des Servers des MDK Hessen in Oberursel gab jedoch Anlass zur Kritik.

4.7.2.1
Gegenstand der Auftragsdatenverarbeitung

Der MDK Hessen hat den MDK Sachsen-Anhalt damit beauftragt, die Daten nach § 301 SGB V, die für gutachterliche Stellungnahmen des MDK Hessen zu Fragen der Krankenkassen nach Krankenhausbehandlung und DRG-Codierung und/oder DRG-Verweildauer erforderlich sind, zu erfassen. Bei diesen Daten handelt es sich um Informationen, welche die Krankenhäuser im Zusammenhang mit der Behandlung eines Patienten an die Krankenkassen (also die Kostenträger) zu übermitteln haben. Unter anderen sind dies z. B. Angaben zur Einweisungs- bzw. Aufnahmediagnose, Verweildauer, Datum und Art der durchgeführten Operation u. a. Die MedFlex-GmbH, ein Tochterunternehmen des MDK Sachsen-Anhalt, erhält die Papierakten zu den Versicherten und erfasst die in den Akten hinterlegten Daten, sog. 301er-Daten.

§ 80 Abs. 1 und 2 SGB X

(1) Werden Sozialdaten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzbuches und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 82 bis 84 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Eine Auftragserteilung für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten ist nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu erhebenden, zu verarbeitenden oder zu nutzenden Daten den Anforderungen genügt, die für den Auftraggeber gelten. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

§ 301 Abs. 1 SGB V

Die nach § 108 zugelassenen Krankenhäuser sind verpflichtet, den Krankenkassen bei Krankenhausbehandlung folgende Angaben im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern zu übermitteln:

1. die Angaben nach § 291 Abs. 2 Nr. 1 bis 10 sowie das krankenhausinterne Kennzeichen des Versicherten,
2. das Institutionskennzeichen des Krankenhauses und der Krankenkasse,

3. den Tag, die Uhrzeit und den Grund der Aufnahme sowie die Einweisungsdiagnose, die Aufnahmediagnose, bei einer Änderung der Aufnahmediagnose die nachfolgenden Diagnosen, die voraussichtliche Dauer der Krankenhausbehandlung sowie, falls diese überschritten wird, auf Verlangen der Krankenkasse die medizinische Begründung, bei Kleinkindern bis zu einem Jahr das Aufnahmegewicht,
4. bei ärztlicher Verordnung von Krankenhausbehandlung die Arztnummer des einweisenden Arztes, bei Verlegung das Institutionskennzeichen des veranlassenden Krankenhauses, bei Notfallaufnahme die die Aufnahme veranlassende Stelle,
5. die Bezeichnung der aufnehmenden Fachabteilung, bei Verlegung die der weiterbehandelnden Fachabteilungen,
6. Datum und Art der im jeweiligen Krankenhaus durchgeführten Operationen und sonstigen Prozeduren,
7. den Tag, die Uhrzeit und den Grund der Entlassung oder der Verlegung, bei externer Verlegung das Institutionskennzeichen der aufnehmenden Institution, bei Entlassung oder Verlegung die für die Krankenhausbehandlung maßgebliche Hauptdiagnose und die Nebendiagnosen,
8. Angaben über die im jeweiligen Krankenhaus durchgeführten Leistungen zur medizinischen Rehabilitation und ergänzende Leistungen sowie Aussagen zur Arbeitsfähigkeit und Vorschläge für die Art der weiteren Behandlung mit Angabe geeigneter Einrichtungen,
9. die nach den §§ 115a und 115b sowie nach dem Krankenhausentgeltgesetz und der Bundespflegesatzverordnung berechneten Entgelte.

Die Übermittlung der medizinischen Begründung von Verlängerungen der Verweildauer nach Satz 1 Nr. 3 sowie der Angaben nach Satz 1 Nr. 8 ist auch in nicht maschinenlesbarer Form zulässig.

4.7.2.2
Ablauf des Verfahrens

Von den einzelnen Geschäftsbereichen in Hessen werden die Papierakten per Post nach Sachsen-Anhalt verbracht. Die Transportbehältnisse sind mit einem Sicherheitssiegel versehen, um ggf. ein unbefugtes Öffnen der Behälter zur Kenntnis nehmen zu können. Zu den Behältnissen wird ein Transferprotokoll angefertigt, in dem die einzelnen Akten bezeichnet sind. Dieses Protokoll wird in Sachsen-Anhalt geprüft, um so die Vollzähligkeit der Akten nachvollziehbar zu machen. In der Geschäftsstelle des MDK Sachsen-Anhalt in Halle werden

die Unterlagen gescannt und mit Schlagworten versehen. Vorhandene Plausibilitätsfehler werden behoben.

Für bestimmte Beschäftigte, die in einer Anlage zum Datenschutzvertrag benannt sind, wurde ein benutzerbezogener Zugriff auf das Datenbanksystem des MDK Hessen eingerichtet. Der berechtigte Personenkreis identifiziert sich über ein persönliches Passwort. Nach den vertraglichen Regelungen (§ 1 Abs. 3 des Dienstleistungsvertrages) soll dies mindestens neun Stellen lang sein und sich aus einer Kombination von Buchstaben- und Zahlenfolgen zusammensetzen.

Tatsächlich ist das individuelle Kennwort aber nur fünf Stellen lang (dies entspricht im Übrigen auch nicht den Empfehlungen des BSI, welches eine Mindestlänge von acht Stellen als erforderlich beschreibt). Auch der nur halbjährliche Wechsel des Passwortes ist in diesem Zusammenhang nicht angemessen. Noch akzeptabel erscheint ein Wechselrhythmus von 90 Tagen, 45 bis 60 Tage entsprechen dem üblichen Standard.

Nachdem der Plausibilitätsfehler behoben sind, veranlassen berechtigten Beschäftigten die Ablage der elektronisch erfassten Unterlagen sowie der dazugehörigen Daten nach § 301 SGB V über den Server des MDK Sachsen-Anhalt auf dem Server des MDK Hessen in Oberursel. Dies erfolgt über eine sichere sog. getunnelte Leitung (VPN). Alle zwei bis drei Wochen werden die vom MDK Hessen gelieferten Papierunterlagen von einem Transportunternehmen an den Absender zurückgebracht.

4.7.2.3
Mängel im Ablauf der Datenverarbeitung

Beim Auftragnehmer selbst gab es in der Ablauforganisation sowie den formalen Erfordernissen an Nachvollziehbarkeit und Transparenz nichts zu kritisieren. Zum Dienstleistungsvertrag wurde ein Datenschutzvertrag abgeschlossen, der in einer Anlage die technischen und organisatorischen Maßnahmen zum Datenschutz und der Datensicherheit nach § 10 Abs. 2 beschreibt. Ein zusätzliches Papier nennt den Personenkreis, der für die Abwicklung der Auftragsdatenverarbeitung zuständig ist. So bleibt einzig die unzureichende Passwortgestaltung, die mittlerweile behoben wurde.

Ein anderer Punkt betrifft die Protokollierung der Zugriffe aus Sachsen-Anhalt auf die Datenbank des MDK-Servers in Hessen. Zwar wird ein sog. „Scan- und Indexprotokoll“ in

Form einer Papierliste geführt, in der die Mitarbeiter in Sachsen-Anhalt u. a. den Zeitpunkt, die Anzahl der Bilddateien sowie die gescannten Seitenzahlen dokumentieren. Eine elektronische Protokollierung der Zugriffe auf den hessischen Server erfolgt jedoch nicht. Begründet wurde dies mit dem hohen technischen Aufwand, der hierfür geleistet werden müsste. Außerdem sehe das vom MDK Hessen genutzte elektronische Archiv eine derartige Protokollfunktion nicht vor. Derzeit stimme ich mich mit dem MDK Hessen darüber ab, wie dieses Defizit behoben werden kann.

4.7.3
Umfang und Inhalt amtsärztlicher Gutachten

Nach wie vor kommt es in Einzelfällen zu Diskussionen darüber, wie amtsärztliche Gutachten, insbesondere bei der Beurteilung der Dienstfähigkeit von Betroffenen, inhaltlich gestaltet sein müssen. Das Hessische Gesetz über den öffentlichen Gesundheitsdienst enthält hierzu Vorgaben.

4.7.3.1
Mögliche Fallkonstellationen für eine Begutachtung

Anlass für Dienstherrn oder Arbeitgeber, Beschäftigte zum Amtsarzt zu schicken, kann entweder deren Einstellung oder die Klärung der Frage sein, ob die zu Untersuchenden den erforderlichen gesundheitlichen Voraussetzungen für das Berufsbild entsprechen. Es kann auch um die Frage gehen, ob der oder die Betroffene gesundheitlich noch in der Lage ist, die konkret übertragenen Aufgaben zu verrichten und deshalb der Gesundheitszustand sowie mögliche Perspektiven für eine Reintegration zu beleuchten sind.

4.7.3.2
Vorgaben für die Durchführung einer amtsärztlichen Untersuchung

Im Hessischen Gesetz über den öffentlichen Gesundheitsdienst (HGöGD) vom 28. September 2007 (GVBl. I S. 659 ff.) ist in § 14 die Aufgabe der Gesundheitsämter hinsichtlich amtsärztlicher Untersuchungen und der Erstellung von Gutachten, Zeugnissen und Bescheinigungen beschrieben. Dabei wird ausdrücklich auf öffentlich Bedienstete und

Bewerberinnen und Bewerber für den Öffentlichen Dienst im Zusammenhang mit dem Dienstverhältnis verwiesen, für welche diese Vorschrift gilt.

§ 14 Abs. 1 HGöGD

Die Gesundheitsämter nehmen amtsärztliche Untersuchungen vor und erstellen hierüber Gutachten, Zeugnisse und Bescheinigungen. Dies gilt insbesondere für die Erstellung von Gutachten, Zeugnissen und Bescheinungen für öffentliche Bedienstete und Bewerberinnen und Bewerber für den Öffentlichen Dienst im Zusammenhang mit dem Dienstverhältnis oder wenn die amtsärztliche Untersuchung zur Aufgabenerfüllung des Trägers des Gesundheitsamtes erforderlich ist.

Hinsichtlich der datenschutzrechtlichen Erfordernisse, die den Umfang sowie den Inhalt solcher Gutachten betrifft, ist § 18 Abs. 1 HGöGD einschlägig.

§ 18 Abs. 1 HGöGD

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

Die Vorschrift beinhaltet drei wesentliche Kernpunkte:

- Vor Beginn der Untersuchung ist die zu untersuchende Person über deren Zweck zu informieren.

- Dabei sind die Stellen zu benennen, an welche die Daten übermittelt werden. Dies ist in der Regel der Auftraggeber des Gutachtens.

- Grundsätzlich darf nur das Untersuchungsergebnis dem Auftraggeber mitgeteilt werden. Darin enthalten sollten auch Aussagen sein, wie der Betroffene künftig in der Behörde eingesetzt werden kann.

Nur mit diesen Informationen ist es dem Dienstherrn möglich, Arbeitsbedingungen zu verändern oder einen speziell auf die betroffene Person zugeschnitten - ggf. neuen - Arbeitsplatz anzubieten. Über das Untersuchungsergebnis hinaus können im konkreten Einzelfall Anamnesedaten oder einzelne Untersuchungsergebnisse mitgeteilt werden, soweit dies erforderlich ist, um im Sinne der Untersuchten Entscheidungen über konkrete Maßnahmen hinsichtlich der Ausgestaltung z. B. des Arbeitsplatzes oder der Arbeitszeit zu treffen.

4.7.3.3
Weitere Rechte des Betroffenen

Das HGöGD verweist im Weiteren hinsichtlich datenschutzrechtlicher Vorgaben auf die allgemeinverbindlichen Regelungen des Hessischen Datenschutzgesetzes. Was die Einsichtsrechte des Betroffenen in das Gutachten sowie die Befunde anbelangt, so ist hier § 18 HDSG einschlägig. Die Einsichtsrechte gelten sowohl für die zur Person des Betroffenen in Akten gespeicherten Daten als auch für die in automatisierten Datenverarbeitungsanlagen gespeicherten personenbezogenen Angaben.

4.7.3.4
Umgang mit den erhobenen Daten durch den Amtsärztlichen Dienst und Einbeziehung weiterer Unterlagen

In den Gesundheitsämtern werden vielfältige, personenbezogene Daten erhoben: ob Schuleingangsuntersuchung, schulzahnärztlicher Dienst, Infektionsschutz, sozialpsychiatrischer Dienst oder amtsärztlicher Dienst, um nur einige Stellen zu nennen, die medizinische Daten erheben und speichern. In jedem Fall bleibt festzustellen, dass das Gesundheitsamt, wie auch andere öffentliche Stellen (z. B. ein kommunales Krankenhaus, ein Rathaus u. a.) keine informationelle Einheit ist, in der personenbezogene Daten ohne konkreten Anlass hin- und herfließen bzw. von jedem Beschäftigten einsehbar sind. Insbesondere die Daten des amtsärztlichen Dienstes, die in der Regel bei Einstellungsuntersuchungen oder aber im Zusammenhang mit der Überprüfung der Dienstfähigkeit von Betroffenen erhoben werden, sind gegenüber anderen Stellen abzuschotten. Umgekehrt dürfen vom amtsärztlichen Dienst für die Erstellung eines Gutachtens keine weiteren Unterlagen aus anderen Bereichen des Gesundheitsamtes hinzugezogen werden.

Im Grundsatz wird die getrennte Datenhaltung in allen von mir befragten Ämtern praktiziert, denn die ärztliche Schweigepflicht gilt auch in der Kommunikation zwischen den Ärzten. Eine Offenbarung medizinischer Informationen gegenüber Dritten (also auch anderen Ärzten innerhalb des Amtes) ist demnach nur mit der Einwilligung des Betroffenen möglich. Zudem verweist das HGöGD hinsichtlich der datenschutzrechtlichen Vorgaben auf die Regelungen des Hessischen Datenschutzgesetzes. So ist die Verarbeitung personenbezogener Daten nach § 11 HDSG zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Hinzu kommt, dass die Daten nur für den Zweck weiterverarbeitet werden dürfen, für den sie erhoben oder gespeichert worden sind (§ 13 HDSG).

In den wenigen Fällen, in dem diese Verfahrensweise nicht umgesetzt war, habe ich für eine Klarstellung gesorgt.

4.7.3.5
Defizite bei der Umsetzung der Vorgaben des HGöGD und HDSG

Immer wieder erhalte ich Eingaben, in denen die Inhalte der Gutachten selbst oder aber deren Umfang bei der Übermittlung an den Arbeitgeber kritisiert werden. Inhaltlich haben sich die Gutachten streng an dem vom Auftraggeber formulierten Gutachtenauftrag zu orientieren. Eine Vermengung von Anamnese- und Befunddaten, gepaart mit Prognosen über den weiteren Gesundheitsverlauf und anderen Aspekten zur Person des Betroffenen, ist grundsätzlich auszuschließen. Eine ebenso strenge wie strukturierte Unterscheidung der einzelnen Untersuchungsabschnitte (Anamnese, Befunde, aktuelle Einschätzung, Prognose) ist im Sinne des § 18 Abs. 1 HDSG zwingend. In den bislang mir zur Kenntnis gelangten Fällen, bei denen dies keine Berücksichtigung fand, habe ich das gegenüber der Gesundheitsverwaltung deutlich zum Ausdruck gebracht.

4.7.4
Patientenlisten auf dem Gehweg

In Kassel wurden im Frühjahr zweimal von Passanten Patientenlisten der Klinik für Psychiatrie und Psychotherapie des Klinikums Kassel mit Namen und Diagnosen gefunden. Das Klinikum

hat den Sachverhalt jeweils umgehend überprüft und in Abstimmung mit meiner Dienststelle Maßnahmen getroffen, damit sich ein solcher Fall nicht wiederholt.

Im Frühjahr 2010 wurde in Kassel von einem Passanten eine Liste mit 21 Namen von Patientinnen und Patienten gefunden. Die Liste enthielt deren Geburtsdaten, Zimmernummern und Aufnahmediagnosen wie z. B. paranoide Depression, dissoziale Persönlichkeitsstörung, paranoide Schizophrenie, wahnhafte Störung, Angststörung oder Borderline-Syndrom. Auf der Liste stand das Datum des Ausdrucks, der 24. März 2010. Der Passant übergab die Liste der Kasseler Redaktion der Hessisch/Niedersächsischen Allgemeinen Zeitung, die schnell herausfand, dass es sich um eine Liste des Klinikums Kassel handelte.

In Absprache mit meiner Dienststelle überprüfte das Klinikum den Sachverhalt umgehend und teilte folgendes Ergebnis mit:

Die meisten Behandlungsunterlagen werden längerfristig in der rechtlich gebotenen Dokumentation der Behandlung aufbewahrt bzw. elektronisch gespeichert. In diesem Fall handelte es sich ausnahmsweise um eine nur vorübergehend benötigte personenbezogene Arbeitsunterlage (Patientenliste). Eine solche Patientenliste wird täglich in der Klinik für Psychiatrie und Psychotherapie des Kasseler Klinikums erstellt und ausgedruckt. Die Liste wird von Ärzten und Pflegekräften für die täglichen Visiten und Übergaben genutzt und darüber hinaus im Klinikum nicht verwendet. Wer die Liste auf dem Gehweg verloren hat, konnte nicht geklärt werden. Patienten konnten innerhalb des Klinikums nicht in den Besitz der Liste gelangen, weil der Drucker in einem öffentlich nicht zugänglichen Dienstzimmer steht. Es lag vermutlich ein menschliches Versagen eines Mitarbeiters oder einer Mitarbeiterin vor, d. h. dass die Liste vom 24. März 2010 versehentlich nicht entsorgt, sondern sie in einer Kleidungstasche vergessen und später aus Unachtsamkeit verloren wurde.

Als Reaktion auf den Vorfall hat das Klinikum Kassel in Abstimmung mit mir folgende Maßnahmen getroffen:

– **Anschaffung von Aktenvernichtungsgeräten**
  Es wurden zusätzliche 8 Aktenvernichtungsgeräte angeschafft, damit die Mitarbeiter und Mitarbeiterinnen nicht mehr benötigte Arbeitsmittel zeitnah direkt selbst vor Ort vernichten können.

– **Dienstanweisung**
  Die Mitarbeiter und Mitarbeiterinnen der Klinik für Psychiatrie und Psychotherapie wurden

sowohl direkt von der Klinik für Psychiatrie und Psychotherapie wie auch in einem Schreiben des Klinikumsvorstands auf die Notwendigkeit einer datenschutzkonformen Entsorgung nicht mehr benötigter Arbeitsmittel hingewiesen.

