19. Wahlperiode

Drucksache **19/289**

HESSISCHER LANDTAG

31. 03. 2014

Zweiundvierzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2013
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes

Eingegangen am 31. März 2014 · Ausgegeben am 8. April 2014
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Inhaltsverzeichnis

3.3.10 Wirtschaftsverwaltung

3.3.10.1 Zulässigkeit massenhafter Abfragen von Eigentümerdaten aus dem Liegenschaftskataster durch Makler

3.3.11 Rundfunk

3.3.11.1 Einmaliger Meldedatenabgleich durch den ARD ZDF Deutschlandradio Beitragsservice (vormals GEZ)

4. Aufsichtsbehörde nach § 38 BDSG

4.1 Ordnungswidrigkeiten und Meldepflichten

4.1.1 Ahndung von Datenschutzverstößen als Ordnungswidrigkeit

4.1.2 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

4.1.3 E-Mail-Versand mit offenem Verteiler – Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG

4.2 Querschnitt nicht öffentlicher Bereich

4.2.1 Internationale Aktion zur Prüfung von Datenschutzerklärungen

4.2.2 Videoüberwachung nach Bundesdatenschutzgesetz

4.2.3 Verhaltenssteuerung durch Attrappen von Videokameras

4.3 Kreditinstitute und Auskunfteien

4.3.1 Aufzeichnung von Telefonanrufen bei Kreditinstituten

4.3.2 Scoring von Handelsauskunfteien

4.3.3 Speicherung der erteilten Restschuldbefreiung durch Auskunfteien

4.3.4 Vorlage von Ausweiskopien bei Auskunfteien zur Erlangung einer Selbstauskunft

4.3.5 Telefonanruf durch Inkassounternehmen bei Nachbarn

4.4 Werbung und Adresshandel

4.4.1 Ethnomarketing

4.4.2 Nutzungsbasierte Internetwerbung/Tracking

4.5 Versicherungen

4.5.1 Bestandsübertragungen bei selbständigen Versicherungsvermittlern

4.5.2 Anforderung von ärztlichen Unterlagen durch Versicherungen und Einsichtsrecht des Versicherungsnehmers

4.6 Verkehr und Energieversorgung

4.6.1 Datenerhebung beim Kauf einer Gruppenfahrkarte bei der Deutschen Bahn AG

4.6.2 Erhebung personenbezogener Daten beim Online-Ticketkauf unter Verwendung eines Personalausweises als Identifikationsdokument

4.6.3 Funktionsweise des Deutsche Bahn-Navigators 2.1.8

4.6.4 Das „Call a Bike“-Angebot der Deutschen Bahn AG

4.6.5 Anruferidentifikation durch Energieversorger bei telefonischen Anfragen

4.7 Handel, Handwerk, Selbstständige und Gewerbetriebe

4.7.1 Beauftragung eines Steuerberaters – Funktionsübertragung oder Auftragsdatenverarbeitung?

Abkürzungsverzeichnis zum 42. Tätigkeitsbericht

ABl.	Amtsblatt des Hessischen Kultusministeriums
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
Alt.	Alternative
App	Application Software
AufenthG	Aufenthaltsgesetz
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BKRG	Bundeskrebsregisterdatengesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	Beispielsweise
BTDrucks.	Bundestagsdrucksache
BußgeldElektAktFV	Verordnung über die elektronische Aktenführung bei Verwaltungsbehörden in Bußgeldverfahren
BverwGE	Entscheidungen des Bundesverwaltungsgerichts
bzgl.	Bezüglich
bzw.	beziehungsweise
CDU	Christlich-Demokratische Union
C-SIS	Zentraler Teil des Schengener Informationssystems
CSU	Christlich-Soziale Union
d.h.	das heißt
DAPIX	Working Party on Information Exchange and Data Protection
DB	Deutsche Bahn
DIMAG	Archivierungssystem des Hessischen Staatsarchives
DMZ	demilitarisierte Zone
DOMEA	Standardprogramm für elektronisches Dokumentenmanagement
Dr.	Doktor
DuD	Zeitschrift „Datenschutz und Datensicherheit“
EDPS	Europäischer Datenschutzbeauftragter
EES	Einreise- und Ausreisesystem der EU

EgovG	E-Government-Gesetz
ERV	Europäische Reiseversicherung
ESS	Employee Self Service
etc.	et cetera
EU	Europäische Union
EUR	Euro
FDP	Freie Demokratische Partei
ff.	fortfolgende/r/s
gem.	gemäß
GemKVO	Gemeindekassenverordnung
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland
GG	Grundgesetz
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
GlüStV	Glücksspielstaatsvertrag
GRCh	Charta der Grundrechte der Europäischen Union
HÄBl.	Hessisches Ärzteblatt
HArchivG	Hessisches Archivgesetz
HBG	Hessisches Beamtengesetz
HBKG	Hessisches Brand- und Katastrophenschutzgesetz
HCC	Hessisches Competence Center
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HeDoc	in der Hessischen Landesverwaltung eingesetztes elektronisches Dokumentenmanagementsystem
HessVwVG	Hessisches Verwaltungsvollstreckungsgesetz
HGO	Hessische Gemeindeordnung
HKHG	Hessisches Krankenhausgesetz
HMDIS	Hessisches Ministerium des Innern und für Sport
HMG	Hessisches Meldegesetz
HMUELV	Hessisches Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HStVollzG	Hessisches Strafvollzugsgesetz
HVGG	Hessisches Vermessungs- und Geoinformationsgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i.d.F.	in der Fassung

i.d.R.	in der Regel
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
ICE	Intercity-Express
IP-Adresse	Internetprotokollbasierte Adresse
IT	Informationstechnik
KFRG	Krebsfrüherkennungs- und -registergesetz
KHEntgG	Krankenhausentgeltgesetz
KHG	Krankenhausfinanzierungsgesetz
KIS	Krankenhausinformationssysteme
KrWG	Kreislaufwirtschaftsgesetz
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
LDSG	Landesdatenschutzgesetz
LfV-Gesetz	Gesetz über das Landesamt für Verfassungsschutz
LG	Landgericht
LHO	Hessische Landeshaushaltsordnung
LIBE	Committee on Civil Liberties, Justice and Home Affairs
LTDrucks.	Landtagsdrucksache
LUSD	Lehrer- und Schülerdatenbank
m.w.N.	mit weiteren Nachweisen
m.W.v.	mit Wirkung vom
MDK	Medizinischer Dienst der Krankenversicherung
MDM	Mobile Device Management
MedR	Zeitschrift „Medizinrecht“
MWV	Medizinisch-Wissenschaftliche Verlagsgesellschaft
NJW	Zeitschrift „Neue Juristische Wochenschrift“
Nr.	Nummer
Nrn.	Nummern
NSA	Nation Institute of Standards and Technology
N-SIS	nationaler Teil des Schengener Informationssystems
o.a.	oben aufgeführt
o.Ä.	oder Ähnliche/s
o.g.	oben genannte/r/s
OLG	Oberlandesgericht
OSCI	Online Service Computer Interface

OWi21	Ordnungswidrigkeiten21 (Software der ekom21 GmbH)
OWiG	Ordnungswidrigkeitengesetz
PAuswG	Personalausweisgesetz
Prof.	Professor
PStG	Personenstandsgesetz
qeS	Qualifizierte elektronische Signatur
RBStV	Rundfunkbeitragsstaatsvertrag
s.	siehe
S.	Seite
SGB	Sozialgesetzbuch
SIENA	Secure Information Exchange Network Application
SMS	Short Message Service
sog.	sogenannte/r/s
SPD	Sozialdemokratische Partei Deutschlands
StAG	Staatsangehörigkeitsgesetz
StAnz.	Staatsanzeiger für das Land Hessen
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
TFTP	Terrorist Finance Tracking Programme
TKG	Telekommunikationsgesetz
TMF	Technologie- und Methodenplattform für vernetzte medizinische Forschung e. V.
TMG	Telemediengesetz
u.a.	unter anderem
US	United States
USA	United States of America
VAG	Versicherungsaufsichtsgesetz
vgl.	vergleiche
VO	Verordnung
VVG	Versicherungsvertragsgesetz
VwVfG	Verwaltungsverfahrensgesetz

z.B.	zum Beispiel
Ziff.	Ziffer/n
ZPO	Zivilprozessordnung
zzgl.	zuzüglich

Register der Rechtsvorschriften

AEUV	Vertrag über die Arbeitsweise der Europäischen Union i.d.F vom 9. Mai 2008 (ABl. EU C 115 S. 47)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) i.d.F. vom 25. Feb. 2008 (BGBl. I S. 162), zuletzt geändert durch Gesetz vom 25. Juli 2013 (BGBl. I S. 2749)
BDSG	Bundesdatenschutzgesetz i.d.F. vom 14. Jan. 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 14. Aug. 2009 (BGBl. I S. 2814)
Berufsordnung für die Ärztinnen und Ärzte	vom 2. September 1998 (HÄBl. 10/1998, S. I - VIII), zuletzt geändert am 26. Juni 2013 (HÄBl. 8/2013, S. 646)
Berufsordnung für hessische Zahnärztinnen und Zahnärzte	Zeitschrift „Der Hessische Zahnarzt“, Ausgabe 1-2/2011, S. 50 ff.
BGB	Bürgerliches Gesetzbuch i.d.F. vom 2. Jan. 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Gesetz vom 1. Okt. 2013 (BGBl. I S. 3719)
BKRG	Bundeskrebsregisterdatengesetz i.d.F. vom 10. Aug. 2009 (BGBl. I S. 2707)
BußgeldElektAktFV	Verordnung über die elektronische Aktenführung bei Verwaltungsbehörden in Bußgeldverfahren vom 23. Juli 2010 (GVBl. I S. 254)
EGovG	Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz) vom 25. Juli 2013 (BGBl. I S. 2749)
GemKVO	Verordnung über die Kassenführung der Gemeinden (Gemeindekassenverordnung) vom 27. Dez. 2011 (GVBl. I S. 830, 2012 S. 19)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert Gesetz vom 11. Juli 2012 (BGBl. I S. 1478)
GlüStV	Staatsvertrag zum Glücksspielwesen in Deutschland (Glücksspielstaatsvertrag) vom 15. Dez. 2011 (GVBl. 2012 S. 190, 197), in Kraft getreten am 1. Juli 2012 gemäß Bekanntmachung vom 10. Aug. 2012 (GVBl. S. 264)
GRCh	Charta der Grundrechte der Europäischen Union vom 18. Dez. 2000 (ABl. EG 2000/C 364/01), zuletzt geändert durch die Erläuterungen zur Charta der Grundrecht vom 14. Dez. 2007 (ABl. EG 2007/C 303/01)
HArchivG	Hessisches Archivgesetz vom 26. Nov. 2012 (GVBl. S. 458)
HBG	Hessisches Beamtengesetz i.d.F. vom 11. Jan. 1989 (GVBl. I S. 218), zuletzt geändert durch Gesetz vom 13. Dez. 2012 (GVBl. S. 622)
HBKG	Hessisches Gesetz über den Brandschutz, die Allgemeine Hilfe und den Katastrophenschutz i.d.F. vom 14. Jan. 2014 (GVBl. S. 26)
HDSG	Hessisches Datenschutzgesetz i.d.F. vom 7. Jan. 1999 zuletzt geändert durch Gesetz vom 20. Mai 2011 (GVBl. I S. 208)
Hessisches Spielhallengesetz	vom 28. Juni 2012 (GVBl. S. 213)
HessVwVG	Hessisches Verwaltungsvollstreckungsgesetz i.d.F. vom 12. Dez. 2008, (GVBl. I S. 2), zuletzt geändert durch Gesetz vom 21. Nov. 2012 (GVBl. I S. 430)
HGO	Hessische Gemeindeordnung i.d.F. vom 7. März 2005 (GVBl. I S. 142), zuletzt geändert durch Gesetz vom 27. Mai 2013 (GVBl. I

	S. 218)
HKHG	Hessisches Krankenhausgesetz i.d.F. vom 21. Dez.2010 (GVBl. I, S. 587), zuletzt geändert durch Gesetz vom 15. Sept. 2011 (GVBl. I S. 425, 426)
HMG	Hessisches Meldegesetz i.d.F. vom 10. März 2006 (GVBl. I S. 66), zuletzt geändert durch Gesetz vom 22. Nov. 2010 (GVBl. I S. 403, 404)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i.d.F. vom 14. Jan 2005, zuletzt geändert durch Gesetz vom 27. Juni 2013 (GVBl. S. 444)
HStVollzG	Hessisches Strafvollzugsgesetz i.d.F. vom 28. Juni 2010 (GVBl. I, S. 185), zuletzt geändert durch Gesetz vom 5. März 2013 (GVBl. I S. 46)
HVGG	Hessisches Vermessungs- und Geoinformationsgesetz i.d.F. vom 6. Sept. 2007, zuletzt geändert durch Gesetz vom 27. Sept. 2012 (GVBl. I S. 290)
JITStG	Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten i.d.F. vom 16. Dez. 2011 (GVBl. I S. 778)
KFRG	Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister (Krebsfrüherkennungs- und -registergesetz) i.d.F. vom 3. Apr. 2013 (BGBl I S. 617)
KHEntgG	Gesetz über die Entgelte für voll- und teilstationäre Krankenhausleistungen (Krankenhausentgeltgesetz) i.d.F. vom 23. Apr. 2002 (BGBl. I S. 1412, 1422), zuletzt geändert durch Gesetz vom 15. Juli 2013 (BGBl. I S. 2423)
KHG	Gesetz zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze (Krankenhausfinanzierungsgesetz) i.d.F. vom 10. Apr. 1991 (BGBl. I S. 886), zuletzt geändert durch Gesetz vom 15. Juli 2013 (BGBl. I S. 2423)
KrWG	Kreislaufwirtschaftsgesetz i.d.F. vom 24. Feb. 2012 (BGBl. I S. 212), zuletzt geändert durch Gesetz vom 22. Mai 2013 (BGBl. I S. 1324)
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie i.d.F. vom 9. Jan. 1907, zuletzt geändert durch Gesetz vom 16. Feb. 2001 (BGBl. I S. 266)
LDSG Rheinland-Pfalz	Datenschutzgesetz des Landes Rheinland-Pfalz i.d.F. vom 5. Juli 1994 (GVBl. S. 293), zuletzt geändert durch Gesetz vom 20. Dez. 2011 (GVBl. S. 427)
LfV-Gesetz	Gesetz über das Landesamt für Verfassungsschutz i.d.F. vom 19. Dez. 1990 (GVBl. I S. 753), zuletzt geändert durch Gesetz vom 27. Juni 2013 (GVBl. I S. 444)
LHO	Hessische Landeshaushaltsordnung i.d.F. vom 15. März 1999 (GVBl. I S. 248), zuletzt geändert durch Gesetz vom 26. Juni 2013 (GVBl. S. 447)
OWiG	Gesetz über Ordnungswidrigkeiten i.d.F. vom 19. Feb. 1987, zuletzt geändert durch Gesetz vom 10. Okt. 2013 (BGBl. I S. 3786)
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) i.d.F. vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Gesetz vom 7. Aug. 2013 (BGBl. I S. 3154)
PStG	Personenstandsgesetz vom 19. Feb. 2007 (BGBl. I S. 122), zuletzt geändert durch Gesetz vom 28. Aug. 2013 (BGBl. I S. 3458)
RBStV	Rundfunkbeitragsstaatsvertrag vom 23. Aug. 2011 (GVBl. I S. 382)
Richtlinie 2002/58/EG	Richtlinie des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den

	Schutz der Privatsphäre in der elektronischen Kommunikation [Datenschutzrichtlinie für elektronische Kommunikation] (ABl. EG 2002/L201/S. 37ff.)
Richtlinie 2009/136/EG	Richtlinie des Europäischen Parlaments und des Rates vom 25. Nov. 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (ABl. EG 2009/L337 S: 11ff.)
Richtlinie 95/46/EG	Richtlinie Europäischen Parlaments und des Rates vom 24. Okt. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG1995/L281 S. 31ff.)
Safe Harbor-Abkommen	Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. L 215/7 bis 215/47)
SGB I	Sozialgesetzbuch Erstes Buch – Allgemeiner Teil – i.d.F. vom 11. Dez. 1975, BGBl. I S. 3015), zuletzt geändert durch Gesetz vom 19. Okt. 2013 (BGBl. I S. 3836)
SGB II	Sozialgesetzbuch Zweites Buch – Grundsicherung für Arbeitsuchende – i.d.F. vom 13. Mai 2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Gesetz vom 7. Mai 2013 (BGBl. I S. 1167)
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung – i.d.F. vom 20. Dez. 1988 (BGBl. I S. 2477, 2482), zuletzt geändert durch Gesetz vom 22. Dez. 2013 (BGBl. I S. 4382)
SGB VIII	Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – i.d.F. vom 26. Juni 1990 (BGBl. S. 1163), zuletzt geändert durch Gesetz vom 29. Aug. 2013 (BGBl. I S. 3464)
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz – i.d.F. vom 18. Jan. 2001 (BGBl. I S. 130), zuletzt geändert Gesetz vom 25. Juli 2013 (BGBl. I S. 2749)
StAG	Staatsangehörigkeitsgesetz i.d.F. vom 15. Juli 1999 (BGBl. I S. 1618), zuletzt geändert durch Gesetz vom 28. Aug. 2013 (BGBl. I S. 3458)
StBerG	Steuerberatungsgesetz i.d.F. vom 4. Nov. 1975 (BGBl. I S. 2735), zuletzt geändert durch Gesetz vom 31. Aug. 2013 (BGBl. I S. 3533)
StGB	Strafgesetzbuch i.d.F. vom 13. Nov. 1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 10. Okt. 2013 (BGBl. I S. 3799)
StPO	Strafprozessordnung i.d.F. vom 7. Apr. 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 28. Aug. 2013 (BGBl. I S. 3313)
TKG	Telekommunikationsgesetz i.d.F. vom 22. Juni 2004 (BGBl. I, S. 1190), zuletzt geändert durch Gesetz vom 7. Aug. 2013 (BGBl. I S. 3154)
TMG	Telemediengesetz i.d.F. vom 26. Feb. 2007 (BGBl. I S. 179)
VAG	Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz) i.d.F. vom 17. Dez. 1992 (BGBl. I S. 2), zuletzt geändert durch Gesetz vom 28. Aug. 2013 (BGBl. I S. 3395)
Verordnung über die Verarbeitung personenbezoge-	vom 4. Feb. 2009, zuletzt geändert durch Art. 20 der Verordnung vom 19. März 2013 (ABl. S. 222)

ner Daten in Schulen und statistische Erhebungen an Schulen	
VVG	Gesetz über den Versicherungsvertrag (Versicherungsvertragsgesetz) i.d.F. vom 23. Nov. 2007 (BGBl. I S. 2631), zuletzt geändert durch Gesetz vom 20. Sept. 2013 (BGBl. I S. 3642)
VwVfG	Verwaltungsverfahrensgesetz i.d.F. vom 23. Jan. 2003 (BGBl. I S. 102), zuletzt geändert durch Gesetz vom 25. Juli 2013 (BGBl. I S. 2749)
ZPO	Zivilprozessordnung i.d.F. vom 5. Dez. 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), zuletzt geändert durch Gesetz vom 10. Okt. 2013 (BGBl. I S. 3786)

Kernpunkte

1. Die skandalösen Abhöraktivitäten ausländischer Nachrichtendienste belegen die generell bestehenden Notwendigkeiten einer zeitgemäßen Fortentwicklung des Datenschutzrechts auf internationaler und europäischer Ebene (Ziff. 1.1, 1.2).

2. Dabei gilt es, das Niveau des Datenschutzes adäquat anzuheben. Unionsrechtliche Regelungen, die diesen Zweck verfolgen, sind grundsätzlich zu begrüßen. Umgekehrt rechtfertigt die unionsrechtliche Vereinheitlichung keine Beschneidung der Fortentwicklungsmöglichkeit des deutschen Datenschutzrechts. Die in dieser Hinsicht bestehenden Bedenken gegen die europäische Grundverordnung bestehen daher fort (Ziff. 1.3).