– **Schulungen zu Datenschutz für alle Mitarbeiterinnen und Mitarbeiter**
  Es wurde beschlossen, dass der interne Datenschutzbeauftragte des Klinikums im April eine Datenschutzschulung in der Klinik für Psychiatrie und Psychotherapie abhält und diese Schulung für alle Mitarbeiter und Mitarbeiterinnen (Ärzte, Pflegekräfte, Verwaltungspersonal etc.) verpflichtend ist.

Trotz dieser Maßnahmen wurde im Frühjahr 2010 nochmals eine Patientenliste der Klinik für Psychiatrie und Psychotherapie in Kassel von einem Passanten aufgefunden, diesmal von einer anderen Station. Damit wurde klar, dass zusätzliche Maßnahmen erforderlich sind zum Schutz der Patientendaten. In Abstimmung mit mir hat das Klinikum die folgenden Maßnahmen getroffen:

– **Ergänzende Dienstanweisung**
  Vom Direktor der Klinik wurde eine Dienstanweisung herausgegeben, die bestimmt, dass nur noch eine Liste pro Tag und Station ausgedruckt werden darf; die Liste ist täglich bei der Übergabe gegen eine aktualisierte Liste auszutauschen und die alte Liste im Schredder zu vernichten.

– **Reduktion der auf den Ausdrucken ersichtlichen Daten**
  Die Daten der Übergabeliste wurden reduziert. Die Liste enthält jetzt insbesondere nicht mehr Informationen über Klinik, Station, Patientennummer und Diagnose.

Vergleichbare Vorfälle sind mir von diesem Klinikum bis zum Frühjahr 2010 nicht bekannt geworden und auch in den Monaten danach nicht mehr. Da das Klinikum den Sachverhalt jeweils sofort soweit wie möglich aufgeklärt und in Abstimmung mit mir die Datenschutzmaßnahmen zügig entschieden und umgesetzt hat, habe ich von einer formellen Beanstandung gem. § 27 HDSG abgesehen.

4.7.5
Auskunftsanspruch gegenüber einer Unfallversicherung

Die Frage, ob gegenüber einer Unfallversicherung ein Auskunftsanspruch Dritter hinsichtlich eines Verstorbenen besteht, richtet sich in erster Linie nach dem allgemeinen Sozialdatenschutzrecht. Darüber hinaus kann Auskunft auch dann gegeben werden, wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen dadurch nicht beeinträchtigt werden.

4.7.5.1
Der Fall

Ein Bürger wandte sich an meine Dienststelle und beschwerte sich, dass ihm die Land- und forstwirtschaftliche Berufsgenossenschaft Hessen, Rheinland-Pfalz und Saarland (LBG) auf seine Anfrage hin keine Auskünfte über Rentenzahlungen an seine zwischenzeitlich verstorbene Mutter erteilte. Der Beschwerdeführer hatte die Anfrage im Zusammenhang mit Ermittlungen des Finanzamtes hinsichtlich einer möglichen Steuerhinterziehung gestellt. Er hatte zusammen mit zwei Geschwistern Erbschaftsansprüche geltend gemacht. Die Miterben wussten von seinem Auskunftsbegehren offensichtlich nichts.

4.7.5.2
Die Position der LBG

Bei den begehrten Auskünften über Rentenzahlungen handelt es sich um die Übermittlung von Sozialdaten. Daher prüfte die LBG zunächst, ob sich nach § 35 Abs. 5 Satz 1 SGB I i. V. m. § 67d Abs. 1 SGB X eine spezielle Rechtsgrundlage für eine Weitergabe der Sozialdaten ergeben könnte.

§ 35 Abs. 5 SGB I

Sozialdaten Verstorbener dürfen nach Maßgabe des Zweiten Kapitels des Zehnten Buches verarbeitet oder genutzt werden. Sie dürfen außerdem verarbeitet oder genutzt werden, wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen dadurch nicht beeinträchtigt werden können.

§ 67d Abs. 1 SGB X

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

Die LBG sah hier keinen rechtlichen Ansatz, dem Betroffenen die Daten seiner verstorbenen Mutter zugänglich zu machen. Auch sah die LBG möglicherweise schutzwürdige Belange der Miterben berührt, die von der Anfrage des Beschwerdeführers keine Kenntnis hatten, so dass sie eine Übermittlung nach § 35 Abs. 5 Satz 2 SGB I ebenfalls ablehnte. Den Vorschlag der LBG, die Miterben in Kenntnis zu setzen und allen gemeinsam die Informationen zu eröffnen, lehnte der Beschwerdeführer ab. Als die LBG auf ihrer Rechtsposition beharrte, schaltete der Betroffene meine Behörde mit dem Ziel ein, die LBG zu einer Auskunft zu veranlassen.

4.7.5.3
Rechtliche Würdigung

Die Position, welche die LBG vertreten hat, war rechtlich nicht zu beanstanden. Aus diesem Grund sah ich auch keine Möglichkeit, sie auf eine Übermittlung der geforderten Daten verpflichten zu können. Im Übrigen hatte die LBG mich ebenfalls eingeschaltet und um eine rechtliche Bewertung gebeten.

Für den Betroffenen bestand ausschließlich die Möglichkeit, zusammen mit den Miterben die geforderten Informationen einzuholen. Anderenfalls wären die schutzwürdigen Interessen der Miterben beeinträchtigt worden. Nur wenn dies hätte ausgeschlossen werden können, wäre die Weitergabe der Informationen aus der Versichertenakte der verstorbenen Mutter rechtlich unangreifbar gewesen. Da aber genau das, auch durch das Verhalten des Beschwerdeführers, nicht ausgeschlossen werden konnte, war es korrekt, dass die LBG die Auskunft ohne Einwilligung der Miterben verweigerte. Im Umkehrschluss stand es meiner Behörde jedenfalls nicht zu, die LBG zur Datenübermittlung anzuhalten.

4.8 Sozialwesen

4.8.1
Datenschutzvorrang im Sozialverwaltungsverfahren

Soweit bei der Ermittlung des Sachverhalts personenbezogene Daten betroffen sind, sind im Verhältnis zum Sozialverwaltungsverfahrensrecht die den Sozialdatenschutz betreffenden Rechtsnormen vorrangig. Für die Zulässigkeit des Verwaltungshandelns im Sozialverwaltungsverfahren hat das erhebliche Bedeutung.

4.8.1.1
Der Anlass

In Besprechungsrunden, in Telefonaten und im Schriftverkehr mit Behörden, die im Sozialbereich tätig sind (z. B. Grundsicherung für Arbeitsuchende, Sozialhilfe, Wohngeld etc.), tritt regelmäßig zum Vorschein, dass Unsicherheiten hinsichtlich des Verhältnisses von Sozialverwaltungsverfahrensrecht einerseits und Sozialdatenschutzrecht andererseits bestehen. Exemplarisch wird hier der Beginn des Schreibens einer Sozialbehörde zitiert, der textbausteinartig auch in vielen anderen Schreiben von Sozialbehörden auftaucht:

„Gemäß § 20 SGB X ermittelt die Behörde den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen. Die Behörde bedient sich der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann insbesondere Auskünfte jeder Art einholen (§ 21 SGB X).“

Damit ist die Rechtslage bei der Sachverhaltsermittlung im Sozialverwaltungsverfahren im Hinblick auf den Datenschutz nur unzulänglich wiedergegeben.

4.8.1.2
Rechtliche Würdigung

Während einerseits die den Untersuchungsgrundsatz und die Beweismittel betreffenden §§ 20, 21 SGB X den Behörden selbstverständlich bekannt sind, ist andererseits die für den Datenschutz im Sozialverwaltungsverfahren entscheidende Rechtsvorschrift des § 37 SGB I nicht immer geläufig.

Das liegt allerdings auch daran, dass diese Norm zum einen an höchst unauffälliger Stelle im Sozialgesetzbuch platziert und dass zum anderen die Bedeutung des Wortlautes der Norm nicht aus sich selbst heraus erschließbar ist.

Konkret geht es um Satz 3 der Vorschrift § 37 SGB I, die den „Vorbehalt abweichender Regelungen“ betrifft. Das SGB I enthält den Allgemeinen Teil des Sozialgesetzbuches, und § 37 Satz 3 SGB I regelt nun eine Frage, die ein ganz anderes Buch des Sozialgesetzbuchs, nämlich das SGB X betrifft; dieses enthält Vorschriften zum Sozialverwaltungsverfahren (§§ 1 ff. SGB X) und zum Sozialdatenschutz (§§ 67 ff. SGB X).

§ 37 Satz 3 SGB I

Das Zweite Kapitel des Zehnten Buches geht dessen Erstem Kapitel vor, soweit sich die Ermittlung des Sachverhalts auf Sozialdaten erstreckt.

Das Zweite Kapitel des Zehnten Buches regelt den Schutz der Sozialdaten. Das Erste Kapitel enthält die Vorschriften zum Verwaltungsverfahren und ist nachrangig, soweit sich die Ermittlung des Sachverhalts auf Sozialdaten erstreckt, und Sozialdaten sind (kurzgefasst) personenbezogene Daten im Sozialbereich (§ 67 Abs. 1 SGB X). § 37 Satz 3 SGB I bedeutet folglich, dass - soweit personenbezogene Daten betroffen sind - bei der Sachverhaltsermittlung das Verwaltungshandeln mit dem Sozialdatenschutzrecht kompatibel sein muss, und es reicht eben nicht, wenn es sich nur mit §§ 20, 21 SGB X (Untersuchungsgrundsatz, Beweismittel) in Einklang bringen lässt. Für die Zulässigkeit des Verwaltungshandelns hat dies gravierende Auswirkungen.

4.8.1.3
Konsequenzen für das Verwaltungshandeln

Der Vorrang des Sozialdatenschutzrechtes bedeutet bspw., dass die Behörde keineswegs Art und Umfang der Ermittlungen schrankenlos bestimmen (§ 20 Abs. 1 Satz 2 SGB X) und Auskünfte jeder Art einholen kann (§ 21 Abs. 1 Satz 2 Nr. 1 SGB X), denn diese Befugnisse sind durch den Sozialdatenschutz eingeschränkt. So legt § 67a Abs. 1 Satz 1 SGB X fest, dass das Erheben von Sozialdaten nur zulässig ist, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. Außerdem sind

Sozialdaten grundsätzlich beim Betroffenen zu erheben (§ 67a Abs. 2 Satz 1 SGB X). Daran knüpfen ergänzend Mitwirkungsobliegenheiten des Betroffenen an (§ 60 ff. SGB I).

§ 60 SGB I

(1) Wer Sozialleistungen beantragt oder erhält, hat
1. alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen.
2. Änderungen in den Verhältnissen, die für die Leistung erheblich sind oder über die im Zusammenhang mit der Leistung Erklärungen abgegeben worden sind, unverzüglich mitzuteilen,
3. Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen.

Ohne seine Mitwirkung dürfen Sozialdaten bei anderen Stellen und Personen nur ausnahmsweise erhoben werden (§ 67a Abs. 2 Satz 2 SGB X).

Der durch §§ 20, 21 SGB X suggerierte weite Gestaltungsspielraum der Sozialbehörden bei der Sachverhaltsermittlung wird also, wenn es um personenbezogene Daten geht, durch das Gebot der Erforderlichkeit und des Grundsatzes der Datenerhebung beim Betroffenen eingeschränkt.

Das Sozialdatenschutzrecht ordnet damit etwas an, was auch im allgemeinen Datenschutzrecht Standard ist. §§ 3 Abs. 3 HDSG, 1 Abs. 4 BDSG bestimmen nämlich ebenfalls hinsichtlich der Sachverhaltsermittlung den Vorrang des Datenschutzrechtes vor dem Verwaltungsverfahrensrecht, soweit personenbezogene Daten betroffen sind. Das Problem im Sozialbereich liegt offenbar darin, dass der den Vorrang des Sozialdatenschutzrechtes anordnende § 37 Satz 3 SGB I augenscheinlich recht unbekannt ist.

Auf diese Vorschrift und den damit verbundenen Vorrang des Sozialdatenschutzrechts im Verhältnis zum Sozialverwaltungsverfahrensrecht mache ich in Gesprächen und im Schriftverkehr regelmäßig aufmerksam.

4.8.2
Abruf von Konteninformationen eines „Doppelgängers“ durch eine Sozialbehörde

Existieren Personen mit identischem Namen und Geburtsdatum, kann nicht vollständig ausgeschlossen werden, dass in einem Kontenabrufverfahren nach der Abgabenordnung Daten von unbeteiligten Dritten an eine abrufende Stelle, hier einen Sozialleistungsträger, übermittelt werden.

Mir lag die Beschwerde eines Bürgers vor, bei dem eine Vielzahl persönlicher Daten von ihm und seinen Angehörigen an einen Sozialleistungsträger gelangt waren. Aufgrund diverser Ereignisse in der Vergangenheit wie z. B. der Beantragung der Sozialversicherungsnummer oder der Eröffnung seines ersten Bankkontos war ihm bekannt, ohne dass es bisher einen direkten Kontakt gegeben hatte, dass es einen Mann gleichen Namens und Geburtsdatums gibt, einen „Doppelgänger“.

Meine Sachverhaltsermittlung ergab Folgendes: Wegen eines Antrages des „Doppelgängers“ bei der Sozialbehörde hatte diese einen Abruf von Konteninformationen beim Bundeszentralamt für Steuern durchgeführt (vgl. zum Kontendatenabrufverfahren die Darstellung in meinem 35. Tätigkeitsbericht, Ziff. 5.10).

§ 93 Abs. 8 AO

Die für die Verwaltung
1. der Grundsicherung für Arbeitsuchende nach dem Zweiten Buch Sozialgesetzbuch,
2. der Sozialhilfe nach dem Zwölften Buch Sozialgesetzbuch,
3. der Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz,
4. der Aufstiegsfortbildungsförderung nach dem Aufstiegsfortbildungsförderungsgesetz und
5. des Wohngeldes nach dem Wohngeldgesetz

zuständigen Behörden dürfen das Bundeszentralamt für Steuern ersuchen, bei den Kreditinstituten die in § 93b Abs. 1 bezeichneten Daten abzurufen, soweit dies zur Überprüfung des Vorliegens der Anspruchsvoraussetzungen erforderlich ist und ein vorheriges Auskunftsersuchen an den Betroffenen nicht zum Ziel geführt hat oder keinen Erfolg verspricht. Für andere Zwecke ist ein Abrufersuchen an das Bundeszentralamt für Steuern hinsichtlich der in § 93b Abs. 1 bezeichneten Daten nur zulässig, soweit dies durch ein Bundesgesetz ausdrücklich zugelassen ist.

§ 93b AO

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

(2) Das Bundeszentralamt für Steuern darf in den Fällen des § 93 Abs. 7 und 8 auf Ersuchen bei den Kreditinstituten einzelne Daten aus den nach Absatz 1 zu führenden Dateien im automatisierten Verfahren abrufen und sie an den Ersuchenden übermitteln.

(3) Die Verantwortung für die Zulässigkeit des Datenabrufs und der Datenübermittlung trägt der Ersuchende.

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

§ 24c Abs. 1 KWG

Ein Kreditinstitut hat eine Datei zu führen, in der unverzüglich folgende Daten zu speichern sind:

1. die Nummer eines Kontos, das der Verpflichtung zur Legitimationsprüfung im Sinne des § 154 Abs. 2 Satz 1 der Abgabenordnung unterliegt, oder eines Depots sowie der Tag der Errichtung und der Tag der Auflösung,
2. der Name, sowie bei natürlichen Personen der Tag der Geburt, des Inhabers und eines Verfügungsberechtigten sowie in den Fällen des § 3 Abs. 1 Nr. 3 des Geldwäschegesetzes der Name und, soweit erhoben, die Anschrift eines abweichend wirtschaftlich Berechtigten im Sinne des § 1 Abs. 6 des Geldwäschegesetzes.

Bei jeder Änderung einer Angabe nach Satz 1 ist unverzüglich ein neuer Datensatz anzulegen. Die Daten sind nach Ablauf von drei Jahren nach der Auflösung des Kontos oder Depots zu löschen. Im Falle des Satzes 2 ist der alte Datensatz nach Ablauf von drei Jahren nach Anlegung des neuen Datensatzes zu löschen. Das Kreditinstitut hat zu gewährleisten, dass die Bundesanstalt jederzeit Daten aus der Datei nach Satz 1 in einem von ihr bestimmten Verfahren automatisiert abrufen kann. Es hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen.

Die Sozialbehörde hatte bei ihrer Anfrage die geforderten Angaben über den Leistungsempfänger (Name, Geburtsdatum, Anschrift) angegeben. Die der Sozialbehörde vom Bundeszentralamt für Steuern zur Verfügung gestellten Daten umfassten die Kontoverbindungen des Betroffenen bei diversen Finanzinstituten, seinen Arbeitgeber, die Namen und Geburtsdaten seiner Ehefrau, seiner beiden Töchter und seiner Mutter sowie die Kontoverbindungen seiner Mutter und Töchter, über die er jeweils mit Vollmacht verfügt. Die Kontodatenauskunft gab den Namen und das Geburtsdatum korrekt wieder, eine Anschrift fehlte. Die Auskunft enthielt den Hinweis, dass es sich bei dem Ergebnis nicht zwingend um die angefragte Person handeln müsse, da der Kontenabruf nur unter den Merkmalen Name und Geburtsdatum erfolgte, nicht jedoch mit der Anschrift.

Da die Sozialbehörde der Ansicht war, es handele sich um die Daten des dortigen Leistungsempfängers (des „Doppelgängers“), legte sie diesem die Kontendaten (Kontonummer und Bank) vor und forderte ihn zur Stellungnahme auf. Durch einen darüber hinaus anhängigen Rechtsstreit zwischen dem „Doppelgänger“ und der Sozialbehörde wurden alle abgerufenen Daten auch bei Gericht aktenkundig.

Wegen der offenbar irritierten Rückmeldung des Leistungsempfängers bekam die Behörde Zweifel an der Richtigkeit der Auskunft. Tatsächlich stellte sich die Verwechslung der beiden namens- und geburtstagsgleichen Personen heraus. Die Daten des Kontenabrufes wurden daraufhin aus den Leistungsakten entfernt.

Der Betroffene hatte sich beim Bundeszentralamt für Steuern wegen der Übermittlung seiner Daten beschwert. Das Bundeszentralamt für Steuern teilte dem Beschwerdeführer mit, es lasse sich leider nicht ausschließen, dass bei dem sehr seltenen Fall der Identität von Name und Geburtsdatum mehrerer Personen im Ergebnis eines Kontenabrufes Konten von verschiedenen Personen aufgeführt würden, ohne dass dies erkennbar sei. Die Prüfung der bekannt gegebenen Daten obliege immer der abfragenden, für die Zulässigkeit des Abrufes verantwortlichen Stelle.

Zu dieser Problematik gab es bis dahin und in der Folge keine weiteren Beschwerden bei mir. Eine länderübergreifende Abfrage bei den Landesbeauftragten für den Datenschutz im Jahr zuvor zu Erfahrungen mit dem Kontenabrufverfahren lieferte hierzu auch keine Erkenntnisse.

Das aufgezeigte Problem liegt nicht an den Stellen, die beim Bundeszentralamt für Steuern Anfragen richten. Denn diese Anfragen enthalten die Anschrift der betroffenen Person. Die

Fehleranfälligkeit des weiteren Verfahrens liegt darin begründet, dass das Bundeszentralamt die Kontenklärung ohne Nutzung der Anschrift durchführt. Dieses müsste geändert werden, um das Problem der „Doppelgänger“ zukünftig auszuschließen.

4.8.3
Fehldrucke mit Sozialdaten als Malpapier für Kinder

Ein Fehldruck des Jugendamtes mit Sozialdaten eignet sich nicht als Malpapier.

Ein Zeitungsjournalist gab mir vor Veröffentlichung eines Artikels telefonisch den Hinweis, ihm lägen mehrere Seiten aus Protokollen eines Jugendamtes vor, in denen es um familientherapeutische Gespräche im Rahmen der Erziehungshilfe gehe. Diese Dokumente seien im Jugendamt als Malpapier ausgegeben worden.

Ich habe mich zur Aufklärung des Hinweises unverzüglich mit dem betroffenen Jugendamt in Verbindung gesetzt. Der für das Jugendamt zuständige Dezernent teilte mir mit, es sei richtig, dass ein Fehldruck einer Beratungsvorlage mit personenbezogenen Daten an jemanden geraten sei, der diese der Zeitung zur Verfügung gestellt habe. Da sich der Informant der Zeitung nicht an den Landkreis gewandt habe, lasse sich der genaue Hergang nicht aufklären.

Nach der Darstellung im Zeitungsartikel war die Rückseite eines Fehldruckes mit personenbezogenen Daten als Malunterlage für ein Kind in einem schwierigen Beratungsgespräch zur Verfügung gestellt worden. Nach den internen Ermittlungen des Jugendamtes ließ sich nicht völlig ausschließen, dass eine Mitarbeiterin oder ein Mitarbeiter diesen zu vernichtenden Fehldruck im Bunde mit leeren Blättern als Malunterlage genommen habe, um das Kind zu beruhigen. Es konnte sich jedoch niemand beim Jugendamt an einen solchen Vorfall erinnern.

Die Verantwortlichen des Jugendamtes haben nach dem Vorfall Einzelgespräche geführt und auf die geltenden datenschutzrechtlichen Bestimmungen ebenso hingewiesen wie auf die Verpflichtung zur Einhaltung einer entsprechenden Dienstanweisung zum Umgang mit fallbezogenen Daten in den Sozialen Diensten der Abteilung Kinder- und Jugendhilfe. Zwar ist eine sofortige Vernichtung von Fehldrucken dann nicht immer möglich, wenn Beratungsgespräche unmittelbar aufeinander folgen oder im Zusammenhang mit kurzfristig eingehenden Notfällen. Die Mitarbeiterinnen und Mitarbeiter wurden aber angewiesen,

Fehldrucke, die nicht sofort vernichtet werden können, in abschließbaren Schreibtischen oder Schränken zu verwahren, bis eine Vernichtung möglich ist. Malvorlagen für Kinder gibt es nun nur noch in Form von Malblöcken.

Von einer förmlichen Beanstandung habe ich nach der unverzüglichen und umfassenden Stellungnahme des Jugendamtes abgesehen, da die ergriffenen organisatorischen Maßnahmen umfassend sind und geeignet erscheinen, einen weiteren solchen Vorfall künftig auszuschließen.

4.8.4
Ausgestaltung des Formulars zur Einwilligung des Sozialleistungsempfängers in eine amtsärztliche Untersuchung

Im Rahmen von Eingliederungsmaßnahmen für Sozialleistungsempfänger in den allgemeinen Arbeitsmarkt ist es erforderlich, dass der zuständige Träger über alle erforderlichen Informationen verfügt, um eine größtmögliche Effektivität bei den Vermittlungsbemühungen zu erzielen. Hierzu gehören auch amtsärztliche Untersuchungen sowie die Informationen von anderen Stellen zum Gesundheitszustand des Leistungsempfängers. Allerdings muss dem Betroffenen gegenüber das Verfahren bekannt gemacht und die daran beteiligten Stellen ausdrücklich benannt werden.

Die Beschwerde eines Sozialleistungsempfängers über ein vom KreisJobCenter (KJC) des Landkreises Marburg-Biedenkopf verwendetes Formular, mit dem eine Einwilligung zur Übermittlung medizinischer Daten abgegeben werden sollte, hat meine Dienststelle veranlasst, tätig zu werden. Dabei wurden mit Vertretern des KJC sowohl der praktische Ablauf des konkreten Verfahrens als auch die Inhalte der Einwilligungserklärung besprochen.

Das KJC benötigt zur Beurteilung der Perspektiven von Sozialleistungsempfängern nicht nur die Feststellung über deren Erwerbsfähigkeit, sondern darüber hinaus auch qualifizierte Aussagen über die zeitliche Entwicklung sowie der Art einer möglichen Tätigkeit, die (noch) ausgeübt werden kann.

Feststellungen dieser Art trifft der Fachdienst Gesundheit, der vom KJC beauftragt wird, ein Gutachten zu dem Betroffenen zu erstellen und darüber hinaus Hinweise zu dessen Einsatzfähigkeit zu geben. Die Rechtsgrundlagen hierfür ergeben sich aus den §§ 14 und 15

SGB II, die den Grundsatz des Förderns sowie die Eingliederungsvereinbarungen festlegen. Hinzu kommen Mitwirkungspflichten des Leistungsempfängers, die sich aus § 62 SGB I ergeben.

§ 14 SGB II

Die Träger der Leistungen nach diesem Buch unterstützen erwerbsfähige Hilfebedürftige umfassend mit dem Ziel der Eingliederung in Arbeit. Die Agentur für Arbeit soll einen persönlichen Ansprechpartner für jeden erwerbsfähigen Hilfebedürftigen und die mit ihm in einer Bedarfsgemeinschaft Lebenden benennen. Die Träger der Leistungen nach diesem Buch erbringen unter Beachtung der Grundsätze von Wirtschaftlichkeit und Sparsamkeit alle im Einzelfall für die Eingliederung in Arbeit erforderlichen Leistungen.

§ 15 SGB II

(1) Die Agentur für Arbeit soll mit jedem erwerbsfähigen Hilfebedürftigen die für seine Eingliederung erforderlichen Leistungen vereinbaren (Eingliederungsvereinbarung). Die Eingliederungsvereinbarung soll insbesondere bestimmen,

1. welche Leistungen der Erwerbsfähige zur Eingliederung in Arbeit erhält,
2. welche Bemühungen der erwerbsfähige Hilfebedürftige in welcher Häufigkeit zur Eingliederung in Arbeit mindestens unternehmen muss und in welcher Form er die Bemühungen nachzuweisen hat.

Die Eingliederungsvereinbarung soll für sechs Monate geschlossen werden. Danach soll eine neue Eingliederungsvereinbarung abgeschlossen werden. Bei jeder folgenden Eingliederungsvereinbarung sind die bisher gewonnenen Erfahrungen zu berücksichtigen. Kommt eine Eingliederungsvereinbarung nicht zustande, sollen die Regelungen nach Satz 2 durch Verwaltungsakt erfolgen.

(2) In der Eingliederungsvereinbarung kann auch vereinbart werden, welche Leistungen die Personen erhalten, die mit dem erwerbsfähigen Hilfebedürftigen in einer Bedarfsgemeinschaft leben.

(3) Wird in der Eingliederungsvereinbarung eine Bildungsmaßnahme vereinbart, ist auch zu regeln, in welchem Umfang und unter welchen Voraussetzungen der erwerbsfähige

Hilfebedürftige schadenersatzpflichtig ist, wenn er die Maßnahme aus einem von ihm zu vertretenden Grund nicht zu Ende führt.

§ 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.

Insbesondere im Zusammenhang mit der Erstellung medizinischer Gutachten, der Heranziehung externer Befunde anderer Ärzte sowie der Weitergabe von Ergebnisgutachten an Dritte bedarf es eindeutiger Informationen gegenüber dem Betroffenen. Die Einwilligung zur Heranziehung externer Daten über den Gesundheitszustand des Betroffenen muss konsequenterweise inhaltlich klar und abschließend sein.

Unverbindliche oder gar irreführende Aussagen über die Informationsbeschaffung gehen zulasten des Hilfeempfängers. Das KJC verwendete für die Einwilligung ein Formular, in welchem tatsächlich einige Informationen zur Datenanforderung durch das Gesundheitsamt und zur Übermittlung von Daten an das JobCenter nicht präzise beschrieben waren, so dass man vermuten musste, dass mehr Daten übermittelt wurden, als für die Beurteilung des Sachverhaltes bzw. der Eingliederungsvereinbarung erforderlich war. Beispielsweise war im ursprünglichen Formular formuliert, der Betroffene entbinde seine behandelnden Ärzte u. a. gegenüber dem Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf von der Schweigepflicht. Im Umfang musste die Schweigepflichtsentbindung aber auf die erforderlichen Auskünfte im sachlichen Zusammenhang mit der Feststellung der gesundheitlichen Eignung für den Arbeitsmarkt begrenzt werden.

Im Gespräch vor Ort wurde die Problematik erörtert. Mit meiner Beteiligung ist die Einwilligungserklärung insbesondere hinsichtlich der Erforderlichkeit der Datenerhebung zur rechtmäßigen Aufgabenerfüllung des Job-Centers sowie der Einschaltung Dritter präzisiert worden. Das neue Formular ist nachfolgend abgedruckt.

KreisJobCenter
Marburg-Biedenkopf

Name, Vorname:

Geb.-Datum:

Anschrift:

Telefon:

E I N W I L L I G U N G S E R K L Ä R U N G

Zur Verbesserung der Eingliederungsmaßnahmen in den allgemeinen Arbeitsmarkt und der Hilfen im Rahmen der §§ 14 ff Sozialgesetzbuch (SGB II), insbesondere zur Erstellung einer Eingliederungsvereinbarung gem. § 15 SGB II, ist es erforderlich, dass sowohl die Maßnahme- / Bildungsträger, als auch das KreisJobCenter Marburg-Biedenkopf über alle erforderlichen Informationen rechtzeitig verfügen, um eine größtmögliche Effektivität bei den Vermittlungsbemühungen zu erzielen.

Hiermit entbinde ich den Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf von der ärztlichen Schweigepflicht gegenüber dem KreisJobCenter des Landkreises Marburg-Biedenkopf und ermächtige den Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf, dem KreisJobCenter erforderliche Auskunfte bzgl. meiner gesundheitlichen Eignung zu erteilen..

Gleichzeitig ermächtige ich den Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf, Auskunft über mich bei meinen behandelnden Ärztinnen/Ärzten persönlich, schriftlich oder telefonisch einzuholen, sofern diese Auskünfte zur Begutachtung/Feststellung meiner Eignung für den Arbeitsmarkt bzw. zu Fragen meiner Erwerbsfähigkeit unerlässlich sind.

Meine behandelnden Ärztinnen/Ärzte entbinde ich von der Schweigepflicht gegenüber dem Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf und bin damit einverstanden, dass die erforderlichen Auskünfte über mich an den Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf, Schwanallee 23, 35037 Marburg erteilen und/oder Kopien von Befunden, Arztberichten, Attesten usw. dorthin senden.

Ich bin damit einverstanden, dass im Rahmen der Eingliederung in Arbeit gem. §§ 14 ff SGB II meine personenbezogenen Daten und die Ergebnisse der Begutachtung durch den Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf dem KreisJobCenter Marburg-Biedenkopf durch den Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf mitgeteilt werden und dass bekannte Daten zwischen dem Fachbereich Gesundheit des Landkreises Marburg-Biedenkopf und dem KreisJobCenter untereinander ausgetauscht werden können, soweit diese **zur Feststellung** meiner **gesundheitlichen** Eignung für den Arbeitsmarkt **benötigt werden** bzw. meine Erwerbsfähigkeit betreffen.
Hierzu zählen insbesondere Auskünfte über alle eingliederungsspezifischen Fragestellungen, gesundheitliche Einschränkungen, aktueller Gesundheitszustand, Ergebnisse der Begutachtung/Untersuchung durch den psychologischen Dienst, auch des der Agentur für Arbeit, Eignungsabklärung bei anderen Trägeren (z. B. Kompetenzzentrum Rehabilitation Hessen), der von mir absolvierten Aus- und Fortbildungen sowie frühere Beschäftigungsverhältnisse.

_____ _____

Datum Unterschrift

4.8.5
Informationsanspruch des Personalrats beim betrieblichen Eingliederungsmanagement

Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen arbeitsunfähig, ist vom Arbeitgeber ein betriebliches Eingliederungsmanagement einzuleiten. Der Personalrat kann mit Blick auf seine Überwachungsfunktion von der Dienststellenleitung die namentlich Nennung der betroffenen Beschäftigten verlangen.

Mehrfach bin ich in diesem Jahr von Behörden auf das betriebliche Eingliederungsmanagement angesprochen worden. Diese Maßnahme ist zwar im SGB IX (Rehabilitation und Teilhabe behinderter Menschen) geregelt, thematisch geht es aber in erster Linie um einen Bereich aus dem Personalwesen.

§ 84 Abs. 2 SGB IX

Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, klärt der Arbeitgeber mit der zuständigen Interessenvertretung im Sinne des § 93, bei schwerbehinderten Menschen außerdem mit der Schwerbehindertenvertretung, mit Zustimmung und Beteiligung der betroffenen Person die Möglichkeiten, wie die Arbeitsunfähigkeit möglichst überwunden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz erhalten werden kann (betriebliches Eingliederungsmanagement). Soweit erforderlich wird der Werks- oder Betriebsarzt hinzugezogen. Die betroffene Person oder ihr gesetzlicher Vertreter ist zuvor auf die Ziele des betrieblichen Eingliederungsmanagements sowie auf Art und Umfang der hierfür erhobenen und verwendeten Daten hinzuweisen. Kommen Leistungen zur Teilhabe oder begleitende Hilfen im Arbeitsleben in Betracht, werden vom Arbeitgeber die örtlichen gemeinsamen Service-Stellen oder bei schwerbehinderten Beschäftigten das Integrationsamt hinzugezogen. Diese wirken darauf hin, dass die erforderlichen Leistungen oder Hilfen unverzüglich beantragt und innerhalb der Frist des § 14 Abs. 2 Satz 2 erbracht werden. Die zuständige Interessenvertretung im Sinne des § 93, bei schwerbehinderten Menschen außerdem die Schwerbehindertenvertretung, können die Klärung verlangen. Sie wachen darüber, dass der Arbeitgeber die ihm nach dieser Vorschrift obliegenden Verpflichtungen erfüllt.

Mit der zuständigen Interessenvertretung im Sinne des § 93 SGB IX ist im öffentlichen Dienst der Personalrat gemeint. Bislang, hierauf zielten auch die Anfragen, bestand eine gewisse

Unsicherheit, ob der Personalrat mit Blick auf die in § 84 Abs. 2 Satz 7 (letzter Satz) normierte Überwachungsfunktion gegenüber der Dienststellenleitung einen Anspruch auf namentliche Nennung der betroffenen Beschäftigten hat.

Über diese Frage hat das Bundesverwaltungsgericht nunmehr entschieden. Es hat ein solches Informationsrecht des Personalrats beim betrieblichen Eingliederungsmanagement bejaht (Beschluss vom 23. Juni 2010 – 6 P 8.09, NZA-RR 2010, 554). Das Gericht stellt klar, dass der Personalrat einen Anspruch auf Kenntnis des behördlichen Anschreibens an die betroffenen Beschäftigten hat, denn der Personalrat benötige das Anschreiben der Dienststellenleitung, um überprüfen zu können, ob der Betroffene über das gesetzliche Angebot des betrieblichen Eingliederungsmanagements ordnungsgemäß unterrichtet worden ist (§ 84 Abs. 2 Satz 3 SGB IX).

Im Unterschied zur Kenntnis des Personalrats vom Anschreiben an die betroffenen Beschäftigten begrenzt das Bundesverwaltungsgericht in seiner Entscheidung den Informationsanspruch hinsichtlich des Antwortschreibens der Beschäftigten. Danach hat der Personalrat keinen Anspruch auf Information über die Antwortschreiben der Beschäftigten, die der Durchführung des betrieblichen Eingliederungsmanagements nicht oder nur ohne Beteiligung des Personalrats zugestimmt haben. Das Bundesverwaltungsgericht betont zu Recht, dass das Recht dieser Beschäftigten auf informationelle Selbstbestimmung es verbietet, deren Haltung zum betrieblichen Eingliederungsmanagement und zur Beteiligung des Personalrats zu offenbaren.

Ich habe die anfragenden Stellen auf diese Entscheidung hingewiesen und dass durch diesen Beschluss die Frage des Informationsrechts des Personalrats höchstrichterlich geklärt ist.

4.8.6
Hessische Familienkarte

Die Hessische Staatskanzlei hat den Hessischen Datenschutzbeauftragten bei der Entwicklung der Familienkarte eingebunden. Gesichtspunkte der Datensparsamkeit und des Datenschutzes wurden so von Anfang an berücksichtigt.

Im Mai 2010 wandte sich die Hessische Staatskanzlei mit dem Anliegen an mich, das Projekt Familienkarte Hessen hinsichtlich der Datenschutzgesichtspunkte mit mir abzusprechen.

Familien mit mindestens einem Kind unter 18 Jahren und Wohnsitz in Hessen können die Familienkarte beantragen. Diese eröffnet im Wesentlichen vier Angebotsbereiche:

– Eine **kostenlose Unfallversicherung** für Kinder bis zum Schuleintritt und ggf. ein betreuendes (nicht berufstätiges) Elternteil bis zum 3. Lebensjahr des Kindes. Kooperationspartner ist hier die Sparkassenversicherung.
– Einen **Vermittlungsservice für eine Kinderbetreuung** (Babysitter, Tagesmütter, Au-Pairs, Ferienbetreuung). Hierbei ist die Vermittlung über die ÖRAG Service GmbH unentgeltlich; die Leistung selbst muss bezahlt werden.
– Zahlreiche Partnerunternehmen aus den unterschiedlichsten Bereichen bieten Familienkarteninhabern **Rabatte, Vergünstigungen und Aktionsangebote**.
– Für Fragen rund um die Erziehung können Familienkarteninhaber einen **Onlineratgeber** erhalten und sich an eine **Telefonhotline** wenden.