3. Die Datenschutzbeauftragten des Bundes und der Länder und die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben eine Orientierungshilfe „Soziale Netzwerke“ erarbeitet, die sich mit der Wahrung des Datenschutzes bei der Verwendung sozialer Medien, insbesondere sozialer Netzwerke, zur Erfüllung eigener Aufgaben oder Geschäftszwecke befasst. Die Orientierungshilfe richtet sich an Betreiber sozialer Netzwerke, aber auch an Behörden und Unternehmen, die beabsichtigen, mit sozialen Netzwerken ihre Aufgaben zu erfüllen oder ihre Geschäftszwecke zu verfolgen (Ziff. 6.5 und 8.1).

4. Auf nationaler Ebene und Landesebene besteht Regelungsbedarf bzgl. der Videoüberwachung. Die Beurteilung der Rechtmäßigkeit der Anfertigung von Videoaufnahmen bindet weiterhin viel Kontroll- und Beratungskapazität (Ziff. 1.8). Die Videoüberwachung erfasst mittlerweile alle Lebensbereiche (Kindergarten/Kindertagesstätten s. Ziff. 3.3.7.6, Schule s. Ziff 3.3.5.1, sonstige öffentliche Einrichtungen s. Ziff. 3.3.9.7). Anders als im Bundesdatenschutzgesetz fehlt im Hessischen Datenschutzgesetz eine Rechtsgrundlage für die Videoüberwachung durch öffentliche Stellen; die im Hessischen Gesetz für die Sicherheit und Ordnung enthaltene Vorschrift erlaubt nur eine Videoüberwachung besonders gefährdeter Einrichtungen oder durch Gefahrenabwehrbehörden (Ziff. 3.3.5.1 und 1.7). Für die sonstigen öffentlichen Stellen besteht somit dringender Regelungsbedarf. Auch im nicht öffentlichen Bereich habe ich vielfach unzulässige Videoüberwachungen angetroffen, z.B. weil öffentlicher Raum oder Mitarbeiter überwacht wurden (Ziff. 4.2.2). Ein wesentlicher Gesichtspunkt ist die Transparenz: der überwachte Bereich muss klar erkennbar sein. Attrappen sind wegen der mit ihnen beabsichtigten und erzielten Verhaltensänderung nach den Zulässigkeitsregeln der echten Videoüberwachung zu beurteilen (Ziff. 4.2.3).

5. Die zentrale Spielersperrdatei nach Glückspielstaatsvertrag und die Sperrdatei nach dem Hessischen Spielhallengesetz sind getrennt zu halten. Für eine Einmeldung einer Spielersper-

re in die zentrale Spielersperrdatei nach Glücksspielstaatsvertrag fehlt es an einer Rechtsgrundlage, die nicht in die Kompetenz des hessischen Gesetzgebers fällt (Ziff. 2.1.2).

6. Im Gesundheitsbereich werden sowohl von öffentlichen Stellen (Kliniken, gesetzlichen Krankenkassen, Krebsregister) als auch von nicht öffentlichen Stellen (niedergelassenen Ärzten und Zahnärzten) sensitive Daten verarbeitet. Zur Datenverarbeitung in Arzt- und Zahnarztpraxen habe ich vielfältige Anfragen von Praxisinhabern und Patienten erhalten und beantwortet. Neue bundesweit gültige Präzisierungen zum Akteneinsichtsrecht der Patienten wurden mit dem Patientenrechtegesetz geschaffen. Im Hessischen Krankenhausgesetz und in der ärztlichen Berufsordnung sollten zur Klarstellung entsprechende Anpassungen vorgenommen werden (Ziff. 2.1.4). Ergebnisse meiner Beratungen und Prüfungen aus diesem Bereich finden sich in Ziff. 2.1.5, 2.1.6, 3.3.6 und 4.9.

7. Auch die Hessische Landesverwaltung darf Daten nur so lange aufbewahren, wie sie für ihre Aufgabenerfüllung erforderlich sind. Zwar sind beim Löschen von Personaldaten im SAP R/3-System die Anfänge für eine routinemäßige Löschung nach Ablauf der Aufbewahrungsfristen gemacht (Ziff. 5.1); leider hat die Landesverwaltung aber noch keine Löschung für die im Dokumentenmanagementsystem HeDoc gespeicherten Daten und noch keinen Übergang in die Archivierung durch die Staatsarchive realisiert. Angesichts der Regelaufbewahrungsfrist von fünf Jahren und dem Einsatz von HeDoc etwa seit Mitte des vergangenen Jahrzehnts ist von Verstößen gegen das HDSG durch unzulässig lange Datenspeicherungen auszugehen, die sich in den kommenden Jahren noch potenzieren werden (Ziff. 3.3.1).

8. Anbieter von Websites und Smartphone-Apps sollen in verständlicher und überschaubarer Weise darüber aufklären, welche Daten sie zu welchen Zwecken erheben. An einer erstmalig durchgeführten internationalen Aktion zur Prüfung solcher Datenschutzerklärungen hat auch meine Dienststelle teilgenommen. Anbieter hessischer Websites haben dabei im internationalen Vergleich gut abgeschnitten – nicht zuletzt auch deshalb, weil deutsches Recht die Anbieter verpflichtet, Informationen zur Datenverarbeitung bereitzustellen (Ziff. 4.2.1).

9. Ein modernes Datenschutzrecht hat dem Charakter des Datenschutzgrundrechts als Kommunikationsgrundrecht Rechnung zu tragen und zur Kenntnis zu nehmen, dass Daten zunehmend als Ware behandelt werden. Dabei gilt es, die Kommerzialisierung der informationellen Selbstbestimmung wenigstens in Schranken zu halten. Diesem Ziel entspricht auch der gemeinsame Standpunkt der deutschen Aufsichtsbehörden, den sie in den Anwendungshinweisen zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke dargelegt haben (s. Ziff. 8.2).

1. Einführung

1.1
Allgemeines

Die sprunghafte Entwicklung der Informationstechnologie stellte auch im Berichtszeitraum hohe Anforderungen an den Datenschutz. Nicht nur die Gesetzgeber in Bund und Ländern sahen sich gezwungen – nach Maßgabe einer intensiven Rechtsprechung des Bundesverfassungsgerichts – Regelungen zum Schutz der informationellen Selbstbestimmung zu erlassen. Vor allem auch die Aufsichtsbehörden sahen sich mit einer Aufgabenzunahme konfrontiert, die alles bisher da gewesene in den Schatten stellte. Die Übergangsphase nach der Zusammenlegung von privatem und öffentlichem Bereich beim HDSB zeigt immer noch Auswirkungen. Die vom HDSB auch im Berichtszeitraum unternommen Anstrengungen, in der Bevölkerung das Bewusstsein von der Notwendigkeit der Datensparsamkeit zu vertiefen, fand eine – unerwünschte – Bestätigung durch das Bekanntwerden von Abhöraktivitäten ausländischer Nachrichtendienste in Deutschland, die zum alles beherrschenden Datenschutzthema des Jahres 2013 wurden. Dadurch gerieten andere datenschutzrechtliche Problembereiche wie die Europäische Nivellierung der Datenschutzstandards, die Unkontrollierbarkeit sozialer Netzwerke, die zunehmende Bespitzelung privater Nachbarn mithilfe von Videokameras unverdient aus dem Blickfeld. Sie sind jedoch im Detail Gegenstand dieses Tätigkeitsberichtes, sodass sich die Einführung auf wenige Bemerkungen zur allgemeinen datenschutzrechtlichen Entwicklung beschränken kann.

1.2
Abhöraktivitäten ausländischer Nachrichtendienste in Hessen

Es ist weder die Aufgabe des Hessischen Datenschutzbeauftragten, noch besteht die Möglichkeit, die aus den Äußerungen des ehemaligen Mitarbeiters des US-amerikanischen Geheimdienstes NSA (National Security Agency) bekannt gewordenen Überwachungsaktivitäten in Europa und Deutschland einer umfassenden datenschutzrechtlichen Würdigung zu unterziehen. Nach den bisher vorliegenden Erkenntnissen muss aber jedenfalls davon ausgegangen werden, dass US-amerikanische und britische Nachrichtendienste anlasslos massenhaft Telekommunikationsverkehre auch in Hessen überwacht haben. Es sollte sich von selbst verstehen, dass auch bei der TK-Überwachung befreundeter Dienste in Deutschland deutsches Recht nicht nur zu achten, sondern strikt zu beachten ist. In diesem Sinne habe ich mich mehrfach geäußert und für den Fall eklatanter Verstöße gegen deutsches Recht auf die Möglichkeit hingewiesen, bei meiner Kontrolle unter-

liegenden Datentransfers in die USA die Datenübermittlung nach Art. 3 Abs. 1 des sog. Safe Harbor-Abkommens auszusetzen.

1.3
Europa

Die in den vorangegangenen Tätigkeitsberichten geäußerten verfassungsrechtlichen Bedenken gegen eine europäische Grundverordnung halte ich ebenso aufrecht wie das Bekenntnis zur Notwendigkeit einer Fortentwicklung des europäischen Datenschutzrechtes. Um dieses Bekenntnis deutlicher zum Ausdruck zu bringen wurde das 20. Wiesbadener Forum Datenschutz zum Thema „Globalisierung und Datenschutz“ am 17. Mai 2013 durchgeführt und dem Kabinettschef des EU-Justizkommissariats Prof. Dr. Martin Selmayr Gelegenheit gegeben, die Position der Kommission noch einmal darzulegen. Eine Annäherung unserer unterschiedlichen Standpunkte konnte allerdings nicht erreicht werden. Ähnlich wie der Europaabgeordnete Jan Philipp Albrecht nahm Prof. Selmayr den Nachrichtendienst-Skandal zum Anlass, die Notwendigkeit eines einheitlichen europäischen Regelwerks zu betonen. Dabei wurde ignoriert, dass nicht nur US-, sondern auch britische Nachrichtendienste gegen deutsches Datenschutzrecht verstoßen haben, sodass letztlich nur die Möglichkeit bleibt, eigenverantwortlich für den gebotenen Datenschutz geeignete Maßnahmen zu ergreifen.

1.4
Öffentlichkeitsarbeit

Nicht nur das 20. Wiesbadener Forum Datenschutz bot Anlass, die Position des HDSB darzustellen, sondern auch eine Vielzahl weiterer öffentlicher Veranstaltungen wie beispielsweise das Gesundheitsforum vom 22. Juni 2013 mit der Landesärztekammer in Bad Nauheim.

1.5
Soziale Netzwerke

Die weitgehende Unkontrollierbarkeit des Datenflusses bei sozialen Netzwerken, insbesondere der Zugriff von ausländischen Nachrichtendiensten und die geringe Wirksamkeit von Verschlüsselungen bereiten Sorgen und bieten Anlass, nach Lösungsmöglichkeiten zu suchen.

1.6
Bundesverfassungsgericht

Das Bundesverfassungsgericht traf auch im Berichtszeitraum grundlegende Entscheidungen zur informationellen Selbstbestimmung. An erster Stelle zu nennen ist das Urteil vom 24. April 2013 – 1BvH 1215/07 – zur informationellen Trennung von Polizei und Nachrichtendiensten. Die Entscheidung stellt einen praktikablen Kompromiss zwischen den Belangen der Polizei und des Datenschutzes dar (in die gleiche Richtung zielt bereits Ronellenfitsch, Abschied vom Trennungsgebot, in: Verfassungsschutz in der freiheitlichen Demokratie, 60 Jahre Landesamt für Verfassungsschutz 2011, S. 71 ff.). Über die Tragweite eines „normalen“ Kammerbeschlusses hinaus gehen auch die Ausführungen im Beschluss vom 17. Juli 2013 - 1BvR 3167/08 - zum Datenschutz im privaten Versicherungsrecht. Die Entscheidungen stellen einen wichtigen Beitrag zur Fortentwicklung des Datenschutzrechtes dar und zeigen, wie unverzichtbar das Bundesverfassungsgericht auch im Hinblick auf die europäischen Tendenzen der Depossedierung der nationalen Verfassungsrechtssprechung und der Datenschutzaufsicht durch europäische Vereinnahmungen und wie inakzeptabel die Vereinnahme der nationalen Datenschutzaufsicht durch europäische Gremien ist.

1.7
Gesetzgebungsanregungen

Zahlreiche datenschutzrechtliche Probleme lassen sich durch eine vernünftige Gesetzesinterpretation lösen. Die unterschiedlichen Standpunkte sind aber vielfach so fest gefahren, dass eine Konfliktlösung durch den Gesetzgeber angezeigt erscheint. Beispielsweise ist die datenschutzrechtliche Relevanz von Videoüberwachung durch Attrappen umstritten. Die hessische Landesregierung hat sich in ihrer Stellungnahme zu meinem 41. Tätigkeitsbericht der wohl herrschenden Ansicht angeschlossen, dass Attrappen nicht vom Datenschutzrecht erfasst würden. Zur Begründung wird ausgeführt, durch Attrappen fände keine Beobachtung mit optisch-elektronischen Einrichtungen statt. Das trifft bei vordergründiger Betrachtung selbstverständlich zu. Datenschutz bedeutet aber nicht Schutz von Daten um ihrer selbst willen. Das „Datenschutzgrundrecht“ ist in Wirklichkeit das Grundrecht auf informationelle Selbstbestimmung. Durch den Umgang mit Informationen Betroffener soll deren Verhalten gesteuert werden. Vor derartiger Fremdbestimmung sind die Betroffenen zu schützen. Attrappen greifen in dieses Selbstbestimmungsrecht ebenso ein wie echte optisch elektronische Einrichtungen. Wie beim polizeilichen Anscheinsstörer kommt es auf die Wirkung beim Betroffenen an. Wenn aber selbst im eingriffsintensiven Polizeirecht Maßnahmen gegen Personen zulässig sind, von denen keine reale Gefahr ausgeht, dann müssen zum Schutz der informationellen Selbstbestimmung ebenfalls effektive Maßnahmen möglich sein. Zwischen Attrappen

und Anscheinsstörung besteht kein qualitativer rechtlicher Unterschied. Es bleibt dabei, dass Attrappen wie echte Videokameras zu behandeln sind (s. auch Ziff. 4.2.3). Gleichwohl wäre eine klärende Regelung des Gesetzgebers sinnvoll und hilfreich. Die Videoüberwachung sollte generell in einer Novelle des Hessischen Datenschutzgesetzes geregelt werden (s. meine Ausführungen in Ziff. 4.2.2).

1.8
Arbeitsschwerpunkte und Statistik

1.8.1
Innerbehördliche Konsolidierung

Nach dem organisatorischen und personellen Aufbau der Behörde als gemeinsame Kontrollstelle für den öffentlichen und nicht öffentlichen Bereich waren innerbehördliche Prozesse und Abläufe zu überarbeiten und neue Strukturen aufzubauen. Die Einarbeitung des neu gewonnenen Personals nahm breiten Raum ein. Schließlich musste gegen Ende des Berichtszeitraums bereits begonnen werden, eine tragfähige und möglichst mittelfristig stabile Raumlösung für die gesamte Dienststelle zu erarbeiten, da ein Teil der Dienststelle bisher nur interimsweise außerhalb des Hauptgebäudes untergebracht ist.

1.8.1.1
Arbeitsschwerpunkte

Für anlassunabhängige Prüfungen war infolge der Notwendigkeit für vorhandene und neue Beschäftigte, sich in die neuen Aufgabengebiete einzuarbeiten, kaum Kapazität vorhanden. Es hat sich herausgestellt, dass die Personaldecke für die Bewältigung der Aufgaben eher knapp bemessen ist.

Deshalb wurden im Berichtszeitraum nahezu ausschließlich Eingaben und Beratungsanfragen bearbeitet sowie anlassbezogene Prüfungen vor Ort durchgeführt. Eingabenintensiv sind nach wie vor die Themen Auskunfteien/Inkassounternehmen, elektronische Kommunikation und Internet, Beschäftigtendatenschutz, Wohnen/Miete/Nachbarschaft (überwiegend wegen der in diesem Bereich anzutreffenden hohen Zahl von Videoüberwachungen), Adresshandel/Werbung, Justiz/Polizei/Strafverfolgung, Gesundheit und Soziales, Kreditwirtschaft sowie fachübergreifend das Thema Videoüberwachung, das erstmals in der Statistik erfasst wurde.

Arbeitsintensiv und sehr komplex sind ferner die Fragestellungen auf dem Gebiet des internationalen Datenverkehrs. Hier hat sich die Situation durch die Unsicherheit der Unternehmen infolge der „Überwachungsaffäre“ durch fremde Geheimdienste noch verschärft. Es gab auch im Jahr 2013 einen erheblichen Beratungsbedarf der Unternehmen, insbesondere zur Klärung der Frage, ob Datenübermittlungen in das außereuropäische Ausland überhaupt noch bzw. unter welchen Rahmenbedingungen diese zulässig sind und ob jetzt frühere Genehmigungen hinfällig sind. Häufig waren auch in diesem Jahr aufwändige Ermittlungen zur Sachlage und zu den technischen Rahmenbedingungen im internationalen Datenverkehr erforderlich. Die Fragestellungen sind hier so komplex und speziell, dass sie sich nicht für eine Darstellung im Tätigkeitsbericht eignen.

Für das Einleiten und Betreiben von Ordnungswidrigkeitenverfahren sowie andere Sanktions- und Meldungsregelungen nach dem BDSG (Zwangsgelder, Meldung von Datenpannen) wurden die organisatorischen Vorgaben wie auch die Maßnahmen zur Sicherstellung einer einheitlichen Handhabung verfeinert. In diesem Bereich findet auch eine ständige Abstimmung mit den anderen Aufsichtsbehörden – u.a. in der AG Sanktionen des Düsseldorfer Kreises – statt (zu den Ordnungswidrigkeitenverfahren s.a. Ziff. 4.1.1, zu den Meldungen nach § 42a BDSG s. Ziff. 4.1.2).

1.8.1.2
Statistik

In nachfolgender Tabelle sind Angaben zur Anzahl der Eingaben und Beratungsanfragen enthalten. Diese Statistik wurde weitgehend automationsgestützt mit Hilfe des eingesetzten Dokumentverwaltungssystems erstellt. Hiermit konnten jedoch nicht die Eingaben und Anfragen erfasst werden, die mich telefonisch erreichten und auch telefonisch erledigt wurden, ohne dass sie einen Niederschlag in Akten gefunden haben. Da dies einen ebenfalls nicht zu vernachlässigenden Aufwand verursacht, habe ich als Stichprobe die Novemberzahlen aufzeichnen lassen und diese für das Jahr hochgerechnet. Diese Zahl ist nicht auf die Fachgebiete heruntergebrochen. Erstmals wurden auch Eingaben und Beratungen gezählt, die Videoüberwachungen betreffen, die ansonsten in den bei den Fachgebieten aufgeführten Zahlen enthalten sind.