Die Familienkarte ist auf fünf Jahre befristet und gilt längstens bis zum 18. Geburtstag des jüngsten Kindes.

Der Antrag auf Erteilung der Karte kann sowohl schriftlich als auch via Internet gestellt werden. Im Fall der schriftlichen Antragstellung überträgt die Hessische Staatskanzlei die Daten aus dem Antragsformular in die Datenbank. Die Familienkarten werden im Auftrag der Hessischen Staatskanzlei von einem Unternehmen hergestellt und der Staatskanzlei zugesandt. Diese versendet sie zusammen mit einem Anschreiben an die Antragsteller.

Aus Sicht des Datenschutzes ist relevant, dass die mit der Familienkarte verbundenen Angebote freiwillige Leistungen des Landes sind. Es gibt deshalb keine Rechtsvorschriften, die die Familienkarte und die damit verbundene Erhebung und Weiterverarbeitung von Daten regeln. Als Ermächtigung für die Datenverarbeitung kommt nur die Einwilligung in Betracht (§ 7 Abs. 1 Nr. 3 HDSG).

§ 7 Abs. 1 und 2 HDSG

(1) 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.

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

Um sicherzustellen, dass die Anforderungen einer informierten Einwilligung nach § 7 Abs. 2 HDSG erfüllt werden, hat mich die Hessische Staatskanzlei bei der Ausarbeitung der Datenschutzhinweise und Nutzungsbedingungen beteiligt und meine Anregungen übernommen.

Bei der Eingrenzung der mit dem Antrag erhobenen Daten wurde darauf geachtet, ob das jeweilige Datum für die Verarbeitung tatsächlich erforderlich ist. So wird z. B. nur der Name und das Geburtsdatum des jüngsten Kindes erhoben, weil es für die Frage der Berechtigung (Kind unter 18 Jahre) und Gültigkeitsdauer (maximal bis zum 18. Geburtstag des jüngsten Kindes) erforderlich ist; Geburtsdaten der älteren Kinder oder der Antragsteller werden nicht abgefragt; die Angabe der Alterskategorie der Kinder und der Familiengröße ist freiwillig.

Die von der Hessischen Staatskanzlei im Zusammenhang mit der Familienkarte gespeicherten personenbezogenen Daten dürfen nur hierfür verwendet werden und sind spätestens einen Monat nach Ablauf des Gültigkeitsdatums zu löschen – falls der Antragsteller nicht bis dahin eine Verlängerung beantragt hat, weil die Anspruchsvoraussetzungen weiterhin bestehen.

Die Partner der Familienkarte sollen eine Abfrage auf die Datenbank auslösen können, in der sie Name und Kartennummer der ihnen vorgewiesenen (oder bei einer Internetbestellung mitgeteilten) Familienkarte benennen. Als Antwort sollen sie aber nur „Ja“ oder „Nein“ erhalten (d. h. zu der Kartennummer und dem angegebenen Namen existiert eine gültige Familienkarte oder nicht).

Dieses Verfahren soll auch für das Versicherungsunternehmen gelten. Die Abfrage auf die Datei der Staatskanzlei dient nur der Sicherstellung, dass der Anspruchsteller tatsächlich im Besitz einer Familienkarte ist und daher die Unfallversicherungsoption hat. Im Fall des Unfalls eines Kindes oder der versicherten Betreuungsperson sind zwar erheblich mehr Angaben zur

Abwicklung des Versicherungsfalls erforderlich (z. B. ob es sich tatsächlich um ein Vorschulkind handelt, ob es ein „Unfall“ war, nicht zuletzt auf welches Konto Zahlungen gehen sollen). Diese erhebt das Versicherungsunternehmen allerdings direkt beim Antragsteller. Das Versicherungsunternehmen erhält von der Staatskanzlei über die Abfrage hinaus, ob der Antragsteller eine gültige Familienkarte hat, keine personenbezogenen Daten. Als statistisches Datum wird ihm nur die Gesamtzahl der ausgestellten Familienkarten mitgeteilt.

Bei weiteren Angeboten – wie dem Neugeborenenpaket für Kinder bis 12 Monaten – werden Daten nur dann an Partnerunternehmen weitergeleitet, wenn die Karteninhaber dies ausdrücklich wünschen. Beim Neugeborenenpaket wird dazu bereits bei der Beantragung der Familienkarte ein Zusatzfeld mit diesen Optionen nur geöffnet, wenn Kinder in dem entsprechenden Alter angegeben werden. Für die schriftliche Beantragung liegt eine entsprechende Karte den bei den Elterngeldstellen ausgelegten Flyern zur Familienkarte bei. Das Angebot ist als Option gekennzeichnet und es wird ausdrücklich darauf hingewiesen, dass die Annahme des Angebots keine Voraussetzung für den Erhalt der Familienkarte Hessen ist. In die Übermittlung der Daten (Name, Adresse, E-Mail-Adresse, Name und Geburtsdatum des jüngsten Kindes) muss ausdrücklich eingewilligt werden.

Die Familienkarte ist mit einer GTIN versehen, die die Karte eindeutig identifiziert und auf der Karte als Strichcode aufgedruckt ist. Hierzu hat sich die Staatskanzlei einen Nummernkreis der GTIN reservieren lassen; die GTIN wird fortlaufend vergeben und in der Datenbank bei der Staatskanzlei gespeichert. Dieser Barcode auf der Karte dient dazu, Abläufe an der Kasse zu vereinfachen: In Geschäften kann die Karte an der Kasse über den Scanner gehalten und der Code gelesen werden. Das Kassensystem erkennt die Karte und es ist hinterlegt, dass es sich um eine Familienkarte Hessen handelt. Wenn ein Rabatt gewährt wird, kann er sofort abgezogen werden. Im Unterschied zu einer normalen Kundenkarte hat das Unternehmen jedoch bei der Familienkarte keine personenbezogenen Daten des Kunden gespeichert. Das Unternehmen kann – wie bei anderen Kundenkarten auch – aber theoretisch die Einkäufe unter der Familienkartennummer zu einem Käuferprofil entwickeln. Sobald man dann die Familienkarte an der Kasse benutzt und mit einer EC-Karte bezahlt, könnte das Unternehmen die Verbindung zu einem Kunden herstellen. Insofern gäbe es dann keinen Unterschied zu einer normalen Kundenkarte.

GTIN

Globale Artikelidentnummer; **G**lobal **T**rade **I**tem **N**umber, auch EAN-13 Code (**E**uropean **A**rticle **N**umber, 13-stellig) genannt, ist eine Zahl, die nach bestimmten Regeln aufgebaut ist

und meist als Artikelnummer verwendet wird; bei Lebensmitteln kann man beispielsweise den Hersteller und den Artikel erkennen. Sie ist auf dem Artikel als Strichcode aufgebracht. In den Kassensystemen sind unter der GTIN für Artikel die Bezeichnung und der Preis gespeichert und werden beim Einkauf dann auf der Rechnung ausgewiesen.

Mit der Herstellung der Familienkarten hat die Hessische Staatskanzlei ein Unternehmen beauftragt, während der Versand der Karten von der Staatskanzlei zunächst selbst durchgeführt wurde. Der Kartenhersteller erhielt dafür nur eine Liste der Namen, zugehöriger Kartennummern und GTIN. Die vertraglichen Vereinbarungen verpflichten das Unternehmen, die Daten nur für den Zweck der Herstellung der Karten zu verwenden und sie nach erfolgreicher Herstellung, spätestens vier Wochen nach dem Druck, zu löschen. Seit Mitte Dezember hat die Hessische Staatskanzlei den Kartenhersteller auch mit dem Versand der Karten beauftragt. Hierfür wird ihm eine Liste der Adressdaten zur Verfügung gestellt für die Verwendung und Löschung der Daten gelten die gleichen Restriktionen wie bei den Kartendaten. Die abgeschlossene Vereinbarung erfüllt die Anforderungen des § 4 HDSG.

Damit die Staatskanzlei erkennen kann, welche Teile des Internetangebotes der Familienkarte besonders nachgefragt werden, werden Nutzungsstatistiken erstellt. Diesen liegt eine anonymisierte Auswertung zugrunde, denn die IP-Adresse, mit deren Hilfe die Statistik erstellt wird, ist für diesen Zweck verkürzt gespeichert. Programme zur Reichweitemessung wie beispielsweise Google-Analytics werden nicht verwendet.

Die Zuständigkeit für die Familienkarte wechselt ab dem Kalenderjahr 2011 zum Hessischen Sozialministerium.

5. Kommunale Selbstverwaltungskörperschaften

5.1
Feststellungen aus Prüfungen von Kommunen

Auch dieses Jahr habe ich bei hessischen Kommunen geprüft, ob der technische, organisatorische und vertragliche Rahmen der IT-Infrastruktur die datenschutzrechtlichen Vorgaben einhält. Aufgrund technischer Entwicklungen haben sich neue Fragestellungen ergeben.

In meinem 35. (Ziff. 6.1), 36. (Ziff. 6.1) und 37. (Ziff. 5.1) Tätigkeitsbericht hatte ich über meine Erfahrungen aus Prüfungen bei Kommunen berichtet. In den Prüfungen hatte ich mein Augenmerk auf die IT-Infrastruktur gelegt. Es ging um die Frage, ob die technischen, organisatorischen und vertraglichen Gegebenheiten den datenschutzrechtlichen Vorgaben genügen. Auch im vergangenen Jahr habe ich die Prüfungen fortgeführt. Die Erfahrungen haben wieder ein heterogenes Bild ergeben. Einige Kommunen haben gute Lösungen erarbeitet, während in anderen Fällen an einigen Stellen Anpassungen nötig sind. Es haben sich dabei neue, durch technische Entwicklungen bedingte, Problembereiche ergeben.

5.1.1
Weiterleitung von E-Mails

Die Weiterleitung von E-Mails im Einzelfall durch den Empfänger ist im Prinzip unkritisch. Wenn der Empfänger den Inhalt prüft und in den Fällen, in denen es zulässig ist, die E-Mail weiteren Personen zur Kenntnis gibt, ist dies datenschutzrechtlich nicht zu beanstanden. Die Regeln, die zu beachten sind, sollten allerdings in einer Dienstanweisung genannt sein. Die automatische Weiterleitung von E-Mails kann aber zum Problem werden.

5.1.1.1
Automatische Weiterleitung und der Vertretungsfall

Wenn Beschäftigte im Urlaub oder aus anderen Gründen verhindert waren, wurden E-Mails automatisch an die Vertretung weitergeleitet. Daraus ergeben sich datenschutzrechtlich verschiedene Probleme:

Ist die private Nutzung der dienstlichen E-Mail erlaubt, muss den Beschäftigten bekannt sein, dass die Weiterleitung im Vertretungsfall auch die privaten E-Mails einschließt und sie müssen darin eingewilligt haben.

In einigen wenigen Fällen war die automatische Weiterleitung auch für Postfächer eingerichtet, die vertrauliche E-Mails beinhalteten können. So war in einer Kommune für das Postfach des Personalrats die automatische Weiterleitung der Posteingänge an die namentlichen dienstlichen Postfächer der Mitglieder eingerichtet. Das war problematisch, soweit die Personalratsmitglieder nicht Vollzeit für die Personalratstätigkeit freigestellt waren, sondern auch Aufgaben in Fachämtern ausübten. Im Urlaub oder bei Krankheit erhielt – durch die automatische Weiterleitung der E-Mails – die fachliche Vertretung Zugriff auf den E-Mail-Posteingang des oder der Vertretenen, um die dort eingehenden Vorgänge bearbeiten zu können. Damit war aber auch die Kenntnis von E-Mails verbunden, die nicht an die Fachfunktion, sondern an den Personalrat gerichtet waren. Durch die automatische Weiterleitung an das E-Mail-Postfach des Funktionsinhabers wurden also vertrauliche E-Mails Unbefugten offenbart. Wenn in Dienstvereinbarungen und Dienstanweisungen vorgesehen ist, dass im Vertretungsfall auf namentlich zugeordnete Postfächer zugegriffen wird oder eine Weiterleitung einzurichten ist, darf für Funktionspostfächer selbst keine automatische Weiterleitung vorgesehen werden.

Es gibt in der Regel Funktionspostfächer für Personalräte, Schwerbehindertenvertretung oder Frauenbeauftragte. Für die Funktion von behördlichen Datenschutzbeauftragten sollte ebenfalls ein separates Postfach eingerichtet werden. Dabei muss beachtet werden, dass in einigen Funktionen eine Stellvertretung nur zum Tragen kommt, wenn der Funktionsinhaber verhindert ist (z. B. bei behördlichen Datenschutzbeauftragten).

Funktionspostfächer sollten nicht mit einer automatischen Weiterleitung versehen sein. Der Zugriff sollte technisch durch eine Berechtigung der jeweiligen Funktionsinhaber auf das Funktionspostfach erfolgen. Im Fall von Funktionen, bei denen die Vertretung nur zeitweise den Zugriff auf E-Mails erhalten darf, könnte ein Vertretungspostfach angelegt werden. Dahin kann der Funktionsinhaber dann gezielt eine automatische Weiterleitung vornehmen, wenn er verhindert ist.

5.1.1.2
Automatische Weiterleitung an externe Mail-Adressen

Bei meinen Prüfungen musste ich feststellen, dass in einigen wenigen Fällen Mitarbeiter für ihr dienstliches, persönliches Postfach eine automatische Weiterleitung an ein privates Postfach eingerichtet hatten. Teilweise war es der Wunsch, von zu Hause weiterarbeiten zu können. In anderen Fällen war es jedoch der Wunsch, immer auf dem Laufenden zu sein. Durch die Verbreitung von Mobilfunkgeräten, die auch die Möglichkeit haben, eine Verbindung zum Internet herzustellen oder E-Mails zu empfangen, zeigte sich eine neue Qualität. So hatte ein Bürgermeister mit einem Mobilfunkbetreiber einen Vertrag zu einem Smartphone vom Typ Blackberry geschlossen. Vertragsbestandteil war die Möglichkeit, e-Mails zu empfangen. In dem Wunsch, jederzeit über eingehende E-Mails informiert zu sein, hatte er die automatische Weiterleitung der an ihn gerichteten E-Mails vom Mail-Server der Kommune einrichten lassen.

Die externe Weiterleitung ist problematisch, da der interne Absender nicht davon ausgehen kann, dass seine E-Mail das Verwaltungsnetz verlässt und auf dem Mailserver eines privaten Betreibers gespeichert wird. Ebenso wenig muss dies ein Absender einer anderen Behörde erwarten, der über einen gemeinsamen Dienstleister mit der Kommune E-Mails austauscht. Auch ein Bürger darf davon ausgehen, dass seine E-Mail nicht noch bei einem weiteren privaten Betreiber gespeichert wird.

Soweit ein Zugriff auf E-Mails von zu Hause aus gewünscht wird, um außerhalb der Arbeitszeit weiterarbeiten zu können, sollte dies mit Hilfe eines entsprechend abgesicherten Telearbeitanschlusses realisiert werden.

Bei Smartphones muss eine Lösung gefunden werden, die insbesondere die Kenntnisnahme durch den Anbieter verhindert. Den Einsatz von Blackberrys in der Landesverwaltung hatte ich für E-Mails mit normalem Schutzbedarf akzeptiert, da ein Enterpriseserver zum Einsatz kommt und die Blackberrys Dienstgeräte sind. In diesem Fall werden die E-Mails zwischen dem Server der Verwaltung und dem Blackberry Ende-zu-Ende verschlüsselt übertragen. Eine Kenntnisnahme durch den Betreiber ist nicht möglich.

Solange kein ausreichender Datenschutz gewährleistet wird, ist auf eine automatische Weiterleitung an externe Postfächer zu verzichten. Als eine Maßnahme sollte die technische Möglichkeit deaktiviert werden, die es Benutzern erlaubt automatische Weiterleitungen an externe Postfächer einzurichten.

5.1.2
Dateiablagen für vertrauliche Daten

Ich musste immer wieder feststellen, dass vertrauliche Daten in Verzeichnissen gespeichert werden, auf die neben den fachlich berechtigten Mitarbeitern auch Administratoren zugreifen können. Dabei ist die Zugriffsberechtigung üblicherweise so gestaltet, dass eine Kenntnisnahme durch die Administratoren möglich ist und nicht nachvollziehbar wäre. Dies gilt beispielsweise für Verzeichnisse der Personalverwaltung, des Bürgermeisters oder für Funktionspostfächer von Personalräten und anderen Personen, bei denen Vertraulichkeit vorausgesetzt wird.

Es sollte über technische Lösungen nachgedacht werden, die verhindern, dass Administratoren vertrauliche Daten zur Kenntnis nehmen können. Dafür gibt es zwei Gründe. Zum einen sieht das HDSG angemessene Maßnahmen nach dem Stand der Technik vor und die technische Entwicklung bietet Lösungen (siehe Ziff. 5.1.2.1), die aber in der Umsetzung aufwendig sind. Zum anderen ist mir aus Eingaben bekannt, dass in einigen Kommunen Zerwürfnisse zwischen Administratoren und anderen Teilen der Verwaltung vorkommen, bei denen unberechtigte Zugriffe der Administratoren unterstellt werden.

5.1.2.1
Lösungsmöglichkeiten

Unter den technischen Alternativen gibt es zwei, auf die ich Kommunen bei meinen Prüfungen hingewiesen habe.

Es könnten den Administratoren die Rechte auf Verzeichnisse mit vertraulichen Daten entzogen werden; für die Sicherung und Wiederherstellung dieser Ordner genügt die Systemrolle „Sicherungsoperator“. Zusammen mit einer entsprechenden Protokollierung wären Zugriffe durch Administratoren dann nachvollziehbar. Dazu würde eine regelmäßige Kontrolle der Protokolle gehören.

Alternativ könnten Dateien mit vertraulichem Inhalt verschlüsselt werden. Dazu gibt es auf dem Markt verfügbare Lösungen. Eine Lösung ist als Bestandteil des Windows-Betriebssystems das EFS (Encrypted File System). Um auf die Daten zugreifen zu können, auch wenn der Benutzer sein Passwort vergessen hat, muss ein Recovery-Agent oder Wiederherstellungsagent eingebunden sein. Dies erklärt sich daraus, dass die EFS-Verschlüsselung eine Dateieigenschaft (Attribut des Ordners bzw. Dokuments) ist. Das Passwort des Benutzers ist Bestandteil des Schlüssels. Wird dieses durch einen Administrator

zurückgesetzt, sind alle verschlüsselten Dokumente des Benutzers nicht mehr lesbar. Deshalb wird ein weiterer Benutzer, der Recovery-Agent, durch das Betriebssystem als zugriffsberechtigt eingetragen und es wird für ihn ein eigener Schlüssel mit gespeichert. Falls eine Dateiverschlüsselung die Kenntnisnahme von Daten durch Administratoren verhindern soll, darf das Passwort des Wiederherstellungsagenten den Administratoren nicht bekannt sein.

Wird die Dateiverschlüsselung nicht gewünscht, so sollte über eine Gruppenrichtlinie entweder die Nutzung von EFS gesperrt werden oder alternativ ein Wiederherstellungsagent erstellt und eingebunden werden. Dadurch wird verhindert, dass ein Mitarbeiter eine Datei irrtümlich oder gewollt so verschlüsseln kann, dass der Arbeitgeber darauf keinen Zugriff mehr bekommen kann.

5.2
Aktion „Gelbe Karte“

Bereits bei der Umsetzung des Pilotprojektes sollte die datenschutzrechtliche Ausgestaltung beachtet werden. Eine landesweite Anwendung darf nur auf geeigneter Rechtsgrundlage erfolgen.

Im April 2010 startete das HMDIS gemeinsam mit der Stadt Wiesbaden das Projekt „Gelbe Karte“ als Pilotverfahren. Danach kann die Fahrerlaubnisbehörde (FEB) durch Alkohol-, Drogenmissbrauch oder Gewalttaten auffällig gewordene Personen im Hinblick auf etwaige Wiederholungsfälle bereits warnen, auch wenn fahrerlaubnisrechtliche Maßnahmen (z. B. Anordnung einer medizinisch-psychologischen Untersuchung) noch nicht angezeigt sind.

Das Pilotprojekt ist Teil der Präventionsoffensive des Landes Hessen gegen Gewalt und Alkoholmissbrauch und zielt vornehmlich auf Jugendliche oder junge Erwachsene, da bei diesem Personenkreis der Besitz einer Fahrerlaubnis oftmals ein Statussymbol darstellt und ihr Verlust oder die erheblich verzögerte Erteilung mit einem unliebsamen Imageverlust einhergeht. Betroffen sind jedoch alle strafmündigen Personen, d. h. alle Personen, die das 14. Lebensjahr vollendet haben (§ 19 StGB). Anhand eines mit der Polizei ausgearbeiteten Kataloges, bestehend aus Ordnungswidrigkeits- und Straftatbeständen des Strafgesetzbuches (z. B. Unerlaubtes Entfernen vom Unfallort, Körperverletzung), Straßenverkehrsgesetzes (z. B. Fahren ohne Führerschein, Fahren unter Drogeneinfluss), Straßenverkehrsordnung und

Betäubungsmittelgesetzes (mehrfacher Drogenkonsum) – der Deliktskatalog ist im Einzelnen auf der Internetseite des HMDIS über das Internetportal www.hessen.de einzusehen – informiert die Polizei bei entsprechenden Vorkommnissen die zuständige Fahrerlaubnisbehörde über den Vorfall. Diese entscheidet, ob sie dem Betroffenen die „Gelbe Karte zeigt“, d. h. einen Brief auf gelbem Papier zusendet, mit dem sie in aller Deutlichkeit darauf aufmerksam macht, mit welchen Konsequenzen der oder die Betroffene zu rechnen hat, sollten sich ähnliche Vorkommnisse wiederholen. Die „Gelbe Karte“ stellt jedoch keine Sanktion dar, da sie nicht der Ahndung des Verhaltens dient. Die Informationen der Polizei über die betroffenen Personen und den Vorfall sollen entsprechend § 29 StVG maximal zehn Jahre aufbewahrt werden. Entscheidet die FEB keine „Gelbe Karte“ zu erteilen, werden die Daten unverzüglich gelöscht. Das Projekt soll, bei positiver Evaluierung, auch in anderen Hessischen Städten umgesetzt werden.

So sinnvoll sich das Verfahren für die Praxis auch darstellen mag, gibt es doch datenschutzrechtliche Gesichtspunkte zu beachten, die bereits in der Pilotphase zu berücksichtigen und bei der Entscheidung, ob eine landesweite Übernahme erfolgen soll, zu beurteilen sind.

Rechtlicher Hintergrund der Maßnahme sind §§ 11, 46 FeV, wonach wiederholte Verstöße gegen verkehrsrechtliche und strafgesetzliche Vorschriften die Eignung zum Führen eines Kraftfahrzeuges und somit die Erteilung einer Fahrerlaubnis ausschließen bzw. Auffälligkeiten in körperlicher oder geistiger Hinsicht zu Anordnungen und Auflagen führen können oder, soweit bereits eine Fahrerlaubnis erteilt ist, zu ihrer Entziehung.

§ 11 FeV

(1) Bewerber um eine Fahrerlaubnis müssen die hierfür notwendigen körperlichen und geistigen Anforderungen erfüllen. Die Anforderungen sind insbesondere nicht erfüllt, wenn eine Erkrankung oder ein Mangel nach Anlage 4 oder 5 vorliegt, wodurch die Eignung oder die bedingte Eignung zum Führen von Kraftfahrzeugen ausgeschlossen wird. Außerdem dürfen die Bewerber nicht erheblich oder nicht wiederholt gegen verkehrsrechtliche Vorschriften oder Strafgesetze verstoßen haben, sodass dadurch die Eignung ausgeschlossen wird...

(2) Werden Tatsachen bekannt, die Bedenken gegen die körperliche oder geistige Eignung des Fahrerlaubnisbewerbers begründen, kann die Fahrerlaubnisbehörde zur Vorbereitung von Entscheidungen über die Erteilung oder Verlängerung der Fahrerlaubnis oder über die

Anordnung von Beschränkungen oder Auflagen die Beibringung eines ärztlichen Gutachtens durch den Bewerber anordnen.....

Nach § 2 Abs. 12 Satz 1 StVG hat die Polizei die ihr bekannt gewordenen Informationen über Eignungszweifel (z. B. bei Gewalttätigkeit, Drogenkonsum) an die FEB weiterzugeben.

§ 2 Abs. 12 Satz 1 StVG

Die Polizei hat Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden zu übermitteln, soweit dies für die Überprüfung der Eignung oder Befähigung aus der Sicht der übermittelnden Stelle erforderlich ist. Soweit die mitgeteilten Informationen für die Beurteilung der Eignung oder Befähigung nicht erforderlich sind, sind die Unterlagen unverzüglich zu vernichten.

Bisher dienen der FEB die eingehenden Informationen zur Prüfung, ob und inwieweit Bedenken gegen die Eignung bestehen, um dann ggf. entsprechende Maßnahmen nach §§ 11 ff. FeV zu veranlassen.

Das Pilotprojekt setzt hier – im Rahmen der Gewalt- und Gefährdungsprävention – bereits zu einem früheren Zeitpunkt an, der graduell noch vor der Pflicht zum Handeln nach der FeV liegt, aber dennoch bereits erkennen lässt, dass das Verhalten des Betroffenen in eine Richtung führt, aus der sich im Wiederholungsfall eine gesteigerte Gefährdung und Bedrohung bei einer Teilnahme im Straßenverkehr i. S. d. Deliktkataloges verwirklichen kann. Eine rechtliche Wirkung entfaltet die „Gelbe Karte“ nicht. Da alle strafmündigen Personen betroffen sein können, können auch Daten Jugendlicher ab 14 Jahren an die FEB übermittelt werden.

Diese Personen sind teilweise noch nicht im Besitz eines Führerscheins bzw. ist es nicht ohne Weiteres absehbar, ob und wann sie eine Fahrerlaubnis beantragen werden. Der frühstmögliche Zeitpunkt mit der FEB in Kontakt zu treten ist zurzeit die Beantragung einer Prüfbescheinigung für Mofas ab dem 15. Lebensjahr, § 10 FeV. Auch bei einer 14-Jährigen, polizeilich auffällig gewordenen Person kann deshalb eine Warnung durch die „Gelbe Karte“ im Hinblick auf die angestrebte eigene Mobilität wirksam sein.

Insoweit halte ich die Datenübermittlung der Polizei an die FEB für datenschutzrechtlich verhältnismäßig und unter Präventionsgesichtspunkten auch angemessen.

Allerdings erscheint mir die Vorgabe zur Datenspeicherung analog § 29 StVG bis zu zehn Jahren problematisch. § 29 StVG betrifft die Tilgung der im Verkehrszentralregister eingetragenen rechtskräftigen Entscheidungen. Eine so langfristige Speicherung der Daten, die nur zu einer „Gelben Karte“ führte, ist weder erforderlich noch verhältnismäßig. Zum einen wird mit ihr kein Verwaltungsverfahren in Gang gesetzt, das eine entsprechend lange Speicherung auslösen würde, zum anderen werden die Daten schlichtweg so lange nicht benötigt.

Angemessen erscheint ein Zeitraum von maximal drei Jahren. Wird in dieser Zeit ein weiterer Vorfall gemeldet, der ebenfalls zu einer „Gelben Karte“ führt, verlängert sich die Frist um weitere drei Jahre. Werden innerhalb des Speicher-Zeitraumes fahrerlaubnisrechtliche Maßnahmen beantragt oder erforderlich (z. B. Antragstellung auf Erteilung einer Fahrerlaubnis oder Anforderung einer MPU) kann die FEB im Rahmen dieses Verwaltungsverfahrens prüfen, ob und in wieweit die gespeicherten Daten noch Wirkung entfalten. Wenn nach einer „Gelben Karte“ drei Jahre lang kein weiterer Vorfall mehr gemeldet ist, hat auch die „Gelbe Karte“ keine Wirkung mehr und die Daten (Information der Polizei sowie die „Gelbe Karte“) sind zu löschen.

Zudem ist die Zweckbindung der Daten strikt zu beachten, d. h. es ist sicherzustellen, dass die Daten ausschließlich im Rahmen der erforderlichen Prüfung der Erteilung einer Fahrerlaubnis verwendet werden. Eine Weitergabe an andere Ämter, wie z. B. Jugendamt ist unzulässig.

Sollte das Verfahren die Pilotphase verlassen und landesweit ausgedehnt werden, muss eine eigenständige Rechtsgrundlage – evtl. auch auf Bundesebene, da das Verfahren auch in anderen Bundesländern pilotiert wird – herbeigeführt werden, die auch eine einheitliche Anwendung des Verfahrens in den Fahrerlaubnisbehörden gewährleistet.

5.3
Beanstandung wegen unzulässiger Datenübermittlung an den Lahn-Dill-Kreis

Die übermittelnde Behörde ist für die Zulässigkeit der Datenübermittlung – ohne Ansehen der betroffenen Person – verantwortlich. Eine unzulässige Datenübermittlung liegt insbesondere vor, wenn sie initiativ erfolgt, obwohl ein Ersuchen Voraussetzung ist, wenn sie trotz gesetzlichen Ausschlusses erfolgt und wenn löschungsreife Daten und Hinweise weitergegeben werden.

Zwischen dem Beschwerdeführer und verschiedenen Abteilungen des Landrats des Lahn-Dill-Kreises sowie des Kreisausschusses ist es in den vergangenen Jahren zu verschiedenen Ordnungswidrigkeits-, Klage- und Beschwerdeverfahren gekommen. Bei der Fahrerlaubnisbehörde (FEB) des Lahn-Dill-Kreises war der Betroffene wegen verschiedener Verstöße gegen verkehrsrechtliche Vorschriften aufgefallen. Die Vorfälle gehen bis 1998 zurück. Zum Entzug der Fahrerlaubnis kam es jedoch nicht, da der dafür notwendige Punktestand nie ganz erreicht wurde.

Gleichwohl nahm die FEB einen Hinweis des Bürgermeisters einer kreisangehörigen Stadt, der gegen den Beschwerdeführer in anderer Sache eine Strafanzeige wegen § 315b StGB (Gefährlicher Eingriff in den Straßenverkehr) gestellt hatte, zum Anlass, erneut die Eignung des Beschwerdeführers zum Führen eines Kfz zu überprüfen. Zu diesem Zweck forderte eine Mitarbeiterin der FEB bei der zuständigen Staatsanwaltschaft die entsprechende Ermittlungsakte an. Aus der Akte konnte sie allerdings keine Erkenntnisse gewinnen, aufgrund derer eine fahrerlaubnisrechtliche Maßnahme angezeigt gewesen wäre. Sie teilte der Staatsanwaltschaft aber schriftlich mit, dass es sich bei dem Beschwerdeführer um einen „uneinsichtigen Mehrfachtäter“ handele und ein öffentliches Interesse an der Strafverfolgung bestehe. Zum Nachweis ihrer Behauptung fügte sie eine tabellarische Übersicht aller bei der FEB aktenkundigen Verstöße nach dem örtlichen Fahrerlaubnisregister der letzten elf Jahre bei, ungeachtet der Tatsache, dass für die meisten der Vorfälle bereits die gesetzliche Tilgungsreife eingetreten und sie aus den Verkehrsregistern gelöscht waren. Dass es sich im Wesentlichen um tilgungsreife Eintragungen handelte, war der Mitarbeiterin dabei bewusst, denn sie wies die Staatsanwaltschaft ausdrücklich auf diesen Umstand hin. Außerdem fügte sie an, dass „aufgrund der Vorgeschichte und Grundeinstellung des (Name des Betroffenen) bezüglich verkehrsrechtlicher Vorschriften oder Strafgesetze ein öffentliches Interesse an der Strafverfolgung des anhängigen Verfahrens“ bestehe. Die Staatsanwaltschaft sah trotz dieses Hinweises nach § 153 Abs. 1 StPO von der Strafverfolgung ab, da die Schuld des Beschwerdeführers gering und ein öffentliches Interesse, das die Strafverfolgung geboten hätte, nicht gegeben war.

Der Beschwerdeführer bat mich um eine datenschutzrechtliche Überprüfung des Vorgangs, da er in der Datenübermittlung einen rechtsgrundlosen, unzulässigen Eingriff in das seinerzeit laufende Ermittlungsverfahren sah. Wegen der langjährigen Streitigkeiten in anderer Angelegenheit zwischen ihm und dem Landrat sei die Datenübermittlung nur zu dem Zweck erfolgt, den Beschwerdeführer bei der Staatsanwaltschaft zu diskreditieren.

Zur Stellungnahme aufgefordert, bestand der Landrat durch den zuständigen Abteilungsleiter darauf, dass die Mitteilungen seiner Mitarbeiterin an die Staatsanwaltschaft „entsprechend der Regeln der Strafprozessordnung“ erfolgt seien und es sich deshalb auch um eine zulässige Datenübermittlung handle. Schließlich habe man ausdrücklich darauf hingewiesen, „dass aufgrund der gesetzlich eingetretenen Tilgungsreife ein großer Teil der Vorfälle bereits gelöscht ist“. Gleichzeitig beklagte er seinerseits, dass der Beschwerdeführer bzw. dessen Bevollmächtigter in anderen Angelegenheiten erfolgreiche Mitarbeiter seiner Behörde diskreditiere. Er bot mir an, detailliert zu der umfangreichen Befassung der Fachdienste des Lahn-Dill-Kreises mit den Belangen des Beschwerdeführers zu berichten. Dieses Angebot habe ich nicht wahrgenommen, sondern die Rechtslage des relevanten Vorganges geprüft.

Zur Erfüllung ihrer Verwaltungsaufgaben speichert die örtliche Fahrerlaubnisbehörde die erforderlichen personenbezogenen Daten von Fahrerlaubnisbewerbern, -inhabern und solchen Personen, denen ein Verbot erteilt wurde ein Fahrzeug zu führen, in örtlichen Fahrerlaubnisregistern und führt dazu gehörende Akten mit den papiernen Unterlagen. Im Register werden dabei die sog. „positiven Daten“ zum Besitz einer Fahrerlaubnis, wie z. B. Angaben zur Person, Gültigkeitsdaten usw. gespeichert. Bis zum abschließenden Aufbau der zentralen Verkehrsregister beim KBA dürfen FEB übergangsweise auch sog. „Negativdaten“, wie z. B. Punkte, rechtskräftige Entscheidungen speichern, da sie diese zu ihrer eigenen Aufgabenerfüllung benötigen und im zentralen Register noch keine vollständige zentrale Datenerfassung gewährleistet ist, § 57 FeV i. V. m. § 50 StVG. Ein Datenabruf beim Zentralregister wäre zurzeit ggf. noch unvollständig. In den entsprechenden Akten werden die angefallenen papiernen Unterlagen aufbewahrt.

Datenschutzrechtliche Gesichtspunkte bzgl. der Datenverarbeitung sind im Wesentlichen bereichsspezifisch im Straßenverkehrsgesetz (StVG) und der Fahrerlaubnisverordnung (FeV) geregelt.

So bestimmt § 60 StVG, dass Datenübermittlungen aus den (örtlichen) Fahrerlaubnisregistern nur auf Ersuchen zulässig sind, es sei denn, es existiert eine besondere Rechtsvorschrift, die eine Datenübermittlung von Amts wegen bestimmt.
Für die Verfolgung von Straftaten und Ordnungswidrigkeiten dürfen zudem nur die sog. „positiven Daten“ übermittelt werden, § 58 FeV i. V. m. § 52 Abs. 1 Nr. 1 StVG.

Die FEB des Lahn-Dill-Kreises hat durch die Übersendung des Schreibens an die Staatsanwaltschaft gegen beide Vorschriften verstoßen. Die das Ermittlungsverfahren führende Staatsanwaltschaft hat weder ein Ersuchen gestellt noch ist eine Rechtsvorschrift

ersichtlich, nach der die Übermittlung von Amts wegen zulässig gewesen wäre. Die FEB hat vielmehr die Daten aus eigener Initiative an die StA übermittelt, nachdem die Prüfung der Ermittlungsakte keine Anhaltspunkte ergeben hat, eigene fahrerlaubnisrechtliche Maßnahmen wegen Eignungszweifeln gegen den Beschwerdeführer zu ergreifen. Mit der Mitteilung aller aktenkundigen Vorfälle und Maßnahmen an die Staatsanwaltschaft hat die FEB zudem Daten übermittelt, die nicht hätten übermittelt werden dürfen, da es sich um sog. „Negativdaten" handelte. Dies gilt auch für ihre beigefügte Wertung sowohl zur Person des Betroffenen („uneinsichtiger Mehrfachtäter") als auch zum Verlauf des Ermittlungsverfahrens („Aufgrund Vorgeschichte und Grundeinstellung ... besteht ein öffentliches Interesse an der Strafverfolgung"). Erschwerend kommt hinzu, dass die FEB die Tilgungsfristen der Eintragungen unbeachtet ließ und die Staatsanwaltschaft absichtlich auch über die Vorfälle informierte, die zu löschen waren. Tilgung bedeutet Löschung, Entfernung oder Unkenntlichmachung eines Eintrags nach einem bestimmten Zeitablauf. Für den zugrunde liegenden Sachverhalt besteht ein Verwertungsverbot und ein Übermittlungsverbot, § 29 Abs. 7 und 8 StVG. Daran hat sich die FEB nicht gehalten, als sie löschungsreife personenbezogene Daten übermittelte und nur auf die Tilgungsreife hinwies.