Arbeitsstatistik des Hessischen Datenschutzbeauftragten

Dokumentierte Eingaben

Fachgebiet	Anzahl
Auskunfteien und Inkassounternehmen	306
Wohnen, Miete und Nachbarschaft	225
Elektronische Kommunikation	160
Werbung und Adresshandel	125
Kreditwirtschaft	114
Beschäftigtendatenschutz	105
Polizei, Justiz, Strafvollzug und Gerichte	102
Soziales	97
Gesundheitswesen	88
Schulen und Hochschulen	79
Verkehr und Daseinsvorsorge	79
Kommunen	58
Handel und Handwerk	42
Versicherungen	29
Vereine und Verbände	23
Rundfunk, Fernsehen, Presse	23
Forschung, Planung und Statistik	21
Sonstiges	73
Summe der dokumentierten Eingaben	**1.749**
Summe der dokumentierten Beratungsanfragen	**333**
davon Eingaben und Beratungen Videoüberwachung betreffend	202
Summe der telefonischen Eingaben und Beratungen	**5.076**
Gesamtsumme	**7.158**

Beratungen waren in aller Regel deutlich aufwändiger als die Bearbeitung von Eingaben (z.B. Beratungen für komplexe Auftragsverhältnisse aus den unterschiedlichsten Fachgebieten, zu Binding Corporate Rules (BCR), grenzüberschreitendem Datenverkehr, zur datenschutzgerechten Ausgestaltung von Beförderungsbedingungen eines Verkehrsunternehmens, zu Cloud-Computing, zur Ausgestaltung der Spielersperrdatei, zur datenschutzgerechten Gestaltung von Forschungsprojekten). Das Spektrum ist ebenso breit wie bei den Eingaben.

Im Berichtszeitraum beschäftigten mich auch wieder Ordnungswidrigkeitenverfahren. In 31 Fällen wurden neue Ordnungswidrigkeitenverfahren anhängig. In diesem Jahr habe ich 29 Verfahren eingestellt sowie fünf Verfahren mit einer Geldbuße abgeschlossen.

Erstmals habe ich in diesem Jahr in zwei Fällen von der Möglichkeit Gebrauch gemacht, einen Strafantrag gemäß § 44 Abs. 2 BDSG zu stellen.

Die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG führte zu 96 Meldungen bei mir. Davon waren 45 Meldungen tatsächlich solche, in denen eine Pflicht zur Information der Aufsichtsbehörde bestand.

2. Übergreifende Themen (öffentlicher und nicht öffentlicher Bereich)

2.1 Querschnittsthemen

2.1.1
Der Abwesenheitskalender

Die Abwesenheit einer bzw. eines Beschäftigten darf in einem Abwesenheitskalender nur neutral vermerkt werden. Erläuternde Zusätze wie z.B. „krank“ oder „Urlaub“ sind unzulässig.

In vielen Behörden werden sogenannte Abwesenheitskalender geführt, mit denen man darüber informiert, welche Mitarbeiterinnen und Mitarbeiter abwesend sind. Dass ich hierzu immer wieder Anfragen erhalte, zeigt, dass die Bedingungen, unter denen ein solcher Kalender datenschutzgerecht geführt werden kann, nicht überall bekannt sind.

Konkret hat eine Lehrerin angefragt, ob es zulässig sei, die Schülerinnen und Schüler über ausfallenden Unterricht zu informieren, indem man den betroffenen Kurs, das Namenskürzel der Lehrkraft und z.B. die Bemerkung „krank“ auf der Homepage der Schule im Internet veröffentlicht.

Eine weitere Anfrage kam aus einer Kindertagesstätte, in der auf einer Tafel mit Fotos der einzelnen Erzieherinnen festgehalten wurde, wer anwesend, krank oder im Urlaub war.

Den Maßstab, an dem derlei Sachverhalte aus datenschutzrechtlicher Sicht zu messen sind, bildet § 34 Abs. 1 und 2 HDSG:

§ 34 HDSG

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

(2) Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches

Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

Das Führen eines Abwesenheitskalenders selbst lässt sich in den meisten Fällen mit einer innerdienstlichen planerischen oder organisatorischen Notwendigkeit, etwa für die Koordination von Besprechungsterminen, begründen. Auch in der Kommunikation mit Bürgern wird es als erforderlich anzusehen sein, dass man z.B. über die Erreichbarkeit eines Mitarbeiters Auskunft geben kann.

So habe ich auch in den beiden Ausgangsfällen ein dienstliches Erfordernis gesehen, die Schülerinnen und Schüler über ausfallenden Unterricht beziehungsweise die Eltern und Kinder über die anwesenden Erzieherinnen zu informieren.

Um diese Zwecke zu erreichen, ist es jedoch ausreichend, abstrakt darüber zu informieren, wer abwesend oder umgekehrt wer anwesend ist. In der Praxis hat sich hierfür der Hinweis „außer Haus“ bewährt. Eine darüber hinausgehende Information, aus welchen Gründen ein Beschäftigter oder eine Beschäftigte an- oder abwesend ist, ist dagegen nicht erforderlich und daher unzulässig. Für den Fall der Veröffentlichung des ausfallenden Unterrichts auf der Schulhomepage ist meines Erachtens auch die Angabe des Lehrerkürzels nicht erforderlich im Sinne des § 34 Abs. 2 HDSG, wenn es eindeutige Kursbezeichnungen gibt.

Das Gesagte gilt ebenso für Unternehmen, die vergleichbare Kalender führen und für die nicht die Regelungen des HDSG, sondern die des BDSG maßgeblich sind. Auch die nach BDSG einschlägigen Vorschriften erlauben eine Verarbeitung von Daten Beschäftigter nur insoweit, als dies erforderlich ist, um einen gesetzlich gebilligten Zweck zu erreichen.

2.1.2
Zentrale Spielersperrdatei nach Glücksspielstaatsvertrag und Hessischem Spielhallengesetz

Abfragen bei der zentralen Spielersperrdatei müssen laut Gesetz protokolliert werden. Umfang und Dauer der Speicherung der Protokolldaten sind auf ein Mindestmaß zu beschränken. Bei Lotterien ohne besonderes Gefährdungspotenzial darf kein Abgleich mit der Spielersperrdatei vorgenommen werden, das gilt auch, wenn die Spielteilnahme online erfolgt. Die Spielhallen können nicht an die zentrale Spielersperrdatei nach § 23 GlüStV angeschlossen werden.

Zur Bekämpfung der Glücksspielsucht schreibt der Glücksspielstaatsvertrag vom 15. Dezember 2011 die Errichtung einer zentralen bundesweiten Spielersperrdatei vor (§§ 8 und 23). Die Datei wird von der Hessischen Zentrale für Datenverarbeitung im Auftrag des HMDIS geführt.

§ 8 GlüStV

(1) Zum Schutz der Spieler und zur Bekämpfung der Glücksspielsucht wird ein übergreifendes Sperrsystem (§ 23) unterhalten.

(2) Spielbanken und Veranstalter von Sportwetten und Lotterien mit besonderem Gefährdungspotential sperren Personen, die dies beantragen (Selbstsperre) oder von denen sie aufgrund der Wahrnehmung ihres Personals oder aufgrund von Meldungen Dritter wissen oder aufgrund sonstiger tatsächlicher Anhaltspunkte annehmen müssen, dass sie spielsuchtgefährdet oder überschuldet sind, ihren finanziellen Verpflichtungen nicht nachkommen oder Spieleinsätze riskieren, die in keinem Verhältnis zu ihrem Einkommen oder Vermögen stehen (Fremdsperre).

(3) Die Sperre beträgt mindestens ein Jahr. Die Veranstalter teilen die Sperre dem betroffenen Spieler unverzüglich schriftlich mit.

(4) Die Veranstalter haben die in § 23 Abs. 1 genannten Daten in eine Sperrdatei einzutragen. Ein Eintrag ist auch zulässig, wenn nicht alle Daten erhoben werden können.

(5) Eine Aufhebung der Sperre ist frühestens nach einem Jahr und nur auf schriftlichen Antrag des Spielers möglich. Über diesen entscheidet der Veranstalter, der die Sperre verfügt hat.

(6) Zum Schutz der Spieler und zur Bekämpfung der Glücksspielsucht sind die Vermittler von öffentlichen Glücksspielen verpflichtet, an dem übergreifenden Sperrsystem (§ 23) mitzuwirken. Zu diesem Zweck übermitteln die Vermittler die bei ihnen eingereichten Anträge auf Selbstsperren unverzüglich an den Veranstalter nach § 10 Abs. 2, in dessen Geltungsbereich der Spieler seinen Wohnsitz hat.

§ 23 GlüStV

(1) Mit der Sperrdatei, die zentral von der zuständigen Behörde des Landes Hessen geführt wird, werden die für eine Sperrung erforderlichen Daten verarbeitet und genutzt. Es dürfen folgende Daten gespeichert werden:

1. Familiennamen, Vornamen, Geburtsnamen,

2. Aliasnamen, verwendete Falschnamen,
3. Geburtsdatum,
4. Geburtsort,
5. Anschrift,
6. Lichtbilder,
7. Grund der Sperre,
8. Dauer der Sperre und
9. meldende Stelle.

Daneben dürfen die Dokumente, die zur Sperrung geführt haben, gespeichert werden.

(2) Die gespeicherten Daten sind im erforderlichen Umfang an die Stellen zu übermitteln, die Spielverbote zu überwachen haben. Die Datenübermittlung kann auch durch automatisierte Abrufverfahren erfolgen.

(3) Datenübermittlungen an öffentliche Stellen, insbesondere an Strafverfolgungsbehörden und Gerichte, sind nach den gesetzlichen Vorschriften zulässig.

(4) Erteilte Auskünfte und Zugriffe im elektronischen System sind zu protokollieren.

(5) Die Daten sind sechs Jahre nach Ablauf der Sperre zu löschen. Es ist zulässig, die Löschung am Ende des sechsten Jahres vorzunehmen.

(6) Soweit in diesem Staatsvertrag nichts anderes bestimmt ist, sind die jeweiligen Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden

Das Hessische Spielhallengesetz vom 28. Juni 2012 verlangt ebenfalls die Errichtung einer Spielersperrdatei (§§ 6 und 11). Veranstalter bestimmter Glücksspiele und die hessischen Spielhallenbetreiber müssen, bevor sie einer Person die Teilnahme am Glückspiel gestatten, durch Abfrage bei der zentralen Spielersperrdatei überprüfen, ob für den Betroffenen eine Sperre eingetragen ist. Gesperrte Spieler dürfen nicht am Glücksspiel teilnehmen.

§ 6 Hessisches Spielhallengesetz

(1) Zum Schutz der Spielerinnen und Spieler und zur Bekämpfung der Glücksspielsucht wird ein Sperrsystem (§ 11) unterhalten. Die Erlaubnisinhaberin oder der Erlaubnisinhaber ist verpflichtet, an dem Sperrsystem mitzuwirken und zu diesem Zweck mit der Betreiberin oder dem Betreiber des Systems eine Vereinbarung abzuschließen.

(2) Die Erlaubnisinhaberin oder der Erlaubnisinhaber sperrt Personen, die dies bei ihr oder ihm beantragen (Selbstsperre) und schließt die Betroffenen vom Spiel aus. Die Verpflichtungen zur Aufnahme in die Sperrdatei und zum Spielausschluss gelten auch bei Personen, von denen die Erlaubnisinhaberin oder der Erlaubnisinhaber aufgrund der Wahrnehmung des Spielhallenpersonals, von Meldungen Dritter wissen oder sonstiger tatsächlicher Anhaltspunkte annehmen müssen, dass sie spielsuchtgefährdet oder überschuldet sind, ihren finanziellen Verpflichtungen nicht nachkommen oder Spieleinsätze riskieren, die in keinem Verhältnis zu ihrem Einkommen oder Vermögen stehen (Fremdsperre).

(3) Die Sperre beträgt mindestens ein Jahr. Die Erlaubnisinhaberin oder der Erlaubnisinhaber teilt die Sperre den Betroffenen unverzüglich schriftlich mit.

(4) Die Erlaubnisinhaberin oder der Erlaubnisinhaber trägt die in § 11 genannten Daten in die Sperrdatei ein. Der Eintrag ist auch zulässig, wenn nicht alle Daten erhoben werden können.

(5) Eine Aufhebung der Sperre ist frühestens nach einem Jahr und nur auf schriftlichen Antrag der Spielerin oder des Spielers möglich. Über diesen entscheidet die Erlaubnisinhaberin oder der Erlaubnisinhaber, der die Sperre verfügt hat.

(6) Verantwortliche Stelle im Sinne des Datenschutzrechts für die Daten gesperrter Spielerinnen und Spieler ist diejenige Stelle, die die Sperre ausgesprochen hat.

§ 11 Hessisches Spielhallengesetz

(1) Mit der Sperrdatei werden die für eine Sperrung erforderlichen Daten verarbeitet und genutzt. Es dürfen folgende Daten gespeichert werden:

1. Familiennamen, Vornamen, Geburtsnamen,
2. Aliasnamen, verwendete Falschnamen,
3. Geburtsdatum,
4. Geburtsort,
5. Anschrift,
6. Lichtbilder,
7. Grund der Sperre,
8. Dauer der Sperre und
9. meldende Spielhalle.

Daneben dürfen die Dokumente, die zur Sperrung geführt haben, gespeichert werden.

(2) Die gespeicherten Daten sind im erforderlichen Umfang an die Spielhallen zu übermitteln, die die Spielverbote zu überwachen haben. Die Datenübermittlung kann auch durch automatisierte Abrufverfahren erfolgen.

(3) Datenübermittlungen an öffentliche Stellen, insbesondere an Strafverfolgungsbehörden und Gerichte, sind im Rahmen bestehender gesetzlicher Verwendungsregeln zulässig.

(4) Erteilte Auskünfte und Zugriffe im elektronischen System sind zu protokollieren.

(5) Die Daten sind sechs Jahre nach Ablauf der Sperre zu löschen.

(6) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweiligen Vorschriften für den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet oder genutzt werden.

(7) Die für den Betrieb des Sperrsystems zuständige Behörde wird durch die für das Glücksspielwesen zuständige Ministerin oder den hierfür zuständigen Minister im Einvernehmen mit der Ministerin oder dem Minister der Finanzen durch Rechtsverordnung bestimmt. Der zuständigen Behörde kann in der Rechtsverordnung gestattet werden, dritte Personen mit dem Betrieb des Sperrsystems zu beauftragen. In der Rechtsverordnung können Einzelheiten zur Einrichtung und Ausgestaltung des Sperrsystems getroffen werden.

Neben der Landesregierung und mehreren Glücksspielverbänden haben sich auch etliche Betreiber von Spielhallen im Zusammenhang mit der Einführung der zentralen Spielersperrdatei von meiner Behörde beraten lassen.

2.1.2.1
Protokollierung der Abfragen

Nach § 23 Abs. 4 GlüStV und § 11 Abs. 4 Hessisches Spielhallengesetz sind Zugriffe auf die Sperrdatei und Auskünfte aus der Datei zu protokollieren. Die im Protokollierungskonzept, das mir die Landesregierung im Sommer 2013 vorgelegt hat, vorgesehene Protokollierung ist jedoch, was Dauer und Umfang betrifft, unverhältnismäßig. Die Protokollierung der Abfragen führt zu einer personenbezogenen Speicherung des Spielverhaltens des betroffenen Spielers. Das gilt auch, wenn die Abfrageparameter wie im Konzept der Landesregierung als Hashwert gespeichert werden. Es bleiben in diesem Fall personenbeziehbare Daten, die datenschutzrechtlich wie unmittelbar perso-

nenbezogene Daten zu behandeln sind (§ 2 Abs. 1 i.V.m. § 1 Abs. 1 Satz 1 HDSG). Die Protokolldaten sollen vier Jahre gespeichert werden. Anhand der geplanten Protokollierung könnte somit für einen Zeitraum von vier Jahren verfolgt werden, wer wann an welchem Glückspiel in Deutschland teilgenommen hat. Die Landesregierung begründet die lange Speicherdauer mit der Verjährungsfrist möglicher Haftungsansprüche eines gesperrten Spielers, der trotz eingetragener Sperre spielen konnte.

Sie konnte allerdings nicht darlegen, ob und wenn ja wie viele Haftungsfälle es in der Vergangenheit gab, in denen sich Spieler darauf berufen haben, zum Spiel zugelassen worden zu sein, obgleich bei der Abfrage bei der bereits existierenden zentralen Sperrdatei der deutschen Spielbanken und des deutschen Toto- und Lotto-Blocks die Eintragung einer Sperre angezeigt worden sei. Die Haftungsgefahr für das Land dürfte eher gering sein. Zunächst würde der Spieler sicherlich vom Veranstalter Schadensersatz verlangen, der dann evtl. das Land in Regress nehmen könnte. Als Haftungsgrund käme nur ein vom HMDIS zu vertretener Bearbeitungs- und/oder Übertragungsfehler beim Abgleich mit der Sperrdatei in Betracht. Beweispflichtig hierfür wäre der Veranstalter. Zur Abwehr haftungsrechtlicher Ansprüche dürfte ausreichen, wenn die verantwortliche Stelle eine regelmäßige Kontrolle der Funktionsfähigkeit des Abfragesystems nachweist. Es erscheint zudem nicht sehr lebensnah, dass ein Spieler erst nach Jahren behauptet, eine für ihn eingetragene Sperre sei beim Abgleich nicht angezeigt worden, sodass er zur Teilnahme am Glücksspiel zugelassen worden sei und dabei – hohe – Verluste erlitten habe.

Das relativ geringe Haftungsrisiko des Landes kann nicht eine Protokollierung des gesamten Spielverhaltens sämtlicher Glücksspielteilnehmer in Deutschland über einen Zeitraum von vier Jahren rechtfertigen. Eine zeitlich derart lange Protokollierung, nur um in einem Haftungsfall, dessen Umfang und Wahrscheinlichkeit nicht näher dargelegt werden konnte, ein Abwehrinstrument zur Verfügung zu haben, würde gegen das Übermaßverbot verstoßen.

Aus der Protokollierungspflicht des § 23 Abs. 5 GlüStV folgt nichts anderes. Sie ist eine Datensicherheitsregelung und zielt darauf ab, missbräuchliche Abfragen zu erkennen und verhindern. Zu diesem Zweck genügt eine Speicherdauer von wenigen Monaten.

Vertretbar wäre eine längere Protokollierungsdauer allenfalls in den Fällen, in denen den anfragenden Veranstaltern Treffer übermittelt wurden. Der betroffene Spieler ist bereits in der Sperrdatei registriert, es werden lediglich seine Versuche, trotz bestehender Sperre zu spielen, zusätzlich erfasst. Ein schutzwürdiges Interesse des Betroffenen wäre durch die Protokollierung nicht beeinträchtigt.

2.1.2.2
Keine Abfragepflicht für Lotterien ohne besonderes Gefährdungspotenzial

Nur Veranstalter von Lotterien mit besonderem Gefährdungspotenzial, Spielbanken und Veranstalter von Sportwetten sind verpflichtet, an einem bundesweiten Spielersperrsystem teilzunehmen (§ 8 Abs. 2 und 4 GlüStV). Vermittler von öffentlichen Glückspielen sind gem. § 8 Abs. 6 GlüStV verpflichtet, an dem Sperrsystem mitzuwirken, indem sie die bei ihnen eingereichten Anträge auf Selbstsperrung an den zuständigen Veranstalter weiterreichen.

Der Glücksspielstaatsvertrag definiert nicht, welche Lotterien ein besonderes Gefährdungspotenzial aufweisen. § 22 Abs. 2 Satz 1 GlüStV regelt, dass gesperrte Spieler an Lotterien mit mehr als zwei Ziehungen pro Woche nicht teilnehmen dürfen.

§ 22 Abs. 2 Satz 1 GlüStV

Gesperrte Spieler dürfen an Lotterien der in § 10 Abs. 2 genannten Veranstalter, die häufiger als zweimal pro Woche veranstaltet werden, nicht teilnehmen.

Daraus lässt sich schließen, dass der GlüStV Lotterien, die nicht mehr als zweimal pro Woche veranstaltet werden, nicht als Lotterien mit besonderem Suchtgefährdungspotenzial ansieht, da für diese Lotterien keine Spielersperren vorgesehen sind. Für die populärste Lotterie „6 aus 49“ käme demnach eine Spielersperre nicht in Betracht. Dafür spricht außerdem der Hinweis in der Erläuterung zu § 8 Abs. 2 (Spielersperre) des Staatsvertragsentwurfs, Lotterien mit besonderem Gefährdungspotenzial seien die in § 22 aufgeführten Jackpotlotterien und Lotterien, die häufiger als zweimal pro Woche veranstaltet würden. § 22 regelt Lotterien mit planmäßigem Jackpot, d.h. Lotterien, bei denen planmäßig Teile der Spieleinsätze angesammelt werden, um die Gewinnsumme für künftige Ziehungen bereitzustellen. Bei der Lotterie „6 aus 49“ entsteht der Jackpot dagegen nicht planmäßig, sondern kommt durch nicht angefallene oder nicht abgeholte Gewinne zustande, er ist rein zufallsabhängig.