Im folgenden Schriftwechsel war die Leitung der FEB des Lahn-Dill-Kreises weder in der Lage eine Rechtsgrundlage für ihr Vorgehen zu benennen, noch erkannte sie die Unzulässigkeit der Datenübermittlung an. Ich habe deshalb eine Beanstandung nach § 27 HDSG ausgesprochen. In der gesetzlich vorgesehenen Stellungnahme zur Beanstandung erklärte der Landrat zwar diese zukünftig zu beachten, wies aber gleichzeitig darauf hin, dass er meine Rechtsauffassung nicht teile. Er kündigte an, auch in zukünftigen vergleichbaren Fällen der Strafanzeige einer seiner Aufsicht unterliegenden Straßenverkehrsbehörde „beizutreten", Hinweise zum Maß der Schuld des Beschuldigten sowie Erklärungen zum besonderen öffentlichen Interesse an der Strafverfolgung abzugeben. Allerdings würde er dann auf die vorhandene Fahrerlaubnisakte hinweisen und der Strafverfolgungsbehörde die Einsichtnahme empfehlen. Es sei schließlich Sache der Staatsanwaltschaft sich damit auseinanderzusetzen, inwieweit der Inhalt der Fahrerlaubnisakte aufgrund von Löschungsvorschriften Berücksichtigung finde. Deswegen müsse eine Fahrerlaubnisakte vor ihrer Übersendung auch nicht auf etwaige zu löschende Inhalte überprüft werden.

Diese Ansichten sind unzutreffend. Einen Beitritt zur Strafanzeige einer anderen Person sieht das Gesetz nicht vor. Der Landrat war am Verfahren in keiner Weise beteiligt oder involviert. Auch sieht gesetzmäßiges Verwaltungshandeln es nicht vor, unbeachtet datenschutzrechtlicher Vorschriften Datenübermittlungen vorzunehmen, selbst wenn es zu Diskreditierungen von Mitarbeitern der Verwaltung durch den Betroffen gekommen ist.

Die FEB speichert in ihren Akten und Registern nur solche personenbezogene Daten, die zur Aufgabenerfüllung erforderlich sind. Daten, die nach den Vorschriften des StVG und der FeV zu löschen sind, sind für die Zwecke der FEB (z. B. Beurteilung der Eignung und Prüfung der Befähigung zum Führen eines Kfz, Ahndung von Verstößen usw.) nicht mehr zu verwerten und daher nicht mehr erforderlich. Ihre Weiterverarbeitung und somit auch ihre Übermittlung sind unzulässig. Solche Daten und Hinweise sind – spätestens bei Wiederbefassung mit der Akte – aus dem örtlichen Register zu entfernen oder als gelöscht zu kennzeichnen.

Die FEB des Lahn-Dill-Kreises ist als „Herrin der Daten“ für die Zulässigkeit einer Datenübermittlung aus ihrem Datenbestand verantwortlich. Sie hat vor einer Weitergabe der Daten zu prüfen, ob

– sie selbst zur Datenübermittlung berechtigt ist,
– die Daten für die empfangende Stelle erforderlich sind und
– die betroffenen Daten übermittlungsfähig sind.

Im Fall einer initiativen Datenübermittlung ist die Verantwortung besonders hoch, da sie die personenbezogenen Daten absichtlich und zielgerichtet in die Sachbehandlung einer anderen Verwaltung einspeist, ohne dass diese an der Übermittlung mitwirkt. Zudem hat die Prüfung der Zulässigkeitsvoraussetzungen ohne Ansehen der betroffenen Person zu erfolgen. Die Tatsache, dass eine Person mit der übermittelnden Stelle im Streit liegt, darf nicht dazu führen, dass gesetzmäßiges Verwaltungshandeln ausgesetzt wird.

Abgesehen davon, dass die FEB im vorliegenden Fall weder initiativ tätig werden durfte, noch die sog. „Negativdaten“ an die Staatsanwaltschaft hätte übermitteln dürfen, hätte sie auch nicht die Prüfung etwaiger eingetretener Tilgungsfristen der Datenempfängerin überlassen dürfen. Übermittlungsverbote sind von der übermittelnden Stelle zu prüfen und zu beachten. Die empfangende Dienststelle trägt ihrerseits (nur) die Verantwortung für die weitere Bearbeitung der übermittelnden Daten.

Meine Möglichkeiten die Behörde zu datenschutzgemäßem Verwaltungshandeln anzuhalten, sind mit dem Mittel der Beanstandung ausgeschöpft. Hier sollte deshalb die Fachaufsicht tätig werden.

5.4
Übermittlung von Bürgerdaten durch einen Bürgermeister an das Kreisgesundheitsamt

Eine Einschaltung des Gesundheitsamtes in umfänglichen Nachbarschaftsstreitigkeiten durch den Bürgermeister als Leiter der Ortspolizeibehörde bzw. den Gemeindevorstand als Kollegialorgan ist grundsätzlich rechtlich möglich. Dies schließt auch die Übermittlung der für ein Tätigwerden erforderlichen Daten ein. Allerdings muss eine derartige Beauftragung gewisse formale Voraussetzungen erfüllen.

Eine Einwohnerin einer hessischen Kommune erhielt eine Einladung zu einem persönlichen Beratungsgespräch beim Gesundheitsamt, ohne dass sie selbst bisher irgendwelche Kontakte mit dem Gesundheitsamt hatte. Auf die Nachfrage beim Gesundheitsamt, warum die Kontaktaufnahme überhaupt erfolgt sei, hat sich das Amt auf die Vertraulichkeit der ihm vorliegenden Informationen (Informantenschutz) berufen und eine Auskunft verweigert.

Daraufhin bat mich die Bürgerin um Unterstützung, ihr Auskunftsbegehren durchzusetzen. Sie vermutete, dass das Tätigwerden des Amtes auf Anzeigen von Nachbarn zurückzuführen sei, mit denen sie eine Auseinandersetzung in einer baurechtlichen Angelegenheit hat.

Meine Recherchen ergaben, dass der Bürgermeister bzw. der Gemeindevorstand der Gemeinde zur Vermittlung in diesem baurechtlichen Nachbarschaftskonflikt Unterstützung beim sozialpsychiatrischen Dienst des Gesundheitsamtes gesucht hat. Dazu wurden an das Gesundheitsamt Informationen aus dem Nachbarschaftskonflikt übermittelt. Zuvor hatte der Bürgermeister selbst vergeblich versucht, in dem Konflikt zu vermitteln. Der Bürgermeister sah dieses Hilfsersuchen als informelle Hilfeleistung an, während das Gesundheitsamt davon ausging, dass es sich um eine offizielle Beauftragung handele.

Aus datenschutzrechtlicher Sicht stellten sich für mich zwei Themenkomplexe:
– Umfang des Auskunftsrechts der Betroffenen gegenüber dem Gesundheitsamt und
– Zulässigkeit der Einschaltung des Gesundheitsamtes.

5.4.1
Umfang des Auskunftsrechts

Das Gesundheitsamt hatte ein Akteneinsichtsrecht bzw. einen Auskunftsanspruch der Bürgerin nur in Bezug auf die Schreiben des Amtes an die Bürgerin selbst für rechtlich geboten gesehen. Alle übrigen Schreiben, Vermerke etc. seien geistiges Eigentum der Verfasser und deshalb dem Einsichts- bzw. Auskunftsrecht der Bürgerin entzogen.

Diesen Ausführungen habe ich nachdrücklich widersprochen.

Gesetzliche Grundlage für die Tätigkeit der Gesundheitsämter ist das HGöGD vom 28. September 2007 (GVBl. I S. 659). Gem. § 18 Abs. 4 HGöGD sind die Bestimmungen des HDSG ergänzend anzuwenden. Nach § 18 Abs. 5 HDSG kann der Betroffene bei der speichernden Stelle Einsicht in die Akten verlangen, die zu seiner Person dort geführt werden. Dieses Akteneinsichtsrecht ist grundsätzlich umfassend und unterliegt allenfalls dann Einschränkungen, wenn personenbezogene Daten Dritter oder geheimhaltungsbedürftige, nicht personenbezogene Daten in der Akte enthalten sind. Personen, die – wie hier – in amtlicher Funktion tätig werden, sind nicht Dritte im Sinne dieser Vorschrift. Andere Gründe für eine Einschränkung des Akteneinsichtsrechts waren im vorliegenden Fall nicht ersichtlich, so dass ich gegenüber der Behörde vorgetragen habe, dass der Bürgerin ein umfassendes, uneingeschränktes Recht auf Einsicht in alle Unterlagen zu gewähren ist. Dabei habe ich hervorgehoben, dass dies auch Aktenvermerke und Notizen betrifft. Das Anlegen von „Nebenakten“ und deren Geheimhaltung gegenüber dem Betroffenen widerspricht dem mit § 18 HDSG angestrebten Ziel der Transparenz der Datenverarbeitung für die Betroffenen. Die Behörde hat daraufhin eine umfassende Akteneinsicht gewährt.

5.4.2
Zulässigkeit der Einschaltung des Gesundheitsamtes

Eine Einschaltung des Gesundheitsamtes in umfänglichen Nachbarschaftsstreitigkeiten durch den Bürgermeister als Leiter der Ortspolizeibehörde bzw. den Gemeindevorstand als Kollegialorgan ist grundsätzlich rechtlich möglich. Dies schließt auch die Übermittlung der für ein Tätigwerden des Gesundheitsamtes erforderlichen Daten ein. Allerdings muss eine derartige Beauftragung gewisse formale Voraussetzungen erfüllen. So halte ich eine telefonische Beauftragung grundsätzlich nicht für zulässig. Die Vorgehensweise der Verwaltung muss für die Betroffenen nachvollziehbar sein. Dazu gehört aus meiner Sicht zunächst eine schriftliche Beauftragung durch den Bürgermeister bzw. den Gemeindevorstand, aus der sich ergibt, aus welchen Gründen das Gesundheitsamt tätig werden soll. Es muss für die Betroffenen bei einer Akteneinsicht erkennbar sein, wer in

welcher Rolle das Gesundheitsamt kontaktiert hat und zu welchem Zweck dieser Kontakt erfolgte. Dies kann einmal die Bitte nach Moderation zwischen den streitenden Nachbarn sein oder ein spezieller Auftrag an das Gesundheitsamt, tätig zu werden. Dies war im vorliegenden Fall nicht erfolgt. Es wurden sensitive Daten über die Betroffene an das Gesundheitsamt weitergegeben. Dabei war offensichtlich nicht einmal zwischen den beteiligten Behörden klar, um welche Art der Beauftragung es sich handelte. Diese Vorgehensweise habe ich unter datenschutzrechtlichen Erwägungen für unzulässig gehalten, da sie Interessen der betroffenen Personen massiv beeinträchtigt. Die beteiligten Stellen wurden entsprechend belehrt.

5.5
Neue Saisonkarten für Schwimmbäder

Vor der Einführung einer neuen Technik ist grundsätzlich zu prüfen, welche Informationen ein System für die Umsetzung der gestellten Aufgabe wirklich benötigt. Maßstab muss immer die Erforderlichkeit sein und nicht die Vorgaben der Lieferfirma.

Durch eine Anfrage wurde ich darauf aufmerksam, dass eine hessische Kommune eine neue Saisonkarte für die örtlichen Freibäder eingeführt hatte, die neben einem Barcode das Foto des Inhabers, seine Anschrift und das Geburtsdatum enthielt. Bei jedem Besuch eines Schwimmbades wurde die Saisonkarte gescannt. Auf Nachfrage gab das Kassenpersonal die Auskunft, dass man mit diesem System auswerten könne, welche Person woher zum Schwimmbad gekommen sei. Für eine solche Kontrolle seiner Schwimmbadbesuche zeigte der Bürger wenig Verständnis.

Rückfragen bei der betroffenen Kommune ergaben, dass die Grundvorgaben der Lieferfirma des Zugangssystems ohne Prüfung der Erforderlichkeit übernommen wurden und der geschilderte Datenumfang für jede Saisonkarte erhoben und auf dem Ausweis gespeichert wurde.

Nach § 11 HDSG ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur rechtmäßigen Erfüllung einer Aufgabe erforderlich ist. Nach § 10 Abs. 2 HDSG ist für die automatisierte Verarbeitung personenbezogener Daten dasjenige Verfahren auszuwählen oder zu entwickeln, welches geeignet ist so wenig personenbezogene Daten zu verarbeiten wie zur Erreichung des angestrebten Zwecks erforderlich ist. Für den regelmäßigen Besuch

eines Schwimmbades muss das Schwimmbadpersonal keine Detailinformationen über jeden Badegast haben.

Nach längeren Verhandlungen wurde das neue Zugangssystem den datenschutzrechtlichen Anforderungen angepasst. Hierbei wurden folgende Änderungen umgesetzt:

– Die neuen Saisonkarten enthalten nur noch ein Bild des Kartenbesitzers, um eine unberechtigte Weitergabe der Karte auszuschließen, die Kundennummer und einen Barcode. Dieser verschlüsselt ausschließlich, wann und an welcher Verkaufsstelle die Saisonkarte gekauft oder verlängert wurde sowie die Kundennummer.

– Der Name, die Adresse und die Kundennummer des Saisonkarteninhabers werden auf einem Server im Rathaus gespeichert, um gestohlene oder verlorengegangene Saisonkarten einer Person zuordnen zu können, denn die wenigsten Badegäste kennen ihre Kundennummer. Alle anderen freiwilligen Angaben wie das Geburtsdatum und die Kommunikationsdaten werden ausschließlich in Papierform in einem Aktenordner im Rathaus aufbewahrt.

– Betritt ein Badegast das Schwimmbad, wird durch das Scannen des Barcodes die Ausweisnummer gespeichert und für einige Zeit gesperrt, um zu verhindern, dass die Saisonkarte durch weitere Personen unberechtigt genutzt wird.

– Gleichzeitig hält das System die Anzahl der Personen fest, die das Schwimmbad betreten haben, um zeitnah die erforderliche Zuteilung von Aufsichtspersonal zu veranlassen bzw. für die Einhaltung der korrekten Wasserqualität zu sorgen. Nur beim Badesee muss die Saisonkarte auch beim Verlassen des Geländes gescannt werden, da hier häufiger die mögliche Gesamtbesucherzahl überschritten wird und der Zugang zum See dann geschlossen werden muss.

– Beim Verlust einer Saisonkarte wird nach einer entsprechenden Anzeige die Kartennummer gesperrt und der Karteninhaber erhält gegen Zahlung der Verwaltungsgebühr eine Ersatzkarte mit einer neuen Kundennummer.

Die durch das Scannen der Saisonkarten gewonnenen Informationen können für statistische Auswertungen genutzt werden, um z. B. die tatsächlichen Besucherzahlen der verschiedenen Schwimmbäder zu ermitteln. Darüber hinaus wurde zugesagt, dass die Schwimmbadmitarbeiter geschult werden, damit sie über die datenschutzrechtlichen Aspekte

beim Umgang mit der Saisonkarte informiert sind. Zusätzlich werden entsprechende Aushänge an den Schwimmbädern angebracht.

5.6
Abgleich von Fahrzeughalterdaten mit der Hundesteuerdatei einer Kommune

Wenn mehrere Ordnungswidrigkeiten gleichzeitig begangen werden, darf eine Verknüpfung der gewonnenen Informationen, z. B. durch den Abgleich mit der Hundesteuerdatei einer Kommune nur erfolgen, wenn dies zur Aufklärung der Ordnungswidrigkeiten erforderlich ist.

Ein Bürger bat mich um rechtliche Prüfung seines mit einer Kommune geführten Schriftverkehrs. Der Beschwerdeführer wurde durch einen Ordnungspolizeibeamten einer Kommune mit einem Hund angetroffenen, der trotz einer in dieser Gemarkung bestehenden Anleinpflicht frei herumlief. Der Ordnungspolizeibeamte wies auf die Anleinpflicht hin, verwarnte den Betroffenen mündlich und händigte ihm eine entsprechende Info-Broschüre aus. Gleichzeitig fragte er den Betroffenen, ob ein im Feld abgestelltes Fahrzeug ihm gehöre, was dieser verneinte. Der Ordnungspolizeibeamte notierte sich daraufhin das amtliche Kennzeichen des Fahrzeugs, ermittelte in der Dienststelle den Fahrzeughalter und stellte eine Verwarnung aus. Zusätzlich glich er das Ergebnis der Halteranfrage mit der Hundesteuerdatei der Kommune ab, um dabei festzustellen, dass der mündlich verwarnte Hundehalter und der Fahrzeughalter dieselbe Person waren.

Meine datenschutzrechtliche Prüfung ergab, dass die mündliche Verwarnung eines Hundehalters und die Ermittlung des Fahrzeughalters rechtmäßig waren. Der Abgleich des Ergebnisses der Halteranfrage mit der Hundesteuerdatei hatte jedoch nur das Ziel, dem Ordnungspolizeibeamten seine Vermutung zu bestätigen, dass er von dem verwarnten Hundehalter falsch informiert wurde. Diese Information konnte keine weiteren Konsequenzen haben, da der Hundehalter bereits mündlich verwarnt worden war und das falsch geparkte Fahrzeug unabhängig davon ein gesondertes Ordnungswidrigkeitenverfahren anhand des amtlichen Kennzeichens nach sich zog.

Nach § 4 Abs. 1 Nr. 1 b) KAG gelten für die Hundesteuer die Vorschriften des § 30 AO zum Steuergeheimnis. Nach § 4 Abs. 1 Nr. 1 b) bb) KAG darf nur in Schadensfällen Auskunft über Namen und Anschrift eines Hundehalters an Behörden oder Schadensbeteiligte erteilt werden. Da durch die Verletzung der Anleinpflicht kein Schaden entstanden war, wurde durch den

Abgleich der Halteranfrage mit den Daten der Hundesteuerstelle gegen das Steuergeheimnis nach § 30 AO verstoßen. Über das Ergebnis meiner Prüfung habe den Betroffenen informiert. Die Kommune habe ich aufgefordert, die Rechtslage künftig zu beachten.

5.7
Datenübermittlung zur Nachwuchswerbung der Freiwilligen Feuerwehren

Die Arbeit der Freiwilligen Feuerwehr dient der langfristigen Sicherung des Brandschutzes einer Kommune. Daher ist für eine Mitgliederwerbeaktion eine Übermittlung personenbezogener Daten aus dem Einwohnermelderegister zulässig.

Immer wieder fragen Kommunen nach, ob sie ihrer Freiwilligen Feuerwehr oder anderen Vereinen zur Nachwuchswerbung die Adressdaten von Kindern und Jugendlichen übermitteln dürfen. Nach § 34 Abs. 3 HMG darf eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) nur erteilt werden, wenn die Auskunft im öffentlichen Interesse liegt. Ein öffentliches Interesse liegt nur dann vor, wenn die Auskunft für Belange der Allgemeinheit wichtig ist und nicht nur Interessen von Einzelnen nützt.

Grundsätzlich habe ich in den letzten Jahren bei der Abwägung zwischen den Interessen der Betroffenen und der Vereine allen Anfragen zur Mitgliederwerbung ein öffentliches Interesse abgesprochen und den Kommunen empfohlen, für Vereine, die z. B. aufgrund ihrer Jugendarbeit unterstützt werden sollen, die sog. „Konsulatslösung“ anzuwenden. Hierfür stellen die Vereine der Gemeindeverwaltung die entsprechenden Werbebriefe zur Verfügung. Die Gemeinde ergänzt die Briefumschläge mit den Namen und Adressen der gewünschten Zielgruppe und versendet diese. So können für den Verein interessante Personen angesprochen werden, ohne personenbezogene Daten an Vereine zu übermitteln.

Für die Freiwilligen Feuerwehren ist ein öffentliches Interesse an der Mitgliederwerbung jedoch anzunehmen, da die langfristige Sicherstellung des Brandschutzes für die Kommunen eine gesetzliche Verpflichtung nach § 3 HBKG ist.

§ 3 Abs. 1 und 2 HBKG

(1) Die Gemeinden haben zur Erfüllung ihrer Aufgaben im Brandschutz und in der Allgemeinen Hilfe

1. in Abstimmung mit den Landkreisen und der jeweils unmittelbar zuständigen Aufsichtsbehörde eine Bedarfs- und Entwicklungsplanung zu erarbeiten, fortzuschreiben und daran orientiert, eine den örtlichen Erfordernissen entsprechende leistungsfähige Feuerwehr aufzustellen, diese mit den notwendigen baulichen Anlagen und Einrichtungen sowie technischer Ausrüstung und zu unterhalten,
   ...

(2) Die Gemeindefeuerwehr ist so aufzustellen, dass sie in der Regel zu jeder Zeit und an jedem Ort ihres Zuständigkeitsbereichs innerhalb von zehn Minuten nach der Alarmierung wirksame Hilfe einleiten kann.

Im Zusammenhang mit der Datenübermittlung müssen die Freiwilligen Feuerwehren allerdings darauf hingewiesen werden, dass die übermittelten Daten nur für den Zweck der Mitgliederwerbung verwendet werden dürfen und im Anschluss an die Werbeaktion zu löschen sind.

6. Sonstige Selbstverwaltungskörperschaften

6.1 Kreditinstitute

6.1.1
Auskunftsanspruch des Kunden bei Aufzeichnung von Telefongesprächen durch Kreditinstitute

Im Zusammenhang mit der sog. Lehman-Pleite verlangte ein geschädigter Kunde von seiner Sparkasse Auskunft über den Inhalt der aufgezeichneten Telefongespräche über den Kauf von Lehman-Zertifikaten. Das Kreditinstitut weigerte sich mit der Begründung, das BDSG sei auf die aufgezeichneten Telefongespräche nicht anwendbar. Nach einer Überprüfung der Angelegenheit habe ich die Sparkasse aufgefordert, dem Kunden die gewünschte Auskunft zu erteilen.

Ein Sparkassenkunde bat mich, zu überprüfen, ob die Sparkasse ihm zu Recht die Auskunft über den Inhalt aufgezeichneter Telefongespräche über den Kauf von Lehman-Zertifikaten verweigere. Die Sparkasse begründete ihre Weigerung damit, dass ein Auskunftsanspruch nach BDSG nicht in Betracht komme, da das BDSG im vorliegenden Fall nicht anwendbar sei, weil die Aufzeichnungen der Telefongespräche im Endlosverfahren erfolgten und eine automatisierte Auswertung der Telefonaufzeichnungen technisch nicht möglich sei. Insbesondere erfolge auch keine Speicherung der Aufzeichnungen in Verbindung mit einem personenbezogenen Datum des Kunden. Eine Auswertung von Telefonaufzeichnungen sei daher mit erheblichem Aufwand verbunden. Im Einzelfall könnten Telefonaufzeichnungen zur Klärung von Streitfragen herausgesucht werden und würden im Rahmen von Gerichtsprozessen auch entsprechend offengelegt.

Eine Überprüfung der in der Sparkasse installierten Telefonanlage, der daran angeschlossenen Aufzeichnungsgeräte und des Aufzeichnungsverfahrens durch meine Mitarbeiter hat ergeben, dass dem Kunden ein Auskunftsanspruch zusteht.

Für die öffentlich-rechtlichen Sparkassen sind nach § 3 Abs. 6 HDSG im Wesentlichen die Vorschriften des BDSG anzuwenden, soweit es sich – wie hier – um Aufgabenbereiche handelt, bei denen sie im Wettbewerb stehen. Die Anwendung des BDSG setzt voraus, dass personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt

oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden (§§ 1 Abs. 2 Nr. 3, 27 Abs. 1 Satz 1 BDSG).

Bei den aufgezeichneten Telefongesprächen handelt es sich um personenbezogene Daten.

Seit der Novellierung des BDSG 2001 ist es nicht mehr erforderlich, dass personenbezogene Daten in einer nach bestimmten Merkmalen auswertbaren Sammlung (auswertbare Datei) verarbeitet werden. Es genügt, wenn die Auswertung durch automatisierte Verfahren erfolgen kann. Ein automatisiertes Verfahren liegt vor, wenn wesentliche Verfahrensschritte, insbesondere das Lesen und Vergleichen von Daten, in programmgesteuerten Einrichtungen ablaufen. Es reicht aus, dass die Sammlung automatisiert ausgewertet werden **kann**. Hiervon ist bereits dann auszugehen, wenn die Datensammlung maschinell gelesen und damit einer automatisierten Auswertung zugänglich gemacht werden kann. Die Datensammlung muss bereits in einem entsprechend aufbereiteten Zustand vorliegen.

Das von der Sparkasse eingesetzte System zur Aufzeichnung von Telefongesprächen legt für die Recherche in den chronologischen Aufzeichnungen jeweils einen Metadatensatz an. Er enthält zwar nicht den Namen des Kunden, aber sehr häufig die jeweils verwendete Telefonnummer. Ausgenommen sind nur analoge Telefonnummern des Gesprächspartners oder die von diesem bei einem Anruf unterdrückte eigene Rufnummer. Bei einer Recherche kann die Telefonnummer als Suchkriterium herangezogen werden.

Im Online-System sind folgende Felder enthalten:
– Telefon- /Agenten-Rufnummer des Beschäftigten des Kreditinstitutes;
– ganz überwiegend die Telefonnummer des Gesprächsteilnehmers (mit wenigen Ausnahmen wie z. B. Analogrufnummer oder unterdrückte Rufnummer des Anrufenden);
– Gesprächsdatum, -uhrzeit, -dauer.

Am Ende können in einem Freifeld Informationen manuell zusätzlich hinterlegt werden. Darüber hinaus wird nach Aussage der Bank bei der Beratung eine Kundenkontakt-Historie dann angelegt, wenn für die Mitarbeiter eine eindeutige Zuordnung erkennbar ist.

Die Software bietet umfangreiche Auswertungskriterien und -möglichkeiten. So sind sehr präzise Suchläufe nach Datum, Zeiträumen/Uhrzeiten, auch kombiniert, möglich; ebenso kann nach der Rufnummer des Gesprächsteilnehmers gezielt gesucht und ausgewertet werden.

Die Herstellerfirma der bei den Telefonaufzeichnungen eingesetzten Software bestätigt ausdrücklich, dass mit der Software nach allen technisch zur Verfügung stehenden Metadaten, die mit dem Anruf bzw. dem Telefonat gespeichert werden, gesucht werden kann. Die Firma bewirbt in einem Prospekt für ihr Produkt ausdrücklich „die gezielte und effiziente Suche und Wiedergabe von Gesprächen“, bei der „die Möglichkeit zur komplexen Suche mit vielen Sonderfunktionen im Vordergrund“ stehe. „Gespräche können anhand verschiedener Parameter wie Zeit, Kanal, Mitarbeiter, interne und externe Telefonnummer sowie Gesprächskommentare gefunden und angehört werden.“

Daher ist z. B. auch eine Auswertung nach den bekannten Kundenrufnummern möglich, dies mit der Einschränkung, dass die Auswertung nicht zwingend zu einem vollständigen Suchergebnis führen muss, da eine Rufnummernübermittlung nicht bei allen Telefonanschlüssen gegeben ist.

Die Aufzeichnung der Telefongespräche ist somit eine automatisierte Verarbeitung personenbezogener Daten, da sie programmgesteuert nach personenbezogenen Merkmalen auswertbar ist. Das BDSG ist daher anwendbar und dem Kunden der Sparkasse steht ein Auskunftsanspruch zu.

6.1.2
Auskunftsanspruch des Erben gegenüber Kreditinstituten bei angeordneter Testamentsvollstreckung

Eine angeordnete Testamentsvollstreckung schließt einen Auskunftsanspruch des Erben gegenüber dem Kreditinstitut nicht aus.

Eine Bürgerin beschwerte sich über eine Sparkasse, die sich weigerte, ihr als Miterbin Auskunft über die Konten ihrer verstorbenen Mutter zu geben. Die Sparkasse berief sich darauf, dass sie keine Auskunft erteilen könne, weil die Mutter den miterbenden Sohn als Testamentsvollstrecker eingesetzt habe und nur diesem ein Auskunftsanspruch zustehe.

In der bank- und erbrechtlichen Literatur ist diese Auffassung zwar verbreitet, es fehlt jedoch durchweg an einer Begründung, weshalb der Erbe eines verstorbenen Kontoinhabers bei bestehender Testamentsvollstreckung keinen Auskunftsanspruch gegenüber dem

Kreditinstitut haben soll. Der Erbe kann sowohl einen zivilrechtlichen als auch einen datenschutzrechtlichen Auskunftsanspruch geltend machen.

Stirbt ein Bankkunde, so endet der Kontovertrag mit der Bank dadurch nicht. Kontokorrent- und Girokonten, Sparkonten und Spareinlagen oder Termingeldkonten gehen auf den oder die Erben über. Die Erben treten an die Stelle des verstorbenen Bankkunden und werden zum Inhaber der Konten. Hat der Erblasser nur einen Erben, werden die Konten auf diesen umgeschrieben. Sind mehrere Erben vorhanden, wird das Einzelkonto als Gemeinschaftskonto fortgeführt. Die Erben können nur gemeinschaftlich Geld abheben oder das Konto auflösen, die Bank kann mit Schuld befreiender Wirkung nur an alle Erben zusammen leisten.

Der aus der Geschäftsverbindung des Erblassers mit der Bank resultierende Auskunftsanspruch des Erblassers gegen die Bank gemäß §§ 675, 666 BGB geht ebenfalls mit dem Tode des Erblassers im Wege der Universalsukzession nach § 1922 BGB auf die Erben über (BGH-Urteil vom 28. Februar 1989, BGHZ 107, 104, 108).

Durch die vom Erblasser angeordnete Testamentsvollstreckung ist den Erben die Verfügungsbefugnis über die Nachlassgegenstände entzogen worden (§§ 2211, 2205 BGB), die Verwaltung des Nachlasses obliegt allein dem Testamentsvollstrecker.

Verfügungen sind Rechtsgeschäfte, die unmittelbar darauf gerichtet sind, auf ein bestehendes Recht einzuwirken, es zu verändern, zu übertragen oder aufzuheben. Zu den Verfügungen zählen die Veräußerung, d. h. die Übereignung oder Übertragung eines Rechts und die Belastung. Neben den sachenrechtlichen Verfügungsgeschäften kommen auch schuldrechtliche Verfügungen wie z. B. Erlassvertrag, Abtretung, Aufhebungs- und Änderungsverträge in Betracht oder Gestaltungsgeschäfte, d. h. Willenserklärungen, durch die der Berechtigte von einem Gestaltungsrecht Gebrauch macht, wie Anfechtung, Rücktritt, Aufrechnung, Kündigung oder Widerruf. Die Ausübung des Auskunftsanspruchs nach §§ 675, 666 BGB, bei der Kontostand und Kontobewegungen erfragt werden, ist demnach keine Verfügung über das Konto. Dem Erben ist durch die Testamentsvollstreckung jedoch nur die Verfügungsbefugnis über die Nachlassgegenstände entzogen. Er kann weiterhin über sein Erbteil als Ganzes verfügen und Rechte, welche die Verwaltung des Nachlasses nicht berühren, ausüben. Daher hat er neben dem Testamentsvollstrecker einen Auskunftsanspruch gegenüber dem Kreditinstitut.

Der Erblasser könnte zwar den Übergang des Auskunftsanspruchs auf die Erben ausschließen. Ein solcher Wille kann aber nicht ohne Weiteres aus der Anordnung einer Testamentsvollstreckung geschlossen werden, sondern dazu bedürfte es einer eindeutigen letztwilligen Verfügung des Erblassers.

Das Interesse des Erben, Auskunft über den Nachlass zu erhalten, ist im Fall der Testamentsvollstreckung schließlich nicht bereits dadurch gesichert, dass der Testamentsvollstrecker zur Mitteilung eines Nachlassverzeichnisses und zur Beihilfe bei der Inventarverwaltung (§ 2215 BGB) verpflichtet ist. Auch die Auskunfts- und Rechenschaftspflicht des Testamentsvollstreckers gegenüber den Erben (§§ 2218 Abs. 1, 666 BGB) und der Anspruch des Erben auf jährliche Rechnungslegung (§ 2218 Abs. 2 BGB) sind kein Äquivalent zum unmittelbaren Auskunftsanspruch des Erben gegenüber der Bank.

Neben dem zivilrechtlichen Auskunftsanspruch hat der Erbe einen datenschutzrechtlichen Auskunftsanspruch gegenüber dem Kreditinstitut gem. § 34 Abs. 1 BDSG. Danach kann der Betroffene Auskunft über die zu seiner Person gespeicherten Daten verlangen. Hat der Erbe durch Vorlage eines Erbscheins bei der Bank die Rechtsnachfolge nachgewiesen und steht damit für die Bank fest, dass er Inhaber oder Mitinhaber des Kontos ist, sind die gespeicherten Kontodaten zu Einzelangaben über sachliche Verhältnisse des Erben geworden, über die er nach § 34 Abs. 1 BDSG Auskunft verlangen kann.

§ 34 Abs. 1 BDSG

Der Betroffene kann Auskunft verlangen über
1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

...

7. Entwicklungen und Empfehlungen im Bereich der Technik

7.1
Sicherheit von Web-Anwendungen

Im Rahmen meiner Prüfungen habe ich unter anderem ein browserbasiertes System zur Verwaltung von Terminen begutachtet. Die Implementierung des Verfahrens zeigte einige Schwächen; sie entsprach nicht dem Stand der Technik. Die Schwächen sind besonders auf die zur Datenübertragung an den Server verwendete Methode „GET“ zurückzuführen.

Ein in der Landesverwaltung angetroffenes Terminverwaltungssystem verwendet zur Datenübertragung die Methode „GET“. Die Anwendung ist mandantenfähig.

7.1.1
Datenübertragungsmethoden

Für die Datenübertragung zum Server stehen dem Client (Browser) zwei Methoden zur Verfügung:

GET	die Übertragung der Daten erfolgt mit der URL sichtbar in der Adresszeile des Browsers
POST	die Übertragung der Daten erfolgt im HTTP-Datenstrom

Beide Methoden sind vom Prinzip her identisch, lediglich die Datenmenge ist bei der „GET-Methode“ begrenzt, sie sollte (einschließlich der URL) 255 Zeichen nicht überschreiten.

In der Webseite ist die Methode im „FORM“-Tag der Seite festgelegt; als Beispiel eine einfache Anmeldemaske mit den Feldern für Benutzername und -passwort:

```
<FORM METHOD=“GET“ NAME=“Anmeldebeispiel“>
        <INPUT TYPE=“TEXT“ NAME=“Benutzer“>
        <INPUT TYPE=“PASSWORD“ NAME=“Passwort“>
        ...
</FORM>
```

Die in das Formular eingegeben Daten werden beim Absenden jeweils in der Form „?NAME1=WERT1?NAME2=WERT2?...“ übertragen.

Bei der „GET-Methode“ sind die übertragenen Werte nach dem Absenden des Formulars in der URL sichtbar:

„http:// ... test.html?Benutzer=USER1&Passwort=GeHeIm“

Setzt man dieses Beispiel mit der „POST-Methode“ um, ändern sich Formular und Datenübertragung:

```
<FORM METHOD=“POST“ NAME=“Anmeldebeispiel“>
        <INPUT TYPE=“TEXT“ NAME=“Benutzer“>
        <INPUT TYPE=“PASSWORD“ NAME=“Passwort“>
        ...
</FORM>
```

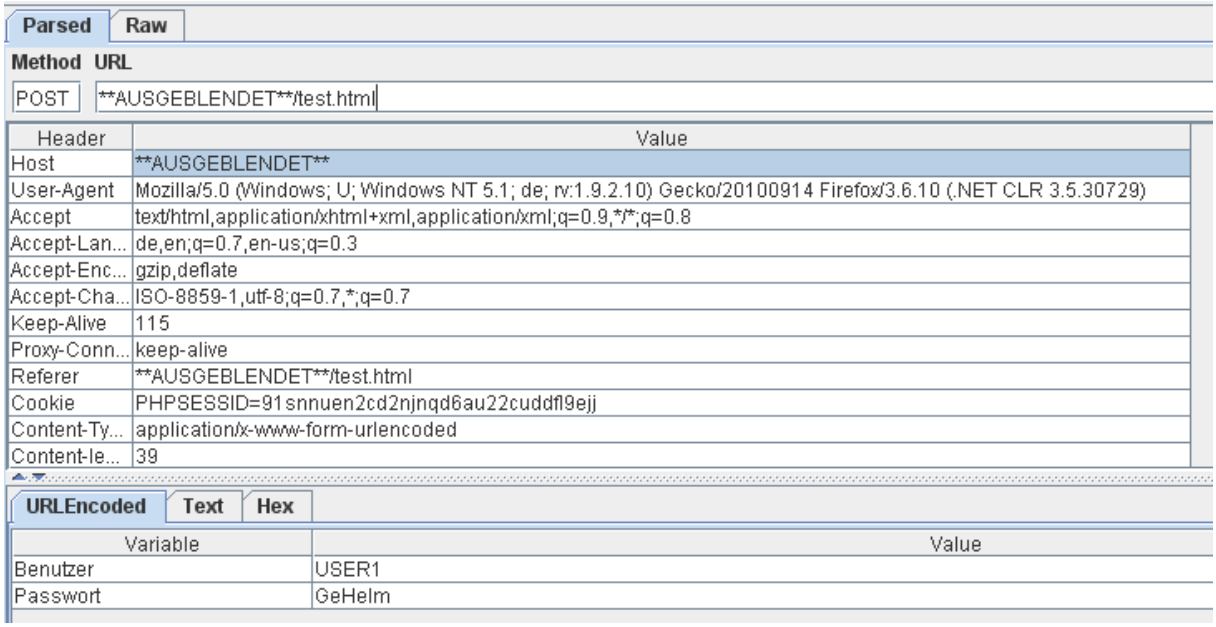
Die Seite wird nun nur als „http:// ... /test.html“ aufgerufen, die übertragenen Nutzdaten sind aber nicht mehr sichtbar.