Den schon seit Jahrzehnten betriebenen Glücksspielen wie „6 aus 49“ (seit Mitte der 1950er Jahre), „Glücksspirale“ (seit 1969), „Spiel 77“ (seit 1975) oder „Super 6“ (seit 1992) wurde bislang keine besondere Suchtgefährdung beigemessen. Eine breit angelegte Umfrage des VG Halle (Urteil vom 11. November 2010 – Az. 3 A 158/09) bei sämtlichen Betreuungsgerichten der Bundesrepublik und 100 Fachkrankenhäusern für Psychiatrie mit in der Regel mehr als 300 Betten hat ergeben, dass von einer nennenswerten Wett- und Spielsucht im Bereich der Glücksspiele des staatlichen Lotto-Toto-Blocks keine Rede sein kann (a.a.O. S. 54 ff.). Diese Feststellung schließt übri-

gens die staatlichen Sportwetten, die nicht häufiger als zweimal pro Woche veranstaltet werden – wie z.B. die Sportwette „Oddset“ – ein (a.a.O. S. 56 f.).

Die Landesregierung hatte mir mitgeteilt, das Glücksspielkollegium sei der Ansicht, jede im Internet veranstaltete Lotterie sei als Lotterie mit besonderem Suchtgefährdungspotenzial anzusehen und dass daher vor jeder Spielteilnahme eine Abfrage bei der Sperrdatei zu erfolgen habe. Das Glückspielkollegium besteht aus 16 durch die obersten Glücksspielaufsichtsbehörden der Länder benannten Mitgliedern. Es dient den Aufsichtsbehörden als Einrichtung zur Erfüllung ihrer Aufgaben (zu Aufgaben, Status, Zusammensetzung und Verfahren des Kollegiums siehe http://verwaltung.hessen.de/irj/HMdI_Internet?cid=c604097466e63b298d8bf68224eb0334 – Stand 4. Oktober 2013). Aus dem Wortlaut des Glückspielstaatsvertrages ist diese Auffassung nicht zwingend abzuleiten. Erlaubnisvoraussetzung für den Eigenvertrieb und die Vermittlung von Lotterien sowie die Veranstaltung und Vermittlung von Sportwetten im Internet ist nach § 4 Abs. 5 Nr. 1 GlüStV, dass der Ausschluss gesperrter Spieler gewährleistet wird.

§ 4 Abs. 5 Nr. 1 GlüStV

Abweichend von Absatz 4 können die Länder zur besseren Erreichung der Ziele des § 1 den Eigenvertrieb und die Vermittlung von Lotterien sowie die Veranstaltung und Vermittlung von Sportwetten im Internet erlauben, wenn keine Versagungsgründe nach § 4 Abs. 2 vorliegen und folgende Voraussetzungen erfüllt sind:

1. Der Ausschluss minderjähriger oder gesperrter Spieler wird durch Identifizierung und Authentifizierung gewährleistet.

Die Gesetzesformulierung lässt offen, ob die Bedingungen für die Sperrung von Spielern bei Offline-Lotterien (Beschränkung auf Lotterien mit besonderem Gefährdungspotenzial) auch für Online-Lotterien gelten. Lediglich in der Erläuterung zu § 4 Abs. 5 GlüStV findet sich die Forderung, dass ein durchgehender Ausschluss gesperrter Spieler bei Lotterien und Sportwetten im Internet gewährleistet sein müsse. Unter Berufung auf ein Urteil des EuGH vom 30. Juni 2011 (Rs. C-212/08 – Zeturf) wird dabei für die Bewertung, ob eine Lotterie ein besonderes Gefährdungspotenzial aufweist, anscheinend allein auf den Vertriebskanal Internet abgestellt, da Glückspiele im Internet ein erheblich höheres Gefährdungspotenzial hätten als traditionelle Vertriebskanäle und mit ihnen nicht austauschbar seien (Erläuterungen zu § 4 Abs. 5 GlüStV – S. 17). Danach käme es nicht darauf an, ob die (Offline-) Lotterie an sich (wie z.B. im Fall der Hochfrequenz-Lotterie) ein besonderes Suchtgefährdungspotenzial birgt, sondern die höhere Suchtgefährdung wird allein dem Vertriebskanal zugeschrieben. Eine Spielersperre wäre dann auch für „6 aus 49“ geboten,

soweit die Lotterie im Internet veranstaltet oder vermittelt wird. An der offline veranstalteten Lotterie „6 aus 49“ könnten gesperrte Spieler indessen weiterhin teilnehmen.

Die in der Erläuterung zum Staatsvertrag enthaltene Begründung für eine restriktivere Regulierung der Teilnahmeberechtigung an Internetglücksspielen beruht auf einer verkürzten Interpretation des EuGH Urteils. Der EuGH stellt bei der Beurteilung des Suchtgefährdungspotenzials gerade nicht allein auf den Vertriebskanal Internet ab. Er erkennt zwar an, dass die Besonderheiten des Angebots von Glücksspielen im Internet zu einem größeren Gefahrenpotenzial führen können, verlangt aber eine Prüfung, ob die Nutzung des Internets die mit den traditionellen Vertriebskanälen verbundene Gefährdung verstärkt (a.a.O. Leitsatz 2 und Rdnr. 82). Es ist nicht ersichtlich, warum der Erwerb eines Lottoscheines im Internet eine größere Suchtgefahr bergen soll als der Erwerb in einer Lottoannahmestelle.

Die Sinnhaftigkeit eines Ausschlusses gesperrter Spieler von einer Teilnahme am Lottospiel im Internet ist auch besonders deshalb zweifelhaft, weil der Spieler problemlos in einer der ca. 25.000 Lottoannahmestellen spielen könnte.

Da absehbar ist, dass sich in Zukunft ein großer Teil des Glücksspiels in das Internet verlagern dürfte, fragt sich zudem, weshalb es dann noch der besonderen Regelungen zu Spielersperren bei den einzelnen Glücksspielen Sportwetten (§ 21 Abs. 5), Lotterien (§ 22 Abs. 2) und Festquotenpferdewetten (§ 27 Abs. 3) bedurfte.

Fazit: Der Glücksspielstaatsvertrag bietet keine Rechtgrundlage für einen Datenabgleich bei der Zahlenlotterie „6 aus 49“ und anderen Lotterien mit geringem Suchtgefährdungspotenzial.

2.1.2.3
Anbindung der Spielbanken an die Spielersperrdatei nach § 23 GlüStV

Das Hessische Spielhallengesetz sieht ein Sperrsystem vor, an dem sich die Spielhallenbetreiber zu beteiligen haben und zu dessen Kernelement eine zentrale Sperrdatei gehört (§§ 6 und 11). Die Vorschriften sind den Regelungen zum zentralen Sperrsystem nach dem Glücksspielstaatsvertrag nachgebildet (§§ 8 und 23 GlüStV), an dem sich die Spielbanken und die Veranstalter von Sportwetten und Lotterien mit besonderem Gefährdungspotenzial zu beteiligen haben. Die zentrale Sperrdatei nach dem Glücksspielstaatsvertrag wird gem. § 23 Abs. 1 S. 1 GlüStV von der zuständigen Behörde des Landes Hessen (Hessisches Innenministerium) geführt. Die Bestimmung der für die Führung der Sperrdatei nach dem Hessischen Spielhallengesetz verantwortlichen Behörde hat gem. § 11 Abs. 1 Hessisches Spielhallengesetz durch Rechtsverordnung zu erfolgen.

Es bestehen keine datenschutzrechtlichen Einwände dagegen, dass die bei der HZD für die Sperrdatei nach den GlüStV eingerichtete technische Infrastruktur auch für die Sperrdatei nach dem Hessischen Spielhallengesetz genutzt wird.

Fraglich ist jedoch, ob die Sperrdatei nach dem Spielhallengesetz und die Datenbestände nach dem GlüStV in einer Datei geführt werden dürfen, in die die Spielhallenbetreiber die von ihnen verhängten Spielersperren einmelden, die dann auch von den Spielbanken und Sportwetten- und Lotterieveranstaltern in den anderen Bundesländern abgerufen werden können.

Die von den Spielbanken und Veranstaltern von Sportwetten und Lotterien verhängten Spielersperren entfalten aufgrund des GlüStV bundesweite Wirkung. Dagegen gelten die von den Spielhallenbetreibern nach dem Hessischen Spielhallengesetz ausgesprochenen Spielersperren nur für das Gebiet Hessens. Ein von einer hessischen Spielhalle gesperrter Spieler kann problemlos in den Nachbarländern Bayern, Baden-Württemberg, Rheinland-Pfalz, Nordrhein-Westfalen, Niedersachsen oder Thüringen in Spielhallen spielen. Selbst in Baden-Württemberg, das als einziges weiteres Bundesland neben Hessen gesetzliche Spielersperren in Spielhallen geregelt hat, hätte eine hessische Spielersperre keine Auswirkung. Dem hessischen Gesetzgeber fehlt die Kompetenz, eine für hessische Spielhallen ausgesprochene Spielersperre mit einer Wirkung außerhalb Hessens zu versehen. Eine Einmeldung der von hessischen Spielhallenbetreibern verhängten Sperren in die zentrale Sperrdatei nach § 23 GlüStV und damit verbunden die Übermittlung an Glückspielbetreiber in anderen Bundesländern bedarf einer Rechtsgrundlage. Diese findet sich weder im Hessischen Spielhallengesetz noch im Glücksspielstaatsvertrag, der dortige 7. Abschnitt enthält keine Datenverarbeitungsregelungen. In einem landesrechtlichen Spielhallengesetz wäre eine Einmelde- und Übermittlungsregelung ohnehin nur funktionsfähig, wenn in allen anderen Bundesländern, aus denen auf die Datei zugegriffen werden kann, korrespondierende Vorschriften geschaffen würden. Praktikabel wäre daher nur eine staatsvertragliche Regelung wie im GlüStV für Spielbanken, Sportwetten und Lotterien. Nach der derzeitigen Rechtslage ist eine Sperrdatei, in die die Sperren nach dem GlüStV und nach dem Hessischen Spielhallengesetz eingemeldet würden und aus der Daten in andere Bundesländer übermittelt würden, nicht möglich.

Es stellt sich die Frage, ob ein lesender Zugriff der hessischen Spielhallen auf die zentrale Sperrdatei nach § 23 GlüStV oder eine Übernahme und anschließende fortlaufende Aktualisierung des Datenbestandes in eine parallele Spielersperrdatei für Spielhallen durch eine Rechtsverordnung nach § 11 Abs. 7 S. 3 Hessisches Spielhallengesetz ermöglicht werden könnte. Der hessische Landesgesetzgeber hat im Glücksspielstaatsvertrag und im Hessischen Spielhallengesetz die wesentliche Entscheidung getroffen, dass spielsuchtgefährdete Personen nicht an Glücksspielen mit besonderem Suchtgefährdungspotenzial teilnehmen dürfen. Er wertet das Glücksspiel in Spielbanken, die Teil-

nahme an Sportwetten und Lotterien mit besonderem Gefährdungspotenzial und – anscheinend im Gegensatz zu anderen Bundesländern – das Glücksspiel in Spielhallen als gleichermaßen Sucht gefährdend. Für Selbst- und Fremdsperren gelten im GlüStV und im Hessischen Spielhallengesetz dieselben Kriterien. Es wäre daher folgerichtig, dass sich Sperren nach dem GlüStV auch auf das Spielen in hessischen Spielhallen auswirken. Selbst wenn man den Zugriff der Spielhallen auf die zentrale Sperrdatei nach dem GlüStV als Einzelheit der Errichtung und Ausgestaltung des Sperrsystems ansieht, welche die zuständige Behörde aufgrund der Verordnungsermächtigung des § 11 Abs. 7 S. 3 regeln könnte, stünde dem jedoch der Glücksspielstaatsvertrag entgegen. In § 23 Abs. 2 GlüStV ist abschließend geregelt, an welche privaten Stellen die Daten aus der Sperrdatei übermittelt werden dürfen: an die Stellen, die Spielverbote (nach dem GlüStV) zu überwachen haben. Dazu zählen Spielhallen nicht. Der einzelne Landesgesetzgeber kann diese staatsvertragliche Festlegung nicht erweitern. Eine Übermittlung der Daten aus der Sperrdatei nach dem GlüStV würde möglicherweise auch dem Willen der Gesetzgeber einiger anderer Bundesländer, die den Vertrag ratifiziert haben, widersprechen, denn nur Hessen und Baden-Württemberg haben bislang ein Sperrsystem für Spielhallen vorgesehen, in allen anderen Ländern können Spieler trotz Sperre nach dem GlüStV in Spielhallen spielen.

2.1.3
Neues Rahmenkonzept für die vernetzte Forschung

Medizinische Forschung arbeitet zunehmend vernetzt in größeren Forschungsverbünden. Ein zentraler Bestandteil dieser Vernetzung ist die überregionale Zusammenführung und Bereitstellung aller forschungsrelevanten Daten in zentralen Datenbanken und von Proben in zentralen Biobanken. Die Technologie- und Methodenplattform für die vernetzte medizinische Forschung und die Datenschutzbeauftragten des Bundes und der Länder haben die aktuellen grundsätzlichen datenschutzrechtlichen Anforderungen hierfür abgestimmt.

2.1.3.1
Ausgangspunkt der Diskussion

Bereits 2003 haben die Technologie- und Methodenplattform für die vernetzte Forschung e.V. (TMF) und die Datenschutzbeauftragten des Bundes und der Länder sich auf ein grundlegendes Datenschutzkonzept für die medizinische Forschung verständigt, das grundsätzlich auf alle Arten vernetzter medizinischer Forschungsvorhaben in Deutschland übertragbar ist und seitdem Forschungsnetzen als Modelllösung für die jeweilige konkrete Ausgestaltung ihrer Kooperation zur Verfügung gestellt werden kann (32. Tätigkeitsbericht, Ziff. 10.2.2; http://www.tmf-ev.de/Produkte/Uebersicht.aspx,

Reng/Debold/Specker/Pommerening, Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin, MWV 2006). Das Datenschutzkonzept enthält modifizierbare Musterlösungen für verschiedene Varianten von medizinischen Forschungsnetzen (Modell A für klinisch fokussierte Netze und Modell B für wissenschaftlich fokussierte Netze). 2006 wurde darüber hinaus zwischen der TMF und den Datenschutzbeauftragten des Bundes und der Länder ein generisches Datenschutzkonzept für den Aufbau und Betrieb von Biomaterialbanken abgestimmt (35. Tätigkeitsbericht, Ziff. 5.6.2 Simon/Paslack/Robienski/Goebel/Krawczak, Biomaterialbanken – rechtliche Rahmenbedingungen, MWV 2006). Ziel der Konzepte war es, einen angemessenen Schutz der Patientendaten zu gewährleisten und gleichzeitig für die Forschung relevante Datenbestände verfügbar zu machen, insbesondere durch eine angemessene Ausgestaltung von Patienteninformation und -aufklärung, Anonymisierungs- und Pseudonymisierungsverfahren, Treuhändereinsatz und technisch-organisatorische Datensicherheitsmaßnahmen, ferner auch durch vertragliche Regelungen zwischen den kooperierenden Institutionen, die sicherstellen, dass die Verantwortlichkeit für die jeweiligen Bestandteile des Datenschutzkonzepts klar und verbindlich festgelegt ist. Durch die abgestimmten und anschließend von der TMF veröffentlichten Musterlösungen konnte die Umsetzung einheitlicher angemessener Datenschutzstandards wesentlich unterstützt und gefördert werden und sowohl Forscher wie auch Datenschutzbeauftragte von jeweils neuen Einzeldiskussionen entlastet werden. Die Konzepte werden mittlerweile auch weit über die Mitgliedschaft der TMF hinaus genutzt und angewendet und haben allgemeine Standards gesetzt.

2.1.3.2
Neues Rahmenkonzept

Aufgrund der Weiterentwicklung der rechtlichen, technischen und wissenschaftlichen Rahmenbedingungen wurde von der TMF eine Aktualisierung und Erweiterung der o.a. Konzepte als notwendig angesehen und den Datenschutzbeauftragten des Bundes und der Länder 2013 ein neues modulares und flexibles Gesamtkonzept „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten“ vorgestellt. Das Gesamtkonzept enthält jetzt insgesamt vier Module, die je nach Zielrichtung des einzelnen Forschungsverbundes einzeln oder auch kombiniert verwendet werden können:

– Klinisches Modul (bisher Modell A)
– Studienmodul (neu, für klinische Studien, die den Vorschriften des Arzneimittelgesetzes oder des Medizinproduktegesetzes unterliegen)
– Forschungsmodul (bisher Modell B) sowie
– Biobankenmodul (bisher als separates Konzept vorhanden).

Die bisherigen zentralen Ziele einer datenschutzgerechten Ausgestaltung von Patienteninformation und -aufklärung, des Einsatzes von Anonymisierungs- und Pseudonymisierungsverfahren einschließlich Treuhändern sowie angemessener weiterer technisch-organisatorischer Datensicherheitsmaßnahmen wurden beibehalten und nicht grundlegend verändert. Der Leitfaden zeigt verschiedene Wege zum datenschutzgerechten Aufbau von Forschungsverbünden auf. Er verfolgt einen modularen und skalierbaren Ansatz, der verschiedene Schwerpunkte zulässt und auf diese Weise den unterschiedlichen Anforderungen von versorgungsnaher Forschung, klinischen Studien, epidemiologischen Projekten, Biobanken, Registern und Langzeitforschungsprojekten gerecht wird.

Das Gesamtkonzept wurde unter meinem Vorsitz in dem Arbeitskreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder mit der TMF intensiv diskutiert, auch unter Beteiligung des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder. Ziel ist es, nach Abschluss des Abstimmungsprozesses mit der TMF und der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Forschungseinrichtungen und Forschungsverbünden zu empfehlen, den Leitfaden als Basis für die Ausgestaltung ihrer Datenschutzkonzepte zu nehmen.

2.1.4
Akteneinsichtsrecht der Patienten

Auch im vergangenen Jahr gab es wieder einige Eingaben, die Fragen zum Akteneinsichtsrecht der Patientinnen und Patienten betrafen. Das im Jahr 2013 in Kraft getretene Patientenrechtegesetz gab Anlass dazu, sich erneut mit der Thematik zu befassen.

2.1.4.1
Die neue Rechtslage: Regelungen im Patientenrechtegesetz

Mit der Verabschiedung des Patientenrechtegesetzes wollte der Bundesgesetzgeber für eine erhöhte Transparenz und Rechtssicherheit im Bereich der Patientenrechte sorgen. Im Wesentlichen ging es darum, die Vielzahl an Vorschriften, aber auch die Fülle an ergangener Rechtsprechung an einer zentralen Stelle zusammenzufassen und dem Einzelnen zu einer Durchsetzung seiner Ansprüche zu verhelfen. Gewissermaßen als Nebeneffekt hiervon sollte den Patientenrechten damit aber auch eine Bedeutung eingeräumt werden, die so bisher nicht zum Tragen kam.

Die Pflicht zur Gewährung von Akteneinsicht wurde auch im Rahmen des Patientenrechtegesetzes neu normiert. Gemäß § 630g Abs. 1 BGB ist dem Patienten „auf Verlangen unverzüglich Einsicht

in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen“.

Zu begrüßen ist zunächst, dass dem bisher unter § 810 BGB bereits bestehenden, jedoch etwas „versteckten“ Anspruch zur Einsicht in Urkunden aus dem Behandlungsvertrag hiermit eine hervorgehobene Stellung eingeräumt wurde (so auch Thole, MedR 2013, 145, 148).