Um diese anzuzeigen, werden Mechanismen benötigt, die in der Lage sind, den HTTP-Datenstrom mitzulesen und zu interpretieren. Beispiele hierfür sind die Firefox-Erweiterung „LiveHTTPHeaders“ oder das Framework „webScarab“.

Beispiel für eine „LiveHTTPHeaders“-Ausgabe:

```
...
POST /test.html HTTP/1.1
...
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Benutzer=user1&Passwort=GeHeIm
HTTP/1.1 200 OK
...
```

Beispiel für eine Ausgabe in webScarab:



7.1.1.1
Nachteile von „GET“

Neben der Beschränkung der Datenmenge hat die „GET-Methode“ einen klaren Nachteil: Der Benutzer sieht in der Adresszeile des Browsers genau, wie die Funktionen der Webanwendung aufgerufen werden.

Bei der Anmeldung ist dies noch nicht so offensichtlich, bei Funktionsaufrufen wie „...?menue=user?menueid=2“ wird dies jedoch problematisch. Der Anwender ist nun nicht nur in der Lage, die ihm zugewiesenen (freigeschalteten/verfügbaren) Menüeinträge aufzurufen, sondern auch weitere Funktionen der Anwendung zu erraten.

<u>Beispiele:</u>
„...?menue=user?menueid=12“

oder gar

„...?menue=admin?menueid=1“

Fehlende serverseitige Sicherungsmaßnahmen und -abfragen führen nun dazu, dass Benutzer Funktionen aufrufen können (und naturgemäß auch tun!), die für sie nicht vorgesehen sind oder für die sie ggf. gar nicht berechtigt sind.

7.1.1.2
Problem „Mandantenfähigkeit“

Die geprüfte Anwendung kann verschiedene Nutzerkreise unter einer Oberfläche bedienen, d. h. sie ist „mandantenfähig“.
Auch dies schlägt sich in den URL-Aufrufen nieder:

„...?mandant=1?menue=user?menueid=12“

Dies führt in Kombination mit einer fehlenden serverseitigen Prüfung dazu, dass nicht nur Daten anderer Nutzerkreise einzusehen, sondern diese auch zu verändern sind.

7.1.1.3
Abhilfen

Grundsätzlich muss natürlich eine serverseitige, eindeutige Identifizierung des Clients erfolgen. Dies beinhaltet bei mandantenfähigen Systemen auch die Zuordnung des Mandantenkreises (ein Nutzer, der dem Mandanten 1 zugeordnet ist, darf keine Daten aus anderen Kreisen erhalten (!) – die Abfrage lässt sich ja nicht verhindern!!)

Als Übertragungsmethode ist „POST“ zu bevorzugen, da für den Client keine Nutzdaten sichtbar sind („Was ich nicht weiß, macht mich nicht heiß“). Grundsätzlich ist es jedem Nutzer möglich, mit den anfangs beschriebenen Hilfsmitteln den HTTP-Datenstrom zu untersuchen, dies setzt allerdings etwas Fachwissen sowie die Installation besagter Hilfsmittel voraus.

Bei Verwendung der „GET-Methode“ bietet es sich an, die Browseroberfläche zu beschränken (z. B. Ausblenden der Adress- und Statuszeile). Dies erschwert die Manipulation der übertragenen Daten, es muss aber sichergestellt sein, dass Benutzer und (weitere) Hilfsprogramme diese Beschränkungen nicht aufheben oder umgehen können.

Ändert man hierzu die Startseite der Anwendung, ist dies problematisch, da bereits angelegte Links von Benutzern, die dann weiterhin auf die ursprüngliche (unbeschränkte) Startseite verweisen, diesen Mechanismus ebenfalls aushebeln.

7.1.2
Allgemeine Ansätze

Meine oben beschriebenen Feststellungen sind ein Beispiel für eine unsauber konzipierte und programmierte Anwendung. Von Anfang an müssen bei der Konzeption Angriffe auf Webanwendungen berücksichtigt werden. Dabei gilt es nicht nur, unbefugte Zugriffe auf Server und die dort gespeicherten Daten zu verhindern. Es muss auch die Übertragung der Daten ausreichend geschützt sein und für den Nutzer und seinen Rechner dürfen sich durch die Anwendung keine neuen Gefahren ergeben.

Die Hessische Landesverwaltung geht das Problem beim Betrieb durch ein entsprechendes Architekturkonzept an, dass sich derzeit in Arbeit befindet. Das Architekturkonzept beschreibt, wie Server geschützt werden sollen. Als Ergänzung müssen aber auch die Anwendungen nach dem Stand der Technik erstellt werden, denn das Architekturkonzept kann nicht festlegen, auf welche Daten durch wen zugegriffen werden darf.

Es gibt eine immer wieder aktualisierte Liste der am weitesten verbreiteten, gefährlichen Angriffsmethoden, die vom Open Web Application Security Project herausgegeben werden, die sogenannte „OWASP Top Ten“. Jeder Anwendungsentwickler muss sein Verfahren dahingehend prüfen, ob insbesondere die dort beschriebenen Angriffe abgewehrt werden.

8. Bilanz

8.1
De-Mail: Sachstand
(38. Tätigkeitsbericht, Ziff. 3.1)

In meinem letztjährigen Tätigkeitsbericht hatte ich über das geplante Bürgerportalgesetz des Bundes berichtet (Ziff. 3.1), das in der 16. Wahlperiode des Bundestages vorgelegt, aber nicht mehr verabschiedet wurde.

Im Frühjahr 2010 hat die Bundesregierung den Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten (De-Mail-Gesetz) vorgelegt, der im Wesentlichen denselben Regelungsgehalt hat, wie das Bürgerportalgesetz. Das Gesetz soll den Rechtsrahmen schaffen, der zur Einführung vertrauenswürdiger De-Mail-Dienste im Internet benötigt wird.

Viele kritische Anmerkungen, die ich bereits zum Bürgerportalgesetz gegenüber dem Bundesbeauftragten für Datenschutz und Informationsfreiheit und dem Hessischen Ministerium des Innern und für Sport geäußert hatte, haben auch für den De-Mail-Gesetzentwurf nach wie vor Gültigkeit. Dies habe ich dem HMDIS vorgetragen, der diese Anmerkungen, in seiner Stellungnahme zum Gesetzentwurf teilweise berücksichtigt hat.

Am 15. Oktober hat die Bundesregierung aufgrund der Länderanhörung einen überarbeiteten Gesetzentwurf (BRDrucks. 645/10) vorgelegt, der weitere Anregungen der Länder aufgegriffen hat.

Folgende Kritikpunkte bestehen allerdings aus meiner Sicht weiterhin bzw. sind neu hinzugekommen:

– Wie auch der Bürgerportalgesetzentwurf sieht der jetzige Gesetzentwurf vor, dass ein Nutzer grundsätzlich eine personenbezogene Hauptadresse haben muss (§ 5 Abs. 1). Eine oder mehrere pseudonyme Adressen kann er nur zusätzlich auf Antrag erhalten. Datenschutzfreundlicher wäre die Möglichkeit, gleich eine pseudonyme Adresse beantragen zu können.

– Durch das Gesetz und die Erläuterungen im Internet werden der sichere Betrieb und dabei insbesondere die Vertraulichkeit des Postfach- und Versanddienstes sowie des Speicherplatzes hervorgehoben. Für die E-Mail-Kommunikation ist jetzt im Gesetz

klargestellt, dass keine Ende-zu-Ende-Vertraulichkeit gegeben ist. Bei der Dokumentenablage gibt es die Ergänzung, dass Dokumente verschlüsselt abzulegen sind. Damit ist jedoch nicht ausgeschlossen, dass der Dienste-Anbieter die gespeicherten Daten zur Kenntnis nehmen kann. Dies ergibt sich aus dem Anspruch, die Verfügbarkeit sicherzustellen, obwohl Passwörter vergessen und Token (Gerät, das zeitlich begrenzte, sichere Schlüssel für den Zugang zu Datenverarbeitungssystemen oder auch für das Internetbanking speichert oder generiert) verloren werden können.

– Es fehlt nach wie vor die Verpflichtung im Gesetz, dass die Nutzer bei der Eröffnung des De-Mail-Kontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen – deutlich hingewiesen werden. Entsprechendes muss bei den Aufklärungs- und Informationspflichten im Gesetzestext klarer als bislang geschehen zum Ausdruck kommen. Das betrifft auch Fragen der Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

– Einvernehmlich war beim Bürgerportalgesetzentwurf kritisiert worden, dass die technischen Einzelfragen erst durch eine Rechtsverordnung festgelegt werden sollten. Die Rechtsverordnung ist jetzt zwar vom Tisch, aber durch den Verweis auf die technische Richtlinie des BSI und die Einrichtung eines Ausschusses De-Mail-Standardisierung, der sich um die Weiterentwicklung der technischen und organisatorischen Anforderungen kümmern soll, ist wenig gewonnen. Konkrete Aussagen zu technischen Einzelsachverhalten sind damit immer noch nicht möglich, da es keine detaillierte Regelung im Gesetz gibt.

– In § 20 heißt es, dass die Aufsicht über die Einhaltung dieses Gesetzes der zuständigen Aufsichtsbehörde (also dem BSI) obliegt. Da nach § 18 Abs. 3 Nr. 4 dem BfDI Aufgaben zugewiesen sind, stellt sich die Frage des Verhältnisses beider Behörden zueinander. In der Begründung zum Gesetzentwurf heißt es dazu: "Das bestehende Regelungssystem der datenschutzrechtlichen Aufsicht bleibt hiervon unberührt." Meines Erachtens sollte dieser Satz im Gesetz selbst stehen.

8.2
Novellierung des HSOG – Regelung zur Videoüberwachung (38. Tätigkeitsbericht, Ziff. 4.2.1.2)

Im letzten Jahr hatte ich im Rahmen der Novellierung des HSOG darüber berichtet, dass jetzt im Gesetz ausdrücklich verlangt wird, die überwachten Bereiche zu kennzeichnen.

§ 14 Abs. 3 Satz 2 HSOG

Der Umstand der Überwachung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

Diese Regelung gilt auch für den Einsatz von Videokameras zum Schutz besonders gefährdeter öffentlicher Einrichtungen.

Mir ist nicht bekannt wie viele Gebäude in Hessen mit Videokameras ausgestattet sind, in denen Dienststellen oder andere als gefährdet eingestufte Einrichtungen – wie etwa jüdische Gemeinden – untergebracht wurden. Es besteht für die jeweilige Einrichtung lediglich eine Verpflichtung, für eine solche Anlage ein Verfahrensverzeichnis gem. § 28 HSOG zu führen. Daher kann ich auch nicht beurteilen, ob für alle diese Gebäude die Voraussetzungen des Gesetzes wirklich vorliegen, d. h. ob sie wirklich besonders gefährdet sind. Unabhängig davon ist jedenfalls häufig festzustellen, dass ein Hinweis auf die Tatsache der Videoüberwachung fehlt. Das gilt u. a. für Ministeriumsgebäude, Polizeidienststellen und Gebäude, in denen Justizbehörden untergebracht sind.

Hier besteht dringend Nachbesserungsbedarf. Je nach Lage der Gebäude erfassen die Kameras häufig auch Teile von Gehwegen. Nicht alle Passanten, die an einem solchen Gebäude vorbeigehen, rechnen damit, von Kameras erfasst zu werden. Zumal die Kameras nicht immer auf den ersten Blick erkennbar sind.

Schließlich ist darauf zu achten, dass die Hinweise so angebracht werden, dass sie in dem Moment wahrgenommen werden können, in dem der erfasste Bereich betreten wird. Ein Schild neben der Kamera – erst recht wenn diese in Höhe des 1. Stockwerks eines Bürogebäudes angebracht ist – wird in aller Regel im Vorbeigehen oder beim Warten auf einen Bus an einer Haltestelle vor dem Gebäude nicht wahrgenommen.

8.3
Einsatz von Videotechnik zur Verkehrsüberwachung (38. Tätigkeitsbericht, Ziff. 4.1.3)

Im letzten Jahr hatte ich über die Konsequenzen für die Verkehrsüberwachung berichtet, die sich aus dem Beschluss der zweiten Kammer des zweiten Senats des BVerfG vom 11. August 2009 (2 BvR 941/08) ergeben haben. In einen Beschluss vom 12. August 2010 (2 BvR 1447/10) hat sich diese Kammer des BVerfG nun nochmals zur Frage der Voraussetzungen für den Einsatz von Videoaufnahmen im Rahmen der Verkehrsüberwachung geäußert.

Der Beschwerdeführer rügte vor allem, dass die Instanzgerichte § 100h Abs. 1 Satz 1 Nr. 1 StPO in Verbindung mit § 46 Abs. 1 OWiG als Rechtsgrundlage herangezogen hatten. Die Erstellung von Aufnahmen zum Beweis eines Verkehrsverstoßes diene der Beweissicherung und sei in der Sache etwas anderes als die verdeckte Anfertigung von Bildern im Rahmen einer Observation.

§ 100h StPO

(1) Auch ohne Wissen der Betroffenen dürfen außerhalb von Wohnungen
1. Bildaufnahmen hergestellt werden,
2. sonstige besondere für Observationszwecke bestimmte technische Mittel verwendet werden,

wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert wäre. Eine Maßnahme nach Satz 1 Nr. 2 ist nur zulässig, wenn Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.

§ 46 OWiG

(1) Für das Bußgeldverfahren gelten, soweit dieses Gesetz nichts anderes bestimmt, sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung, des Gerichtsverfassungsgesetzes und des Jugendgerichtsgesetzes.

Dem widerspricht das BVerfG. § 100h StPO lasse auch Videoaufnahmen zu, wenn sichergestellt sei, dass die Maßnahme nicht auf Unbeteiligte ziele, sondern nur auf Fahrzeugführer, die selbst Anlass zur Erstellung dieser Aufnahmen gegeben haben, da der Verdacht eines bußgeldbewehrten Verkehrsverstoßes bestehe. Die Verfahrensvorschriften der

StPO insbesondere § 101 StPO reichten als grundrechtssichernde Regelung aus, einen Eingriff in das Recht auf informationelle Selbstbestimmung auf § 100h StPO zu stützen.

Weitere Voraussetzung sei, dass die Anfertigung der Aufnahmen verdachtsabhängig erfolge. Die Geräte müssen deshalb so eingestellt werden, dass im Ergebnis nur dann eine Aufnahme eines Fahrzeuges erstellt wird, wenn die vorab definierte Schwelle des bußgeldbewehrten Verkehrsverstoßes erreicht wird. Das heißt z. B., dass das Fahrzeug die am Messpunkt zulässige Höchstgeschwindigkeit auch nach Abzug des üblicherweise berücksichtigten Toleranzwertes überschreitet.

Damit sollte nunmehr sowohl für die Verwaltungspraxis, aber auch für die Verkehrsteilnehmer Klarheit bestehen, dass Videoaufnahmen, die unter den genannnten Voraussetzungen erstellt werden, geeignete Beweismittel im Ordnungswidrigkeitenverfahren sind.

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

9.1
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

– Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.

– Es darf keine Fach- und Rechtsaufsicht geben.

– Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.

– Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.

– Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.

– Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

9.2
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Eckpunktepapier: Ein modernes Datenschutzrecht für das 21. Jahrhundert

Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die

Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne

Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

9.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Keine Vorratsdatenspeicherung

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

9.4
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Körperscanner – viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.

2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.

3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z. B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

9.5
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002

sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiterzuentwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

9.6
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften.

Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

9.7
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. Juni 2010

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz

gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz „Qualität vor übereilten Regelungen“ gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zugunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substanzielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

– Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

– Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur „Verhinderung und Aufdeckung von Vertragsverletzungen zulasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten“ würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss

vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln - etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.

– Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn – wie im Entwurf vorgesehen – Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv - und nicht erst auf Nachfrage - darüber aufzuklären, woher die verwendeten Daten stammen.

– Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.

– Die im Gesetzentwurf an mehreren Stellen vorgesehene „Einwilligung“ der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-)Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

9.8
Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes

und der Länder vom 24. Juni 2010

zur Erweiterung der zentralen Steuerdatenbank um elektronische Lohnsteuerabzugsmerkmale (ELStAM)

Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z. B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

– Vorherige Information der Arbeitnehmer
  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

– Keine Speicherung auf Vorrat
  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

– Verhindern des unzulässigen Datenabrufs
  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies

tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

– Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept
  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

9.9
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2010

Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des

15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrag – RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

– die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,

– bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und

– auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

9.10
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010

Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwerung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die – ggf. gänzlich unverdächtigen – Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

9.11
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010

Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z. B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im

häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz

bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

9.12
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4. November 2010

Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

– die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
– die größtmögliche Transparenz der Tätigkeit garantiert ist und
– die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

Informationen zum Datenschutz gibt es insbesondere auf folgenden Seiten im Internet

Homepage des Hessischen Datenschutzbeauftragten

www.datenschutz.hessen.de

Virtuelles Datenschutzbüro

Ein gemeinsamer Service Ihrer Datenschutzinstitutionen

www.datenschutz.de

Homepage des ZAfTDa

Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz an der Fachhochschule Gießen-Friedberg

www.fh-giessen-friedberg.de/zaftda

Sachwortverzeichnis zum 39. Tätigkeitsbericht