Zu begrüßen ist ferner die eindeutige Klarstellung des Gesetzgebers, dass das Recht auf Einsicht grundsätzlich sowohl objektive als auch subjektive Daten umfasst. Hierzu heißt es im Referentenentwurf: „Schließlich können Niederschriften über persönliche Eindrücke oder subjektive Wahrnehmungen des Behandelnden betreffend die Person des Patienten letzteren in seinen Persönlichkeitsrechten berühren und sollten dem Patienten daher grundsätzlich offengelegt werden“ (siehe Referentenentwurf, zu § 630g, Einsichtnahme in die Patientenakte, S. 33).

Aus dem Referentenentwurf geht auch hervor, dass der Beschluss des Bundesverfassungsgerichts vom 9. Januar 2006 die Vorschrift maßgeblich mitgeprägt hat (Az. 2 BvR 443/02; NJW 2006, 1116).

Positiv zu bewerten ist schließlich ebenfalls, dass Einschränkungen ausschließlich wegen erheblicher therapeutischer Gründe oder sonstiger erheblicher Rechte Dritter möglich sind (Die Formulierung „oder sonstige Rechte Dritter“ ist allerdings unglücklich. Die therapeutischen Gründe sind ersichtlich patientenbezogen und kein Unterfall der Rechte Dritter.). Damit liegen einheitliche Formulierungen für alle Behandlungssituationen vor. Die Formulierungen müssen selbstverständlich in den nächsten Jahren in der Praxis konkretisiert werden. Normiert ist im Gesetz, dass die Ablehnung der Einsichtnahme zu begründen ist.

Wenn im Einzelfall die Voraussetzungen einer Einschränkung des Einsichtsrechts vorliegen, so muss dies nicht nur begründet werden. Dem Recht auf informationelle Selbstbestimmung muss vielmehr auch dadurch Rechnung getragen werden, dass nach alternativen Möglichkeiten zur umfassenden Akteneinsicht durch den Patienten gesucht wird. Entsprechende Alternativen stellen etwa das Schwärzen von Aktenbestandteilen dar, wie auch die Einsichtnahme unter Zuhilfenahme eines Dritten, z.B. eines Nachbehandlers.

2.1.4.2
Verhältnis der bestehenden Regelungen zueinander

Regelungen zur Akteneinsicht der Patientinnen und Patienten bestehen u.a. auch in den Krankenhausgesetzen der Länder und in den Berufsordnungen für Ärztinnen und Ärzte der Länder. Insoweit wurde hier auch das Verhältnis der verschiedenen Regelungen zueinander untersucht.

Festzuhalten ist zunächst, dass das Patientenrechtegesetz für alle Behandlungsverträge bundesweit gilt. Soweit die zuvor verabschiedeten Landesregelungen und die Berufsordnungen betroffen sind, sind Anpassungen an das Patientenrechtegesetz zumindest wünschenswert. Derzeit lesen sich u.a. Passagen zur Akteneinsicht aus den Krankenhausgesetzen einzelner Länder im Vergleich zu § 630g BGB deutlich anders. Es besteht daher die Gefahr, dass die bundesgesetzlichen Regelungen nicht überall adäquat umgesetzt werden, beziehungsweise dass es Missverständnisse hinsichtlich des Umfangs der Patientenrechte gibt. Die Unsicherheit des Patienten bleibt hierdurch nach wie vor bestehen, selbst wenn im Nachhinein Korrekturen durch Berücksichtigung der Rechtsprechung vorgenommen werden könnten – gerade dieser Effekt sollte jedoch durch das Patientenrechtegesetz vermieden werden.

2.1.4.3
Ausblick

Im Rahmen der EU-Patientenrichtlinie ist mit einer weiteren gesetzlichen Ausgestaltung des Akteneinsichtsrechts von Patienten zu rechnen.

Hinsichtlich der EU-Richtlinie wird den Mitgliedstaaten im Übrigen noch eine Umsetzungsfrist bis Oktober 2013 gewährt. Der Begriff „Patientenakte“ wird in der RL 2011/24/EU wie folgt definiert: „Sämtliche Unterlagen, die Daten, Bewertungen oder Informationen jeglicher Art über die Situation und Entwicklung eines Patienten im Verlauf des Behandlungsprozesses enthalten“. Der ausdrücklichen Nennung von „Bewertungen“ ist dieser Ansicht nach zu entnehmen, dass auch auf europarechtlicher Ebene die subjektiven Elemente der Akte den Kern der Patientenakte darstellen.

Die nach wie vor bestehende Aktualität des Themas lässt sich auch dem Bericht der Unabhängigen Patientenberatung Deutschland (UPD) aus dem Jahr 2013 entnehmen. Demnach waren Fragen zum Recht auf Einsichtnahme in die Krankenunterlagen das mit Abstand häufigste Beratungsthema (s. UPD, Monitor Patientenberatung 2013, Berichtszeitraum 1. April 2012 bis 31. März 2013, S. 13 und 14).

2.1.5
Prüfung der Rollen- und Berechtigungskonzepte für das Klinikinformationssystem in hessischen Krankenhäusern

Als Reaktion auf bundesweit festgestellte Defizite haben die Datenschutzbeauftragten des Bundes und der Länder 2011 eine Orientierungshilfe „Krankenhausinformationssyteme“ veröffentlicht. Eine stichprobenhafte Überprüfung der aktuellen Situation in hessischen Krankenhäusern ergab, dass Rollen- und Berechtigungskonzepte entwickelt und viele Punkte der Orientierungshilfe umgesetzt werden. Probleme habe ich insbesondere bei der Ausgestaltung von begründungsbedürftigen erweiterten Zugriffsmöglichkeiten, der Protokollierung der Zugriffe sowie bei der Sperrung und Löschung der Daten festgestellt.

2.1.5.1
Hintergrund

In meinen vorausgegangenen Tätigkeitsberichten habe ich ausführlich über die bundesweit existierenden Probleme hinsichtlich der Zugriffsausgestaltung in Krankenhausinformationssystemen (38. Tätigkeitsbericht, Ziff. 4.6.2, 39. Tätigkeitsbericht, Ziff. 4.7.1) sowie Inhalt und Ziel der neuen Orientierungshilfe „Krankenhausinformationssysteme (40. Tätigkeitsbericht, Ziff. 3.8.3) berichtet. Die Orientierungshilfe soll Krankenhausträgern, Anwendern, Herstellern und betrieblichen bzw. behördlichen Datenschutzbeauftragten eine detaillierte Orientierung bezüglich der datenschutzrechtlichen Anforderungen insbesondere an ein Rollen- und Berechtigungskonzept ermöglichen. Eine Patientin bzw. ein Patient rechnet nicht damit und muss nicht damit rechnen, dass ihre bzw. seine sensitiven detaillierten medizinischen Daten während der Behandlung – und möglicherweise sogar noch Jahre danach – jederzeit von allen, unter Umständen mehreren tausend Beschäftigten des Krankenhauses zur Kenntnis genommen werden können.

In Hessen ist die Notwendigkeit einer Zugriffsbegrenzung ausdrücklich in § 12 Abs. 3 HKHG geregelt (s. 38. Tätigkeitsbericht, Ziff. 4.6.2.1.1). Im Grundsatz gilt bundesweit, dass Krankenhausbeschäftigten nur dann ein Zugriff auf die Daten eines Patienten bzw. einer Patientin möglich sein darf, wenn sie in die Behandlung einbezogen sind oder die Behandlung verwaltungsmäßig abwickeln.

2.1.5.2
Stichprobenhafte Prüfungen

Meine Dienststelle hat an der Erarbeitung der Orientierungshilfe mitgewirkt und jetzt stichprobenhaft in Krankenhäusern die Umsetzung der Anforderungen geprüft, wobei darauf hinzuweisen ist, dass die Orientierungshilfe Anforderungen zusammenstellt und erläutert, die keineswegs neu sind. Sie konkretisiert die Anforderungen, die sich aus den derzeit bereits geltenden datenschutzrechtlichen Regelungen z.B. in Landeskrankenhausgesetzen, sowie den Vorgaben zur ärztlichen Schweigepflicht i.S.v. § 203 StGB und der Ärztlichen Berufsordnung ergeben.

Positiv habe ich festgestellt:

– Alle stichprobenhaft geprüften Krankenhäuser haben ein differenziertes Rollen- und Berechtigungskonzept erstellt.

– In dem Berechtigungskonzept wird generell nach Benutzergruppen differenziert. Jeder Benutzergruppe werden Gruppenrechte zugeordnet, und darüber hinaus werden teilweise zur genaueren Differenzierung individuelle Rechte an einzelne Benutzer vergeben.

– Differenziert wird bei der Rechtevergabe nach Standardzugriffsberechtigungen und erweiterten Zugriffsberechtigungen in besonderen Situationen (z.B. genannt Sonderuserzugriffsberechtigung, etwa bei Notfall oder Konsil).

– Sammelkennungen wurden nicht eingesetzt.

– Interne Datenschutzbeauftragte waren bestellt und in der Regel in die Diskussionen einbezogen.

Probleme habe ich insbesondere bei den folgenden Punkten festgestellt:

Ausgestaltung der erweiterten begründungsbedürftigen Zugriffsmöglichkeiten

– Gefordert wurde im Regelfall die Eingabe einer Begründung für den beabsichtigten erweiterten Datenzugriff. Allerdings war die Eingabe einer Begründung nicht immer ein technisches Hindernis für den erweiterten Datenzugriff – das Begründungserfordernis konnte teilweise auch schlichtweg ignoriert werden. Es stellte keine technische Hürde für den Zugriff dar.

– Als Begründung für den benötigten erweiterten Datenumfang konnten bestimmte vorformulierte Standardsituationen angeklickt werden – teilweise aber darüber hinaus auch die Begründung „Sonstiges“ – eine Kontrolle dieser Begründung ist kaum denkbar. Diese Begründung wurde nach meinen Feststellungen bevorzugt verwendet.

Protokollierung

– Erweiterte Datenzugriffe z.B. über eine Sonderuserfunktion wurden zwar protokolliert. Die Protokolle waren aber inhaltlich teilweise nicht geeignet, die Berechtigung im Einzelfall nachvollziehen zu können.

– Eine Auswertung der Protokolle insbesondere hinsichtlich der Nutzung der erweiterten Zugriffsmöglichkeiten wurde bisher nicht durchgeführt. Ein schlüssiges Gesamtkonzept, wer in welchem Umfang wann und wie die Protokolle auswertet, welche Maßnahmen bei fehlender Plausibilität des Zugriffs von wem getroffen werden und wie lange die Protokolle aufbewahrt werden, lag nicht vor.

– Eine Sperrung der Patientendaten nach Abschluss und Abrechnung der Behandlung wurde von den eingesetzten Krankenhausinformationssystemen nicht unterstützt, und der Kreis der zugriffsberechtigten Beschäftigten blieb auch nach Abschluss und Abrechnungsabwicklung der Behandlung gleich.

– Löschungen im System konnten nur manuell vorgenommen werden. Ein Löschkonzept lag nicht vor.

Insbesondere habe ich folgende Forderungen aufgestellt:

– Ohne Eingabe einer Begründung darf ein erweiterter Datenzugriff nicht möglich sein.

– Die Begründungen für die Verwendung einer erweiterten Zugriffsberechtigung (z.B. Sonderuserfunktion) müssen inhaltlich vorgegeben werden. Eine Begründung „Sonstiges“ verfehlt das Ziel der Datenschutzmaßnahme. Wenn dafür im Krankenhaus ein zwingender Bedarf gesehen wird, ist zusätzlich ein Freitextfeld denkbar, in dem der besondere Bedarf zu begründen ist.

– Erforderlich ist ein schlüssiges Gesamtkonzept für eine effektive Kontrolle der Protokolle. Dies schließt den Einsatz von Software ein, die eine zeitnahe effektive Plausibilitätskontrolle unterstützt.

– Für die Sperrung und Löschung von Patientendaten muss ein Konzept erarbeitet und umgesetzt werden.

Zeitpunkt und Art und Weise der Umsetzung der Forderungen wird 2014 Gegenstand weiterer Gespräche mit den betroffenen Krankenhäusern sein.

2.1.6
Umgang mit Leichenschauscheinen in Kliniken

Auch bei der Übergabe von Leichenschauscheinen an ein Bestattungsunternehmen finden datenschutzrechtliche Grundsätze Anwendung. Das jeweilige Klinikum hat sicher zu stellen, dass der nur für den Amtsarzt bestimmte Leichenschauschein so an den Bestatter übergeben wird, dass eine Kenntnisnahme von seinem Inhalt ausgeschlossen ist.

2.1.6.1
Der Anlass

Dem Beitrag liegen die Eingaben zweier Bestatter betreffend das Universitätsklinikum Gießen und Marburg zugrunde. Diese haben unabhängig voneinander vorgetragen, dass ihnen bei Abholung der Verstorbenen in der Pathologie ein vertraulicher nur für den Amtsarzt bestimmter Leichenschauschein in einem unverschlossenen Umschlag übergeben worden sei.

Die Thematik „Unzulässige Öffnung von Leichenschauscheinen“ war schon zuvor Gegenstand eines Tätigkeitsberichts (s. 21. Tätigkeitsbericht, Ziff. 9.3). Darauf wurde in einer der Eingaben bereits Bezug genommen.

Die Eingebenden äußerten übereinstimmend ihre Sorge, dass aus dem vertraulichen (gelben) Leichenschauschein die Krankheitsgeschichte und die genaue Todesursache betreffend den Verstorbenen hervorgehe. Darin wurde eine Verletzung von Privatgeheimnissen und eine Verletzung der ärztlichen Schweigepflicht gesehen. Auch wenn die Übergabe lediglich den Zweck hatte, den Leichnam zweifelsfrei zu identifizieren, wurde mithin bemängelt, dass die Summe der preisgegebenen Daten zu diesem Zweck nicht erforderlich sei. Letztlich gebe es einen öffentlichen (blauen)

Leichenschauschein mit begrenzten Angaben, der zu diesem Zweck herangezogen werden könne. Dieser befand sich jedoch nach den Angaben der Eingebenden beim Standesamt und konnte aus diesem Grund nicht ausgehändigt werden.

2.1.6.2
Datenschutzrechtliche Bewertung

Die medizinischen Angaben im Leichenschauschein unterstehen der ärztlichen Schweigepflicht i.S.v. § 203 StGB. Diese gilt auch über den Tod der jeweiligen Person hinaus. Die Angaben im nicht öffentlichen Leichenschauschein sind allein für den Amtsarzt zweckbestimmt angelegt worden. Einer zufälligen Kenntnisnahme durch Dritte (z.B. Angehörige oder Bestatter) ist insoweit vorzubeugen. Auch wenn die Problematik bereits Gegenstand des 21. Tätigkeitsberichtes war, sollen die geschilderten Fälle Anlass dazu geben, dass Kliniken in Hessen ihre eigenen Handlungsabläufe noch einmal im Sinne eines Qualitätsmanagements einer Prüfung unterziehen.

2.1.6.3
Weitere Entwicklung

Aufgrund der genannten Schilderungen habe ich das Universitätsklinikum Gießen und Marburg um Stellungnahme zu den Vorfällen gebeten. Der dortige Datenschutzbeauftragte hat sich umgehend der Angelegenheit angenommen.

Da nicht auszuschließen war, dass die bisher verwendeten Umschläge, die nur durch Befeuchten zu verschließen waren, nicht mehr richtig geschlossen haben, wurden Umschläge mit selbstklebendem Verschluss beschafft. Hierdurch soll zunächst sicher gestellt werden, dass künftig nicht versehentlich ein Umschlag nicht korrekt verschlossen übergeben wird. Zusätzlich hierzu wurden Stempel mit der Aufschrift „Nur von Amtsärztin/Amtsarzt zu öffnen“ bestellt, die künftig auf den Umschlägen, die den vertraulichen Leichenschauschein enthalten, anzubringen sind. Die Eingabe wurde ferner zum Anlass genommen, die bisherige Verfahrensanweisung „Versorgung von Verstorbenen“ zu überarbeiten. Eine neue Arbeitsanweisung zur „Übergabe von Verstorbenen“ wurde ebenfalls erstellt. Darin ist noch einmal festgehalten, dass der nicht für die Öffentlichkeit bestimmte Leichenschauschein verschlossen an den Bestatter zu übergeben ist. Der Abgleich des Verstorbenen mit den Unterlagen des Bestatters ist künftig über ein ID-Armband vorzunehmen, welches am Verstorbenen anzubringen ist. Nach dem Abgleich wird das ID-Armband sofort entsorgt.

2.1.6.4
Abschließende Kontrollprüfung

Im Rahmen eines internen Qualitätsmanagements fand seitens des Universitätsklinikums Gießen und Marburg nach einem halben Jahr eine stichprobenhafte Kontrolle zu dem umgestellten Verfahren statt. Die Prüfung erfolgte ohne Voranmeldung.

Geprüft wurde die Übergabe eines Leichnams zur Erdbestattung im Inland und eine Überführung eines Leichnams in das Ausland außerhalb der EU-Grenzen.

Wie mir der Datenschutzbeauftragte des Universitätsklinikums Gießen und Marburg mitteilte, fanden die Verfahrens- und Arbeitsanweisungen in beiden Fällen Beachtung. Die übergebenen Umschläge mit dem vertraulichen Inhalt waren jeweils gestempelt und fest verschlossen.

3. Datenschutz im öffentlichen Bereich

3.1 Europa

3.1.1
Geplante EU-Datenschutz-Grundverordnung und EU-Richtlinie für Polizei- und Justizbehörden

Die Entwürfe wurden im Berichtszeitraum in den zuständigen Gremien im Europäischen Parlament und im Rat der Europäischen Union diskutiert. Der Beitrag stellt die wichtigsten Entwicklungen dar.

Im 41. Tätigkeitsbericht, Ziff. 1.2 habe ich auf die Entwürfe für eine „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (Datenschutz-Grundverordnung – KOM[2012]11 endg.; hier abgekürzt: GVE) sowie für eine „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“ (KOM[2012]10 endg.; hier abgekürzt: RLE) hingewiesen und einige mir wichtige Fragen aufgeworfen. Diese Entwürfe sollen die aus dem Jahr 1995 stammende „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995, ABl. Nr. L281 vom 23. November 1995 S. 31 - 50) ersetzen. Während die Grundverordnung direkt in den Mitgliedstaaten gilt, muss die Richtlinie erst durch nationale Rechtsakte umgesetzt werden.

Im Berichtszeitraum erreichten meine Mitarbeiterinnen viele Anfragen zum Stand des Reformvorhabens und den zu erwartenden Änderungen in der Rechtspraxis gegenüber der bisherigen Rechtslage.

3.1.1.1
EU-Datenschutz-Grundverordnung

3.1.1.1.1
Die inhaltliche Diskussion seit Veröffentlichung des Berichterstatter-Entwurfs

Am 10. Januar 2013 hat der zuständige Berichterstatter Jan Philipp Albrecht im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) den Entwurf eines Berichts zu dem Verordnungs-

vorschlag veröffentlicht (COM[2012]0011 – C7-0025/2012 – 2012/0011[COD]). Der Vorlageentwurf ist datenschutzfreundlicher als der Kommissionsentwurf, insbesondere in folgenden Punkten:

– Einfluss der Kommission: Die starke Stellung der Kommission soll zurückgedrängt werden. Zum Beispiel hat die Kommission nicht mehr das Recht, Maßnahmen von Aufsichtsbehörden auszusetzen,

– ausdrückliche Einwilligung: Um Nutzer darüber zu informieren, was mit ihren Daten geschieht, müssen einfache verständliche Informationen (z.B. Icons) verwendet werden. Nur bei ausdrücklicher Einwilligung darf dann eine Datenverarbeitung erfolgen,

– Profiling: An das Sammeln von Informationen, um ein Nutzerprofil zu erstellen (Profiling), sollen strengere Anforderungen gestellt werden. Durch technische Standards (z.B. Do Not Track) sollen Nutzer über die Privatsphäre-Einstellungen ihres Browsers einer Webseite automatisch signalisieren können, ob sie etwa dem Erstellen von Nutzungsprofilen zustimmen,

– Betroffenenrechte: Die Rechte der Betroffenen sollen dadurch gestärkt werden, dass Ausnahmetatbestände, die die Rechte verkürzen, reduziert werden. Insbesondere sollen die Auskunftsrechte der Nutzer gegenüber den Anbietern gestärkt werden,

– datenschutzfreundliches Design: Nicht nur die Datenverarbeiter, sondern auch die Hersteller von IT-Systemen sollen sich künftig an datenschutzfreundliches Design halten müssen,

– weniger Bürokratie: Ein betrieblicher Datenschutzbeauftragter soll künftig auch unabhängig von der Unternehmensgröße ernannt werden, wenn besonders sensible Daten verarbeitet werden. Andererseits sollen viele der ursprünglich vorgesehenen Vorabgenehmigungen und Audits durch die Datenschutzbehörden entfallen,

– einheitliche Rechtsdurchsetzung: Der geplante europäische Datenschutz-Ausschuss – der Zusammenschluss der nationalen Datenschutzaufsichtsbehörden – soll gestärkt werden. Für eine einheitliche Auslegung und Durchsetzung des Datenschutzrechts soll er europaweit bindende Entscheidungen treffen können, auch über die Höhe von Bußgeldern.

Zu dem Vorlageentwurf des Berichterstatters gingen im Frühjahr 2013 rund 3000 Änderungsanträge der anderen EU-Abgeordneten ein.

Im Oktober 2013 einigten sich die EU-Parlamentarier auf einen parteiübergreifenden Kompromisstext, der unter anderem Folgendes beinhaltet:

– Höchststrafe für Verstöße: 100 Millionen Euro oder fünf Prozent des Jahresumsatzes,

– betriebliche und behördliche Datenschutzbeauftragte:
  Wer Daten verarbeitet, die sensibel sind oder sich auf 5.000 Betroffene pro Jahr beziehen, muss u.a. einen betrieblichen bzw. behördlichen Datenschutzbeauftragten benennen sowie eine Risikoanalyse und eine Folgenabschätzung durchführen,

– Profiling:
  Jeder hat das Recht, der Profilbildung zu widersprechen,

– „Recht auf Vergessenwerden“:
  Jeder Bürger hat das Recht, ihn betreffende Daten löschen zu lassen; das weitergehende „Recht auf Vergessen“ hat sich nicht durchgesetzt,

– „One-Stop-Shop“-Ansatz: Bürger können Beschwerden über private Unternehmen unabhängig vom Ort des Sitzes des Unternehmens an die Datenschutzbehörde in ihrem Mitgliedstaat richten. Für ein Unternehmen, das in mehreren Mitgliedstaaten Niederlassungen hat, ist zunächst die Datenschutzaufsichtsbehörde des Mitgliedstaats zuständig, in dem das Unternehmen seine Hauptniederlassung hat.

– Übermittlungen an (Sicherheits-)Behörden in Drittstaaten:
  Telekommunikations- und Internetkonzerne dürfen Daten von EU-Bürgern nur aufgrund eindeutiger Rechtsgrundlage (z.B. EU-Verordnungen, Verträge, Rechtshilfeabkommen) an Behörden in Drittstaaten übermitteln.
  Wird ein Unternehmen von einem Drittstaat ersucht, Daten offenzulegen, die in der EU verarbeitet wurden, so hat das Unternehmen vor der Übermittlung die Zustimmung der nationalen Aufsichtsbehörde einzuholen und die betroffene Person über den Datentransfer zu informieren.
  Die Verschärfung der Übermittlungsregelungen an Behörden in Drittstaaten ist eine Folge der „Überwachungsaffäre“ des Jahres 2013, d.h. der Überwachung der weltweiten Kommunikation durch Geheimdienste.

Zeitgleich wurde der GVE in der Arbeitsgruppe „Informationsaustausch und Datenschutz“ (DAPIX) des Rates der EU, die für den Datenschutz verantwortlich zeichnet, diskutiert. Die Diskussionen in den Gremien wurden von intensiven Lobby-Aktivitäten begleitet, insbesondere aus den USA.

3.1.1.1.2
Zeitlicher Rahmen

Auf der Grundlage des Kompromisstextes sollte der Trilog mit dem Europäischen Rat und der Kommission beginnen. Der Zeitplan ist jedoch bereits nachhaltig in Verzug gekommen. Der Rat ließ anlässlich seiner Sitzung am 24./25. Oktober 2013 erkennen, dass er das Projekt bis 2015 verschieben möchte (Übermittlungsvermerk vom 25. Oktober 2013 [EUCO 169/13]). Um noch in dieser Legislaturperiode des Parlaments verabschiedet werden zu können, müsste eine Einigung zwischen Kommission, Parlament und Rat bis zum Frühjahr 2014 erfolgen. Allerdings gibt es auf europäischer Ebene nicht das Prinzip der Diskontinuität, das heißt der Entwurf könnte, wenn es nicht mehr zu einer Einigung kommt, in einem neu zusammengesetzten Parlament weiter verhandelt werden. Dies hätte jedoch eine deutliche Verzögerung zur Folge: Die konstituierende Sitzung des neuen Parlaments findet am 1. Juli 2014 statt, und die neue Kommission wird erst am 1. November 2014 die Tätigkeit aufnehmen. Dann wäre sogar das Inkrafttreten der Verordnung im Jahr 2015 ein ehrgeiziges Ziel.

3.1.1.2
EU-Richtlinie für Datenschutz bei Polizei- und Justizbehörden

3.1.1.2.1
Inhaltliche Diskussion seit Veröffentlichung des Berichterstatter-Entwurfs

Der für den RLE zuständige Berichterstatter Dimitrios Droutsas hat gleichfalls im Januar 2013 einen Entwurf vorgestellt (COM[2012]0010 – C7-0024/2012 – 2012/0010[COD]). Aus datenschutzrechtlicher Sicht zu kritisieren war vor allem das gegenüber dem GVE niedrigere Datenschutzniveau des RLE. Während im GVE die Rechte des Bürgers – Recht auf Information, auf Datenzugang und auf Richtigstellung oder Löschung – recht weit gefasst sind, werden diese Rechte beim RLE stark eingeschränkt. Diesen und weiteren Punkten trägt der Entwurf von Droutsas Rechnung. Insbesondere versucht er, das Schutzniveau an das des GVE anzugleichen.

Die Artikel 29-Datenschutzgruppe hat im Februar 2013 auf europäischer Ebene zu dem RLE und dem Berichterstatterentwurf eine Stellungnahme verfasst (Stellungnahme 01/2013 (00379/13/DE) vom 26. Februar 2013). In dieser Stellungnahme werden vier wichtige Aspekte angesprochen:

– Hinsichtlich der Daten unverdächtiger Personen sollte der RLE sicherstellen, dass solche Daten nur verarbeitet werden dürfen, wenn bestimmte Voraussetzungen erfüllt sind und ein zusätzlicher Schutz bei der Verarbeitung dieser Daten geschaffen wird.

– Rechte von Personen, die von der Datenverarbeitung betroffen sind (z.B. Recht auf Information, Berichtigung oder Löschung), sind im RLE stark eingeschränkt. So kann zum Beispiel das Recht des Bürgers auf Information darüber, dass personenbezogene Daten erhoben wurden, ohne besondere Anforderungen weitgehend beschnitten werden. Hier sollte stets die Möglichkeit einer Einzelfallentscheidung verbleiben.

– Da bereits im GVE Datenschutz-Folgeabschätzungen vorgeschrieben werden sollen, um die mit neuen Datenverarbeitungsvorgängen verbundenen Risiken zu bewerten, sind diese Folgeabschätzungen auch in einem datenverarbeitungsintensiven Sektor wie dem Strafverfolgungsbereich vorzusehen.

– Schließlich muss im RLE auch der Notwendigkeit Rechnung getragen werden, den Aufsichtsbehörden europaweit einheitlich Zugang zu den Räumlichkeiten der Strafverfolgungsstellen zu gewähren. Zudem sollte der RLE sicherstellen, dass die Datenschutzbehörden auf alle Informationen zugreifen dürfen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist.

Auch zur Richtlinie gab es im Oktober 2013 einen Kompromisstext des Europäischen Parlaments; auch hier hat das Europäische Parlament dem Berichterstatter Droutsas das Mandat erteilt, in den Trilog zu gehen.

3.1.1.2.2
Zeitlicher Rahmen

Es erscheint insgesamt am Ende des Berichtszeitraums nicht sicher, dass eine Einigung über den RLE noch in dieser Legislaturperiode des Europäischen Parlaments erfolgen kann. Europäisches Parlament und Europäische Kommission fordern, dass der GVE inhaltlich konsistent und zeitgleich mit dem RLE verabschiedet wird („Paketlösung“), während die Meinungen im Rat der EU zu dieser Frage auseinandergehen: Offensichtlich wollen einige Mitgliedstaaten sowohl die Grundprinzipien des GVE abschwächen als auch an der „Paketlösung“ rütteln.

3.1.2
Defizite einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste

Im Anschluss an meinen Beitrag im vorangegangenen Tätigkeitsbericht zur geplanten EU-Verordnung über elektronische Identifizierung und Vertrauensdienste ist als weiterer Kritikpunkt festzustellen, dass der Verordnungsentwurf keinerlei Regelung zur Vertraulichkeit enthält.

In meinem 41. Tätigkeitsbericht (Ziff. 2.1.1) hatte ich bereits verschiedene Schwachpunkte des Vorschlags der Europäischen Kommission für eine Verordnung des europäischen Parlaments und des Rates über die elektronischen Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (COM [2012] 238 final) dargelegt. Darüber hinaus ist festzustellen, dass die für Datenschutz und IT-Sicherheit wichtige Vertraulichkeit dort nicht umgesetzt ist.

Zwar ist mehrfach der für eine Rechtsvorschrift ungewöhnliche Begriff „Vertrauen“ erwähnt: So sollen Signaturen und Siegel „mit einem hohen Maß an Vertrauen“ erstellt werden, und es ist von den „vertrauenden Beteiligten“ (relying parties) die Rede. Statt Signaturen und Siegel „mit einem hohen Maß an Vertrauen“ zu erstellen, sollte besser ein hohes Maß an IT-Sicherheit bei der Erstellung gewährleistet werden. Die „vertrauenden Beteiligten“ (relying parties) sollten über Prüfmöglichkeiten und technisch sichere Verfahren verfügen, damit sie nicht nur auf das mit einem „hohen Maß an Vertrauen“ Erstellte wiederum „vertrauen“ müssen.

Umgekehrt sieht der VO-Entwurf keinen einzigen Vertrauensdienst vor, der die Vertraulichkeit der Kommunikation unterstützt, weder für E-Mail noch für das Internet. Das ist für die Wahrung der Privatsphäre und die Gewährleistung des Datenschutzes ein zentraler Punkt, der europaweit interoperabel geregelt werden sollte. In Zeiten von PRISM, TEMPORA, XKeyScore und anderen von Geheimdiensten in Europa und außerhalb Europas genutzten umfassenden, flächendeckenden Spähprogrammen ist ein laxer Umgang mit personenbezogenen Daten – und mit Geschäftsgeheimnissen – nicht mehr zu verantworten.

Für E-Mail würde die Vertraulichkeit dem verschlossenen Umschlag bei der herkömmlichen Briefpost entsprechen. Die De-Mail entspricht lediglich der offenen Postkarte: während des Transports ist der Postsack zu – die De-Mail verschlüsselt – in den Sortier- und Verteilzentren ist der Sack offen – die De-Mail liegt auf allen Servern im Klartext vor – und die Postkarte bzw. De-Mail kann gelesen werden.

Eine Ende zu Ende Verschlüsselung wäre für E-Mail einfach zu realisieren: Jeder E-Mail-Provider braucht dafür nur zu der jeweiligen E-Mail-Adresse einer Bürgerin oder eines Bürgers den öffentli-

chen Schlüssel in einer (Zertifikats-)Liste zum Abruf bereitzuhalten. Dann könnte sogar weltweit jeder dieser Person – vorausgesetzt er kennt ihre E-Mail-Adresse – eine verschlüsselte E-Mail quasi „per Knopfdruck“ senden. Auch De-Mail wäre dafür nicht erforderlich: De-Mail bietet für den Versand keine Ende zu Ende Verschlüsselung der Nachricht selbst an, sondern erlaubt – wie E-Mail auch – lediglich den Versand verschlüsselter Dokumente als Anhang. Das ist zum einen keine Transportverschlüsselung und zum anderen im Einzelfall wesentlich aufwendiger.

In jedem Fall ist darauf zu achten, dass die Schlüssel wirklich vertrauenswürdig sind. Es darf also keine Hinterlegung von Schlüsseln (Key Escrow) oder von Schlüsselteilen oder von Parametern zur Schlüsselerzeugung stattfinden. Dazu gehört aber auch, dass alle Schlüssel unter Verwendung von echten Zufallszahlen und ohne Einschränkung des Werteraumes erzeugt werden. Diese Forderung ist deshalb derzeit besonders schwer zu erfüllen, weil die NSA den Standardisierungsprozess des amerikanischen National Institute of Standards and Technology (NIST) gezielt unterwandert hat. Das NIST lässt nun entsprechende Standards erneut öffentlich auf weitere Hintertüren (Backdoors) prüfen. Wobei die dafür gewährte Verlängerung gemessen an der Komplexität des Themas wohl erheblich zu kurz ist.

Wer mit kompromittierten Schlüsseln, Verfahren oder Standards arbeitet, gibt die Vertraulichkeit preis, bevor sie begonnen hat. Vor dem Hintergrund der klaren Ansage von NIST-Chef Gallagher, dass das Institut allerdings auch weiterhin zwingend mit der NSA zusammenarbeiten wird, werden die amerikanischen NIST-Standards wohl in der Zukunft international neu bewertet werden und dann hoffentlich keine so dominierende Rolle mehr spielen.

Für das Internet ist unbedingt zu beachten, dass *Perfect Forward Secrecy* wirklich aktiv genutzt – und nicht beispielsweise vom Zielserver abgelehnt – wird.
Diese „Folgenlosigkeit“ (englisch *perfect forward secrecy*; auf deutsch etwa *perfekte vorwärts gerichtete Geheimhaltung*) bedeutet in der Kryptographie die Eigenschaft von Schlüsselaustauschprotokollen, dass aus einem aufgedeckten geheimen Langzeitschlüssel nicht auf damit ausgehandelte Sitzungsschlüssel (Session Key) eines Kommunikationskanals geschlossen werden kann.

Dazu ist wichtig, dass der Session Key zwischen den Kommunikationspartnern ausgehandelt wird, ohne dass er zwischen ihnen übertragen oder im Log gespeichert wird. Dies kann beispielsweise mit Hilfe des Diffie-Hellmann-Schlüsselaustauschs geschehen. So kann verhindert werden, dass die mitgeschnittene/abgehörte Kommunikation nachträglich allzu einfach entschlüsselt werden kann.

3.1.3
Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrung der Interessen der Landesdatenschutzbeauftragten in der Europäischen Kontrollinstanz des Schengener Informationssystems übertragen. Meine Mitarbeiterin hat im Berichtszeitraum an zwei Sitzungen in Brüssel teilgenommen. Der Beitrag stellt die Arbeitsschwerpunkte im Jahr 2013 dar.

3.1.3.1
Schengener Informationssystem der zweiten Generation (SIS II)

3.1.3.1.1
Inbetriebnahme des SIS II

Der zuletzt im 41. Tätigkeitsbericht (Ziff. 3.1.1.1) genannte Zeitpunkt für den immer wieder verschobenen Start des SIS II wurde eingehalten: Am 9. März 2013 ging das SIS II mit großer Verspätung in Betrieb. Erste Planungen für ein neues SIS II gehen auf das Jahr 2002 zurück. Ursprünglich sollte es 2006, dann 2010 an den Start gehen, dazu kam es jedoch nicht, da die notwendigen technischen Tests mehrmals misslangen.

Das SIS II wird auf einem Zentralrechner (C-SIS) in Straßburg betrieben, der durch die IT-Agentur der EU in Tallinn gemanagt wird und an den in jedem Schengen-Mitgliedsland ein System (N-SIS) – zurzeit insgesamt 28 Systeme – angeschlossen ist. Dateneingaben werden vom N-SIS an das C-SIS übermittelt, sodass die Daten bereits Sekunden nach der Eingabe gleichzeitig allen Vertragspartnern zur Verfügung stehen. Die bisher angefallenen Kosten sollen sich auf 160 Millionen EUR belaufen. Ursprünglich waren für die gesamte Entwicklung 20 Millionen EUR geplant.

3.1.3.1.2
Rechtsgrundlagen

Rechtsgrundlagen für das SIS II sind die Verordnung 1987/2006 vom 20. Dezember 2006 (ABl. L381, S. 4), die Verordnung 1986/2006 vom 20. Dezember 2006 (ABl. L381, S. 1) sowie der Beschluss 2007/533 vom 12. Juni 2007 (ABl. L 205, S. 63). Diese Regelungen treten an die Stelle der Art. 92 bis 119 des Schengener Durchführungsübereinkommens (SDÜ). Die unterschiedliche

Rechtsnatur der Rechtsakte (Verordnung / Beschluss) ist der Tatsache geschuldet, dass ihr Erlass auf unterschiedliche Kompetenznormen im Primärrecht zu stützen war. Erst mit Inkrafttreten des Vertrags über die Arbeitsweise der Europäischen Union (AEUV i.d.F. der Bekanntmachung vom 9. Mai 2008 , ABl. C115, S. 47) am 1. Dezember 2009 ist die Trennung in verschiedene Säulen weggefallen, sodass jetzt ein einheitlicher Rechtsakt möglich wäre.

Wesentliche Änderungen des materiellen Rechts sind:

- Es können jetzt auch biometrische Merkmale (Fingerabdrücke u. Lichtbilder) gespeichert werden
- Verschiedene Ausschreibungen können miteinander verknüpft werden, z.B. eine Personenausschreibung mit einer Fahrzeugausschreibung.

Während mit Hilfe des bisherigen SIS ausschließlich nach bestimmten Personen oder Gegenständen gefahndet werden konnte (hit/no hit), entwickelt sich das neue SIS II durch die zahlreichen Verknüpfungsmöglichkeiten zu einem Recherchesystem.

3.1.3.1.3
Von der GKI zur koordinierten Kontrollgruppe für SIS II

Mit Inbetriebnahme des SIS II am 9. März 2013 ist die Kontrolle von der Gemeinsamen Kontrollinstanz auf den Europäischen Datenschutzbeauftragten (EDPS) übergegangen, der in koordinierter Weise mit den Aufsichtsbehörden der Mitgliedstaaten zusammenzuarbeiten hat.

Art. 62 Beschluss über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)

(1) Die nationalen Kontrollinstanzen und der Europäische Datenschutzbeauftragte arbeiten im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und gewährleisten eine koordinierte Überwachung des SIS II.

(2) Im Rahmen ihrer jeweiligen Zuständigkeiten tauschen sie einschlägige Informationen aus, unterstützen sich gegenseitig bei Überprüfungen und Inspektionen, prüfen Schwierigkeiten bei der Auslegung oder Anwendung dieses Beschlusses, gehen Problemen bei der Wahrnehmung der unabhängigen Überwachung oder der Ausübung der Rechte betroffener Personen nach, arbeiten harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme aus und fördern erforderlichenfalls die Sensibilisierung für die Datenschutzrechte.

(3) Die nationalen Kontrollinstanzen und der Europäische Datenschutzbeauftragte treffen zu diesem Zweck mindestens zweimal jährlich zusammen. Die Kosten und die Ausrichtung dieser Sitzungen gehen zu Lasten des Europäischen Datenschutzbeauftragten. In der ersten Sitzung wird eine Geschäftsordnung angenommen. Weitere Arbeitsverfahren werden je nach Bedarf gemeinsam festgelegt. Ein gemeinsamer Tätigkeitsbericht wird dem Europäischen Parlament, dem Rat, der Kommission und der Verwaltungsbehörde alle zwei Jahre übermittelt.

Die koordinierte Kontrollgruppe trat erstmals am 11. Juni 2013 zusammen. Die deutsche Delegation setzt sich aus einem Vertreter des BfDI und einem Vertreter der Landesdatenschutzbeauftragten zusammen. Auch die Vertretung der LfD in diesem neuen Gremium nimmt meine Mitarbeiterin derzeit wahr. Zur Vorsitzenden der koordinierten Kontrollgruppe wurde die portugiesische Kollegin Clara Guerra und als Vertreter David Cauchi aus Malta gewählt.

3.1.3.2
Gemeinsame Überprüfungen der Ausschreibungen zur Festnahme im Schengener Informationssystem

Die im 41. Tätigkeitsbericht, Ziff. 3.1.1.1.2 erwähnte in allen Schengen-Staaten gemeinsam durchgeführte Überprüfung von Ausschreibungen nach Art. 95 SDÜ (jetzt Art. 29 des Beschlusses 2007/533/JI über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)) ist beendet und der entsprechende Prüfbericht verabschiedet. Es ging dabei um die Ausschreibung im SIS von Personen, die wegen einer Straftat mit Haftbefehl zur Verfolgung oder zur Vollstreckung gesucht werden. In Deutschland liegen der Ausschreibung im SIS ein durch den Richter ausgestellter Haftbefehl sowie ein von der Staatsanwaltschaft erlassener europäischer Haftbefehl (European Arrest Warrant, EAW) zugrunde.

Die deutsche Delegation hatte im Rahmen der Überprüfung festgestellt, dass vor der Ausschreibung im SIS in Deutschland nicht alle erforderlichen Kontrollen getätigt wurden. So wurde von den deutschen ausschreibenden Behörden nicht – wie in Art. 95 Abs. 2 SDÜ vorgesehen – in allen Fällen geprüft, ob die Festnahme des Betroffenen nach dem Recht der ersuchten Staaten zulässig ist. Man wies dabei darauf hin, dass es z.B. kaum möglich sei, vor der Ausschreibung zu prüfen, ob die der Ausschreibung zugrundeliegende Straftat in allen Schengen-Staaten strafbar sei. Es wurde weiter darauf verwiesen, dass in jedem Fall im Rahmen der Stellung des Antrags auf Auslieferung eine derartige Prüfung erfolge und damit die Interessen des Betroffenen gewahrt seien.

Das Problem hat sich jetzt insoweit entschärft, als nach der nunmehr einschlägigen Vorschrift des SIS II-Beschlusses eine derartige der Ausschreibung vorangehende Prüfung nicht mehr vorgesehen ist. Vieles spricht dafür, dass in Art. 26 des Beschlusses für SIS II diese Pflicht zur Prüfung aus Praktikabilitätsgründen nicht mehr aufgenommen wurde.

3.1.3.3
Probleme bei der Ausschreibung von Kraftfahrzeugen im Schengener Informationssystem

Wenn auch die Ausschreibung von Personen, insbesondere von Drittausländern. den größten Teil der Datenbank ausmacht, so kann im SIS auch nach Sachen gefahndet werden, die zur Sicherstellung oder Beweissicherung im Strafverfahren gesucht werden. Derartige Sachen können insbesondere Kraftfahrzeuge sein, die dem Eigentümer u.a. gestohlen wurden oder die Gegenstand eines Versicherungsbetrugs sind.

Art. 38 Beschluss 2007/533/JI über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)

Ausschreibungsziele und –bedingungen

(1) Daten in Bezug auf Sachen, die zur Sicherstellung oder Beweissicherung in Strafverfahren gesucht werden, werden in das SIS II eingegeben.

(2) Es werden folgende Kategorien von leicht identifizierbaren Sachen einbezogen:
a) Kraftfahrzeuge
…

Der ausschreibende Mitgliedstaat ist dabei für die Richtigkeit und Aktualität der Daten verantwortlich (Art. 49).

Probleme treten auf, wenn ein – möglicherweise im Fall des vorausgehenden Versicherungsbetrugs gutgläubiger – Käufer ein von einem anderen Schengen-Staat im SIS ausgeschriebenes Kraftfahrzeug erwirbt. Derartige Fälle sind z.Z. beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aktenkundig. Auch ein hessischer Bürger, der von der Problematik betroffen ist, hat sich an mich gewandt, um Hilfe bei der Rechtsdurchsetzung zu erhalten.

Die Käufer eines derartigen Kraftfahrzeugs haben regelmäßig folgende Probleme: Sobald der Betroffene das Fahrzeug zulassen möchte, erhält er von der Zulassungsstelle die Auskunft, dass eine SIS-Ausschreibung besteht. Das Fahrzeug wird dann i.d.R. polizeilich sichergestellt (§ 94 Abs. 1 StPO). Die zuständigen Polizeibehörden nehmen mit der ausschreibenden Behörde des anderen Schengenstaats Kontakt auf, um die Gründe für die Ausschreibung zu erfahren. Wenn von dort keine Reaktion erfolgt und der Erwerber mit dem Kauf des Fahrzeugs keinen Straftatbestand (z.B. Hehlerei) erfüllt hat bzw. ihm dies nicht nachgewiesen wird, wird ihm das Fahrzeug in der Regel zurückgegeben. Die SIS-Ausschreibung bleibt jedoch weiter bestehen. Deshalb kann der Erwerber das Fahrzeug nur mit Schwierigkeiten weiterveräußern, da bei jeder erneuten Zulassung die Ausschreibung im SIS erscheint. Auch jeder Grenzübertritt kann für den Erwerber zum Problem werden, da er Gefahr läuft, mit der Ausschreibung im SIS konfrontiert zu werden.

Der SIS II-Beschluss sieht für den Betroffenen sowohl einen Auskunfts- als auch einen Berichtigungs- und Löschungsanspruch vor.

Art. 58 Beschluss 2007/533/JI über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)

Recht auf Auskunft Berichtigung unrichtiger Daten und Löschung unrechtmäßig gespeicherter Daten

(1) Das Recht jeder Person, über die gemäß diesem Beschluss zu ihrer Person in das SIS II gespeicherten Daten Auskunft zu erhalten, richtet sich nach dem Recht des Mitgliedstaats, in dessen Hoheitsgebiet das Auskunftsrecht beansprucht wird.
...
(5) Jeder hat das Recht, auf seine Person bezogene unrichtige Daten berichtigen oder unrechtmäßig gespeicherte Daten löschen zu lassen.

Die Realisierung dieser Ansprüche scheitert aber in den vorliegenden Fällen häufig schon daran, dass die Rückfragen deutscher Behörden bei der Behörde des Schengen-Staates, die für die Ausschreibung zuständig ist, ergebnislos bleiben.

Auf Wunsch der deutschen Delegation wurde das Thema von der koordinierten Kontrollgruppe in der Oktobersitzung d.J. aufgegriffen. Ein Ergebnis liegt bisher nicht vor.

3.1.4
Gemeinsame Kontrollinstanz für EUROPOL

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

3.1.4.1
EUROPOL als Dienstleister (Serviceprovider) für die Mitgliedstaaten

Neben der klassischen Zielsetzung, eine europäische Polizeibehörde zu sein, die die Bekämpfung von bestimmten schweren Straftaten und Terrorismus durch die zuständigen Behörden der Mitgliedstaaten unterstützt, strebt es EUROPOL an, als reiner Dienstleister (Serviceprovider) für die Mitgliedstaaten zu fungieren. Für diese Entwicklung von EUROPOL hatte sich der Europäische Rat im Stockholmer Programm (ABl. C 115 vom 4. Mai 2010, S. 1) ausgesprochen. Ein Beispiel hierfür ist die geplante Ausweitung der Kommunikation im Rahmen des bestehenden Informationsaustauschnetzwerks [Secure Information Exchange Network Application (SIENA)]. Bisher wurden über SIENA die Informationen zwischen EUROPOL und den Mitgliedstaaten ausgetauscht. Nunmehr kam EUROPOL mit Plänen auf die Gemeinsame Kontrollinstanz (GKI) zu, die beinhalten, dass SIENA als sicheres Netz auch für ganz andere Situationen des Informationsaustauschs zur Verfügung gestellt werden soll. Danach sollen u.a. Informationen zwischen einem Mitgliedstaat und einem Drittstaat, für den EUROPOL gar nicht zuständig ist, über SIENA ausgetauscht werden.

Die GKI hat hierzu eine Stellungnahme verfasst und klargestellt, dass es für diese Dienstleistung keine gesetzliche Grundlage im EUROPOL-Beschluss gibt. Der Zielsetzung von EUROPOL, die national zuständigen Polizeibehörden zu unterstützen, kann nicht entnommen werden, dass darunter auch die von den Aufgaben von EUROPOL losgelöste Bereitstellung eines Informationsaustauschnetzes fällt.

3.1.4.2
Vereinbarungen zwischen EUROPOL und Drittstaaten

EUROPOL kann zu Drittstaaten Kooperationsbeziehungen herstellen und zu diesem Zweck Abkommen mit anderen Staaten über den Austausch operativer oder strategischer Informationen

abschließen (Art. 23 EUROPOL-Beschluss). Sofern diese Abkommen personenbezogene Daten betreffen, ist die Stellungnahme der GKI einzuholen. EUROPOL hat bereits eine Reihe dieser Abkommen abgeschlossen. Im Berichtszeitraum ging es um Abkommen mit der Russischen Föderation, Serbien, Albanien, Bosnien, Herzegowina und Montenegro. Das Verfahren läuft regelmäßig folgendermaßen ab: Beabsichtigt EUROPOL die Aufnahme von Vertragsverhandlungen, so muss vorher festgestellt werden, ob der Drittstaat ein angemessenes Datenschutzniveau gewährleistet. In dem von EUROPOL zu erstellenden Bericht werden der Rechtsrahmen und die Verwaltungspraxis im Bereich des Datenschutzes evaluiert. Insbesondere wird auch festgestellt, ob eine unabhängige Aufsichtsbehörde für die Überwachung von Datenschutzangelegenheiten besteht. Die GKI nimmt dann zu diesem Bericht Stellung und kann weitere Informationen anfordern, was in vielen Fällen geschieht. Gibt die GKI „grünes Licht", kann EUROPOL Vertragsverhandlungen aufnehmen. Der Vertragsentwurf ist dann wiederum der GKI vorzulegen.

Insbesondere im Fall der Russischen Föderation ist die GKI der Auffassung, dass kein ausreichendes Datenschutzniveau besteht. Grundlegende Zweifel bestehen an der Unabhängigkeit der Aufsichtsbehörde sowie daran, dass das russische Datenschutzrecht für alle vorgesehenen Übermittlungssituationen anwendbar ist.

3.1.4.3
Neue Rechtsgrundlage für EUROPOL

Im 41. Tätigkeitsbericht, Ziff. 3.1.2.3, hatte ich berichtet, dass es in der ersten Hälfte des Jahres 2013 eine neue Rechtsgrundlage für EUROPOL geben soll. Die Kommission hat nunmehr am 27. März 2013 einen Entwurf für eine entsprechende Verordnung vorgelegt [Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der EU für die Zusammenarbeit und die Ausbildung auf dem Gebiet der Strafverfolgung (EUROPOL) und zur Aufhebung der Beschlüsse 2009/371/JI und 2005/681/JI des Rates, COM (2013/173 endg.)].

Die GKI hat im Juni eine auf das Wesentliche beschränkte und im Oktober d.J. eine ausführliche Stellungnahme zu den einzelnen Rechtsvorschriften des Entwurfs abgegeben. Insgesamt ist sie der Auffassung, dass der vorliegende Entwurf ein deutlich schlechteres Datenschutzniveau vorsieht als der bestehende EUROPOL-Beschluss.

Die wesentlichen Punkte sind folgende:

– Die bestehende Datenverarbeitungsstruktur wird vollständig neu gestaltet. Die bei EUROPOL eingehenden Informationen werden nicht mehr wie bisher in bestimmte Dateistrukturen (Informationssystem, Analysedateien, Index-System) eingegeben, sondern werden alle in einer

Datenbank gespeichert. Abgestellt wird nur noch auf den Zweck der Datenverarbeitung: Kreuzproben (cross-matching), strategische oder sonstige Analysen allgemeiner Art sowie operative Analysen in spezifischen Fällen. Unter dem Stichwort größere Flexibilität soll EUROPOL einfacher Zusammenhänge zwischen den vorliegenden Daten erkennen und analysieren können.

Es soll EUROPOL überlassen werden, die effizienteste IT-Struktur selbst auszuwählen. Diese soll dann nach Maßgabe des „eingebauten Datenschutzes“ (Privacy by Design) entwickelt werden.

Mit der Wahl dieses Konzepts entfallen auf die jeweilige Verarbeitungssituation abstellende datenschutzrechtliche Vorkehrungen wie das Prinzip der Erforderlichkeit, der Zweckbegrenzung, der bereichsspezifischen Löschungsvorschriften oder der Beschränkung der zu verarbeitenden Datenkategorien. Der Begriff Privacy by Design wird nicht konkretisiert.

Nach Ansicht der GKI räumen die bisherigen Änderungen des materiellen Rechts (z.B. die Einführung einer Norm, die die Einführung neuer Datensysteme zulässt) und der Praxis EUROPOL schon jetzt eine weitgehende Flexibilität ein.

– Andererseits sind im Entwurf bestimmte Aufgaben von EUROPOL nicht geregelt, die bereits praktiziert oder die weiter entwickelt werden sollen. Dies trifft für das angestrebte Ziel von EUROPOL zu, als Dienstleister für die Mitgliedstaaten zu fungieren und das Informationsaustauschnetzwerk SIENA (s. Ziff. 3.1.4.1) auszuweiten.

  Es fehlt auch an einer Rechtsgrundlage für die Aufgabe, die EUROPOL im Rahmen des Terrorist Finance Tracking Programme (TFTP), einem Abkommen zwischen der EU und den Vereinigten Staaten (s. 41. Tätigkeitsbericht, Ziff. 3.1.2.2), zugewiesen bekam. EUROPOL hat nach diesem Abkommen die Aufgabe, Ersuchen amerikanischer Behörden um Übermittlung von Zahlungsverkehrsdaten an den Dienstleister SWIFT auf ihre Konformität mit dem TFTP-Abkommen zu überprüfen. Diese Aufgabe ist nicht von den Zielsetzungen für EUROPOL des jetzt vorliegenden Entwurfs gedeckt.

  Nicht geregelt ist weiterhin – anders als im EUROPOL-Beschluss – die Befugnis für EUROPOL, die von den Mitgliedstaaten übersandten Informationen kurzfristig zu speichern, um zu prüfen, ob sie in den Zuständigkeitsbereich von EUROPOL fallen.

– Der Entwurf sieht vor, dass die datenschutzrechtliche Kontrolle von EUROPOL nicht mehr durch die GKI, sondern vom Europäischen Datenschutzbeauftragten (EDPS) vorgenommen

wird. Lediglich nach Bedarf sollen sich die nationalen Datenschutzbehörden und der EDPS treffen.

Diese Regelung wird von der GKI kritisiert, da es bei den von EUROPOL verarbeiteten Daten zum größten Teil um solche der Mitgliedstaaten geht und deshalb deren Einbeziehung erforderlich scheint. Die GKI spricht sich für ein unabhängiges Kontrollgremium aus, in dem die nationalen Kontrollbehörden und der EDPS gleichwertig vertreten sind. Dieses Gremium könnte an den Datenschutzausschuss, wie er im Entwurf für eine Datenschutzgrundverordnung vorgesehen ist (s. Ziff. 3.1.1), angebunden sein.

3.1.5
„Smart Borders“ – Intelligente Grenzen im Europäischen Raum

Im Februar dieses Jahres hat die Europäische Kommission unter dem Stichwort „Smart Borders“ drei Verordnungsvorschläge zur Erfassung von Reisenden vorgestellt. Im Mittelpunkt des Reformpakets steht eine neue Datenbank, in der alle Reisen von Drittstaatsangehörigen in und aus dem Schengenraum erfasst werden sollen mit dem vorrangigen Ziel, die illegale Migration zu bekämpfen. Daneben soll es auch ein Vorzugsprogramm für Vielreisende geben.

3.1.5.1
Intelligente Grenzen – Einreise-/Ausreisesystem und Vorzugsprogramm für Vielreisende

Die Art. 29 Arbeitsgruppe, bestehend aus den europäischen Datenschutzbeauftragten, hat im Juni dieses Jahres eine umfassende Stellungnahme zu dem Vorhaben der Kommission vorgelegt. Vorbereitet wurde dieses Dokument von der Unterarbeitsgruppe „Border, Travel and Law Enforcement“ (BTLE), in der meine Mitarbeiterin als Vertreterin der Landesdatenschutzbehörden mitarbeitet. Die Entwürfe der EU-Kommission beinhalten Verordnungsvorschläge über ein Einreise-/Ausreisesystem zur Erfassung der Einreise- und Ausreisedaten von Drittstaatsangehörigen an den Außengrenzen der EU [KOM(2013) 95 endg.], über ein Registrierungsprogramm für Reisende [KOM(2013) 97 endg.]. und über eine entsprechende Anpassung des Schengener Grenzkodexes [KOM(2013) 96 endg.]. Die Gesamtkonzeption ist erläutert in der Pressemitteilung „“Intelligente Grenzen“: Mehr Mobilität und Sicherheit“ der Europäischen Kommission vom 28. Februar 2013. Die Vorschläge sind Bestandteil der in der Mitteilung zur Migration vom 4. Mai 2011 (IP/11/532 und MEMO/11/273) angekündigten Initiative zur Stärkung der allgemeinen Verwaltung des Schengen-Raums.

Das Einreise- und Ausreisesystem (EES) und das Registrierungsprogramm für Reisende (RTP) sollen die Kontrolle des Personenreiseverkehrs an den EU-Außengrenzen verbessern. Laut der zuständigen EU-Kommissarin Malmström wird durch den Einsatz der neuen Technologien „Bürgerinnen und Bürgern aus Drittländern, die in die EU einreisen wollen, ein reibungsloserer und rascherer Grenzübertritt ermöglicht. Außerdem wird die Modernisierung unserer Systeme für mehr Sicherheit sorgen, da irreguläre Grenzübertritte verhindert und Überschreitungen der zulässigen Aufenthaltsdauer aufgedeckt werden."

Im Rahmen des Vorzugs- bzw. Registrierungsprogramms für vielreisende Drittstaatsangehörige (z.B. Zeitarbeitskräfte, Wissenschaftler, Studierende) sollen an wichtigen Grenzübergängen automatische, biometriegestützte Grenzkontrollsysteme (Schleusen) eingesetzt werden, um registrierte Reisende schneller abfertigen zu können. Da dieses Vorhaben datenschutzrechtlich weniger kritisch ist, beschäftigt sich der Beitrag im Weiteren mit dem EES.

3.1.5.2
Die Ausgestaltung des Einreise-/Ausreisesystems

Die Kontrolle von Drittstaatsangehörigen an den Außengrenzen der EU erfolgt heute hauptsächlich aufgrund der im Reisedokument enthaltenen Stempel. Mit dem System EES sollen nunmehr Zeitpunkt und Ort der Einreise und Ausreise von Drittstaatsangehörigen erfasst werden. Drittausländer müssen sich außerdem mit allen zehn Fingern bei der Einreise in die EU von der Grenzkontrolle registrieren lassen. Anstelle des heutigen manuellen Verfahrens soll das neue elektronische System die zulässige Dauer eines Kurzaufenthalts automatisch berechnen. Sofern der eingereiste Drittstaatsangehörige bis zum Ablauf der Aufenthaltsdauer nicht ausgereist ist, wird ein Warnhinweis an die nationalen Behörden generiert.

Interessant ist, dass schon jetzt an eine Einbeziehung der Sicherheitsbehörden gedacht wird. So sieht Erwägungsgrund 11 des Verordnungsvorschlags vor, dass für den Fall, dass die Verordnung später den Datenzugang zu Strafverfolgungszwecken erlaubt, eine solche Zugangsmöglichkeit bei der technischen Entwicklung des Systems bereits vorgesehen werden sollte. Ob ein solcher Datenzugang gewährt wird, soll vom Ergebnis einer Evaluierung abhängen, die zwei Jahre nach Inbetriebnahme des EES erfolgen soll. Angesichts der immensen Kosten für das EES (1,1 Mrd. Euro für EES und RTP) ist zu erwarten, dass die Datenbank im Fall ihrer Realisierung auch möglichst umfassend genutzt werden soll.

3.1.5.3
Datenschutzrechtliche Bedenken

Das gesetzgeberische Vorhaben der Europäischen Kommission zur Einführung des EES ist kritisch zu sehen.

Zum einen ist es fraglich, ob es neben dem Schengener Informationssystem, dem Visa-Informationssystem und EURODAC (Datenbank zur Speicherung von Fingerabdrücken) einer weiteren Datenbank auf europäischer Ebene bedarf. Der Europäische Datenschutzbeauftragte weist in einer Stellungnahme darauf hin, dass es bislang noch nicht einmal eine klare politische Linie im Umgang mit Visa-Inhabern gebe, die eingetragene Fristen bewusst überziehen [Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), 18. Juli 2013]. Daher sei eine weitere Datenbank unverhältnismäßig, da Auslaufdaten von Aufenthaltsgenehmigungen bereits in dem seit 2011 laufenden Visa-Informationssystem aufbewahrt würden.

Zum anderen ist vollkommen unsicher, ob das Hauptziel, die Verhinderung der Überschreitung der zulässigen Aufenthaltsdauer, überhaupt erreicht wird. Drittstaatsangehörige, die ihre zulässige Aufenthaltsdauer überziehen („Overstayer"), werden zwar erfasst, eine Rückführung in den Heimatstaat ist damit aber noch nicht gewährleistet. Das EES kann für sich genommen die Überziehung der zulässigen Aufenthaltsdauer nicht unterbinden, es können allenfalls statistische Aussagen u.a. über „ Overstayer" getroffen werden. Die Effizienz des EES hängt deshalb wesentlich davon ab, ob und wieweit die nationalen zuständigen Behörden eine Rückführung der betroffenen Drittausländer tatsächlich realisieren. Zudem besteht das Risiko, dass Drittstaatsangehörige unverschuldet als „Overstayer" erkannt werden, sei es aufgrund unvorhersehbarer Zwischenfälle (z.B. Erkrankung) oder aufgrund technischer Schwierigkeiten.

Problematisch ist auch der bereits heute schon in Aussicht gestellte Zugang für die Strafverfolgungsbehörden. Die Berichterstatterin im LIBE (Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres), Renate Sommer, unterstützte bei einer ersten Diskussion im September 2013 das Vorhaben, das System zur Bekämpfung terroristischer und anderer schwerer Straftaten zu nutzen. Aus datenschutzrechtlicher Sicht ist allerdings nicht ohne Weiteres nachvollziehbar, dass Strafverfolgungsbehörden routinemäßig Zugriff zu einer Verwaltungsdatenbank erhalten sollten, die zu ganz anderen Zwecken, nämlich insbesondere der Aufdeckung von „Overstayern" eingerichtet wurde.

Die Datenbanken EES und RTP sollen nach dem Willen der Kommission 2017 bzw. 2018 in Betrieb gehen. Es wird sich zeigen, ob die oben genannten Bedenken in den Verhandlungen mit dem

Europäischen Parlament und dem Rat Berücksichtigung finden. Wie schwierig die technische Umsetzung solcher Vorhaben sein kann, zeigte sich bereits bei der Einführung des neuen SIS II-Systems, die jahrelang aufgrund technischer Probleme immer wieder verschoben werden musste (vgl. Ziff. 3.1.3.1.1).

3.2 Bund

3.2.1
E-Government-Gesetz des Bundes in Kraft getreten

Der Bundesgesetzgeber hat mit der Verabschiedung des E-Government-Gesetzes die Chancen für einen besseren Datenschutz und mehr Transparenz ungenutzt gelassen.

Am 1. August 2013 ist das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz) in Kraft getreten. Der Auftrag für die Erarbeitung eines derartigen Gesetzes stammte aus dem zwischen CDU, CSU und FDP geschlossenen Koalitionsvertrag „Wachstum. Bildung. Zusammenhalt“ der 17. Legislaturperiode. Das Gesetz trägt zur Umsetzung der nationalen E-Government-Strategie bei.

Auch die neue Koalition von CDU, CSU und SPD knüpft in ihrer Koalitionsvereinbarung an diese Strategie an. So ist vereinbart, dass Bürgerinnen und Bürger auf Wunsch die Möglichkeit haben sollen, einen einheitlichen Stammdaten-Account, ein sogenanntes Bürgerkonto zu verwenden, um die Kommunikation mit der Verwaltung zusätzlich zu vereinfachen. Zur Identifizierung soll der neue elektronische Personalausweis genutzt werden.

Ziel des E-Government-Gesetzes ist es, durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung zu erleichtern. Das Gesetz soll dadurch über die föderalen Ebenen hinweg Wirkung entfalten und Bund, Ländern und Kommunen ermöglichen, einfachere, nutzerfreundlichere und effizientere Verwaltungsdienste anzubieten.

Jede Verwaltung ist mit Wirkung zum 1. Juli 2014 verpflichtet, einen elektronischen Zugang zur Verwaltung zu schaffen. Die Bürger können zwar nicht gezwungen werden, elektronisch mit der Verwaltung zu kommunizieren, die Verwaltung selbst muss aber in Zukunft offen sein für diesen Dialogweg.

Die Kommunikation soll auch dadurch erleichtert werden, indem das Schriftformerfordernis neben der qualifizierten elektronischen Signatur durch weitere – als sicher eingestufte – Verfahren ersetzt werden kann. Das erste Verfahren betrifft die Bereitstellung von Formularen durch die Verwaltung im Internet. Hier soll die qualifizierte elektronische Signatur ersetzt werden können, wenn ein Identitätsnachweis nach § 18 PAuswG oder nach § 78 Abs. 5 des AufenthG erfolgt. Beim zweiten Verfahren werden Anträge und Anzeigen mittels De-Mail an die Behörde versandt. Auch soll durch sonstige sichere Verfahren, die durch Rechtsverordnung festgelegt werden sollen, die qualifizierte Elektronische Signatur ebenfalls ersetzt werden können.

§ 3a Abs. 2 VwVfG

Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach Signaturgesetz versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die Behörde ermöglicht, ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2. bei Anträgen oder Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4. durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrats festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.

Das HMDIS hat mir Gelegenheit zur Stellungnahme zu dem Gesetzentwurf gegeben, die ich gerne wahrgenommen habe. Insbesondere die nachfolgenden Aspekte erschienen mir erörterungsbedürftig.

Sowohl die Formularserver-Lösung als auch die De-Mail-Lösung unterscheiden sich in einem wichtigen Punkt von der qualifizierten elektronischen Signatur (qeS). Bei einer qeS wird ein Dokument

signiert. Der Empfänger kann für die Dauer von 30 Jahren prüfen, ob das Dokument unversehrt ist und von wem es signiert wurde. Der Absender kann sicher sein, dass jede nachträgliche Änderung am Dokument zu einer Fehlermeldung führt. Das entspricht weitgehend den Prüfmöglichkeiten bei Papierdokumenten.

Im Fall der Bereitstellung von Formularen und Nutzung des elektronischen Identitätsnachweises durch den Absender kann der Empfänger sicher sein, dass das Formular von der richtigen Person ausgefüllt wurde. Nachdem das Formular ausgefüllt abgelegt wurde, müssen aber die technischen Sicherheitsmaßnahmen des Empfängers Änderungen verhindern und die Urheberschaft dokumentieren. Der Absender muss folglich darauf vertrauen, dass der Empfänger alle erforderlichen Maßnahmen ergriffen hat, um nachträgliche Änderungen zu verhindern.

Im Fall der De-Mail Nutzung gilt, dass der De-Mail-Anbieter die Identität des Absenders prüft, ein angehängtes Dokument auf Schadsoftware prüft und dann signiert. Der Empfänger bekommt die Bestätigung, dass ein Dokument / eine E-Mail eines sicher identifizierten Absenders vorliegt. Hier wäre es technisch möglich, dass der De-Mail Anbieter Änderungen vornimmt. Allerdings ist nach der Übertragung eine Änderung wie bei einer qeS nicht mehr möglich. Ich habe aber Zweifel, dass die Signatur selbst mit einer qeS vergleichbar ist. Mit einer qeS drückt eine Person ihren Willen aus. Um ein Dokument mit einer qeS zu versehen, gibt daher eine Person ihre PIN ein, und daraufhin wird die Signatur erzeugt. Im Fall des De-Mail-Anbieters wird die Signatur aber ohne Zutun einer Person automatisch erzeugt. Es ist daher nur eine technische Signatur, die der Integritätssicherung dient.

Man kann also feststellen, dass drei Verfahren als gleichwertig definiert werden, die durchaus unterschiedliche Qualität haben. Vor diesem Hintergrund hatte ich angeregt, dass die Fälle mit einem Schriftformerfordernis sinnvoll reduziert werden sollen, statt die Anforderungen an eine technische Umsetzung zu verändern. Dort wo ein Schriftformerfordernis nach wie vor bestehen soll, sollte dann auch mit einer qeS signiert werden.

Nicht jedes Formular mit einem Unterschriftenfeld steht für einen Vorgang mit dem Erfordernis einer Schriftform. Dies wird auch in § 13 EGovG festgestellt. Allerdings ist es kaum nachvollziehbar, wenn bei elektronischer Versendung keine Unterschrift verlangt wird, diese aber auf dem Papierformular noch erwartet wird.

§ 13 EGovG

Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt. Bei

einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.

Ich hatte auch angemerkt, dass die Regelung des § 11 EGovG zu gemeinsamen Verfahren sinnvollerweise in das BDSG hätte aufgenommen werden sollen, da es hier explizit um datenschutzrechtliche Fragestellungen geht.

§ 11 Abs. 1 EGovG

Gemeinsame Verfahren sind automatisierte Verfahren, die mehreren verantwortlichen Stellen im Sinne des Bundesdatenschutzgesetzes die Verarbeitung personenbezogener Daten in oder aus einem Datenbestand ermöglichen. Soweit gemeinsame Verfahren auch Abrufe anderer Stellen ermöglichen sollen, gilt insoweit für die Abrufverfahren § 10 Bundesdatenschutzgesetz.

Auch die Vorschrift zur Georeferenzierung in § 14 EGovG habe ich kritisch gesehen.

§ 14 Abs. 1 EGovG

Wird ein elektronisches Register, welches Angaben mit Bezug zu inländischen Grundstücken enthält, neu aufgebaut oder überarbeitet, hat die Behörde in das Register eine bundesweit einheitlich festgelegte direkte Georeferenzierung (Koordinate) zu dem jeweiligen Flurstück, dem Gebäude oder zu einem in einer Rechtsvorschrift definierten Gebiet aufzunehmen, auf welches sich die Angaben beziehen.

Die Datenerhebung ist zu zulässigen Zwecken nicht erforderlich und birgt stattdessen die Gefahr einer unzulässigen Zusammenführung von Daten mittels dieser Referenzierung. Gleichwohl wurde die Vorschrift nicht geändert.

Die ausschließliche Publikation von amtlichen Mitteilungs- und Verkündungsblättern durch eine elektronische Ausgabe, wie sie § 15 EGovG vorsieht, habe ich abgelehnt.

Eine generelle Einführung der Veröffentlichung via Internet bei personenbezogenen Daten ist deshalb problematisch, weil sie weder dem datenschutzrechtlichen Erforderlichkeitsgrundsatz entspricht (die weltweite dauerhafte Veröffentlichung ist nicht erforderlich) noch die Rechte der Betroffenen und deren schutzwürdige Interessen berücksichtigt.

§ 15 Abs. 1 EGovG

Eine durch Rechtsvorschrift des Bundes bestimmte Pflicht zur Publikation in einem amtlichen Mitteilungs- oder Verkündungsblatt des Bundes, eines Landes oder einer Gemeinde kann unbeschadet des Artikels 82 Absatz 1 des Grundgesetzes zusätzlich oder ausschließlich durch eine elektronische Ausgabe erfüllt werden, wenn diese über öffentlich zugängliche Netze angeboten wird.

Ferner ist durch die Änderungen in Artikel 6 und 7 des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, dessen Artikel 1 das EGovG ist, festgestellt worden, dass bei der De-Mail die kurzzeitige Entschlüsselung, Prüfung und dann Signatur der Dokumente keine unbefugte Übermittlung bzw. Kenntnisnahme im Sinne des SGB X oder der Abgabenordnung darstellt (Änderung in § 67 Abs. 6 S. 2 Nr. 3 SGB X, § 30 Abs. 7 AO, § 87a Abs. 1 AO). So sinnvoll diese Feststellung sein mag, um die elektronische Verwaltung zu fördern, so wäre es doch besser gewesen, den Bürgern eine Ende-zu-Ende-Verschlüsselung zur Verfügung zu stellen. Nur durch eine Ende-zu-Ende-Verschlüsselung ist sichergestellt, dass eine Kenntnisnahme während der Datenübertragung nicht möglich ist.

Das Hessische Innenministerium hat zwar einige meiner Kritikpunkte geteilt (u.a. die Kritik an der fehlenden Ende-zu-Ende-Verschlüsselung), wertete jedoch den Gesetzentwurf insgesamt als tragfähige Grundlage für die Förderung der elektronischen Verwaltung und hat deswegen den Gesetzentwurf im Bundesrat nicht abgelehnt.

3.3 Hessen

3.3.1 Querschnitt

3.3.1.1
Die behördlichen Datenschutzbeauftragten als interne und externe Ansprechpartner

Behördliche Datenschutzbeauftragte sind nicht nur interne Ansprechpartner für Behördenleitung und Mitarbeiter, sondern auch Anlaufstelle für Außenstehende und den Hessischen Datenschutzbeauftragten. Insofern ist es wichtig, dass nach innen und außen transparent gemacht wird, wer behördliche Datenschutzbeauftragte bzw. behördlicher Datenschutzbeauftragter ist.

Zu diesem Thema hatte ich bereits im 39. Tätigkeitsbericht, Ziff. 4.1.1. grundsätzliche Ausführungen gemacht und darauf hingewiesen, dass behördlich bestellte Datenschutzbeauftragte intern und extern namentlich bekannt sein müssen. Um dies zu gewährleisten habe ich gefordert, dass die Behörde dafür Sorge zu tragen hat, dass sowohl die Beschäftigten als auch insbesondere die Telefonzentrale wissen muss, wer die oder der behördliche Datenschutzbeauftragte ist. Darüber hinaus hielt ich eine entsprechende Veröffentlichung auf der Homepage und im Organisationsplan der Behörde für erforderlich.

In einem Beschwerdefall eines Mitarbeiters einer großen Mittelbehörde gegen die personalverwaltende Stelle beabsichtigte ich, zur Beurteilung des Sachverhaltes die Unterstützung der bzw. des behördlichen Datenschutzbeauftragten einzuholen.

Meine Recherche auf der Homepage der Behörde, welche Person diese Funktion ausübt, lief zunächst ins Leere, da dies weder aus dem Organisationsplan hervorging, noch an anderer Stelle auf der Homepage ein Hinweis zu finden war.

Eine mündliche Anfrage über die Telefonzentrale hatte zur Folge, dass die Mitarbeiterin erst im Organisationsdezernat nachfragen musste, wer bestellt ist, um mir dann Auskunft geben zu können.

Ganz im Sinne meiner Ausführungen zu diesem Thema im 39. Tätigkeitsbericht, Ziff. 4.1.1, forderte ich den behördlichen Datenschutzbeauftragten auf, zu veranlassen, dass er namentlich und der Behördenleitung unmittelbar zugeordnet im Organisationsplan – als Stabsstelle – aufgeführt wird.

Dies lehnte die Behörde mit folgenden Argumenten ab:

Der Organisationsplan solle informativ, übersichtlich und als Ausdruck auf einer DIN A4-Seite lesbar sein. Man könne daher nicht alle Sonderfunktionen und Beauftragten einer Behörde im Organisationsplan aufführen. Im Übrigen würde im Organisationsplan beim Dezernat Justiziariat als Zusatz das Wort „Datenschutz“ aufgeführt, dies sei Hinweis genug.

Darüber hinaus hätte der Datenschutzbeauftragte in erster Linie hausinterne Zuständigkeiten und die Mitarbeiter der Behörde seien über Person und Aufgaben des Datenschutzbeauftragten ausreichend durch den Geschäftsverteilungsplan und das Intranet informiert. Außerdem könne dann im Rahmen der Gleichbehandlung jeder andere Beauftragte auch verlangen, im Organisationsplan genannt zu werden, und dies sei aus den genannten Gründen nicht machbar.

Diese Argumente überzeugten mich nicht. Anders als z.B. Personalrat, Frauenbeauftragte, Vertrauensperson der Schwerbehinderten, Arbeitssicherheitsbeauftragter ist der oder die behördliche Datenschutzbeauftragte nicht nur Anlaufstelle für Beschäftigte, sondern auch für Außenstehende. Dies ist Ausfluss des Transparenzgrundsatzes, der wichtige Säule des europäischen Datenschutzrechts ist, wie ich bereits im 39. Tätigkeitsbericht ausführlich dargelegt habe. Zur Transparenz nach außen gehört – ergänzend zu meinen bereits im 39. Tätigkeitsbericht formulierten Forderungen – auch, dass behördliche Datenschutzbeauftragte im Organisationsplan von Behörden namentlich und entsprechend § 5 Abs. 1 Satz 3 HDSG der Behördenleitung unmittelbar zugeordnet – als Stabsstelle – aufzuführen sind.

Erfreulicherweise haben meine Hinweise bei der Behördenleitung schließlich doch noch gefruchtet. Inzwischen ist der behördliche Datenschutzbeauftragte im Organisationsplan der Behörde als Stabsstelle dargestellt und namentlich benannt.

3.3.1.2
Löschen im Dokumentenmanagementsystem der hessischen Landesverwaltung

In der hessischen Landesverwaltung müssen die elektronischen Dokumente aus dem eingesetzten Dokumentenmanagementsystem am Ende der Aufbewahrungsfristen dem Hessischen Staatsarchiv angeboten werden. Von diesem als nicht archivwürdig eingestufte Dokumente müssen gelöscht werden. Dies ist derzeit noch nicht möglich, da die technischen Voraussetzungen hierzu fehlen. Es muss zeitnah Abhilfe geschaffen werden.

3.3.1.2.1
Sachstand des Einsatzes des Dokumentenmanagementsystems

Die Einführung eines Dokumentenmanagementsystems (HeDok) ist eines der Ziele der eGovernment-Strategie des Landes Hessen.

Nach der Auswahl des Systems DOMEA wurde das Ziel bisher in drei abgeschlossenen Teilprojekten 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), das im 39. Tätigkeitsbericht (Ziff. 4.4.1) beschrieben ist, stellte im Jahr 2009 den Abschluss dieses Gesamtprojektes dar. Dabei ging es – entgegen dem Eindruck, den die Bezeichnung weckt, – nicht um die Überführung der Dokumente in das Archiv, sondern um die längerfristige Aufbewahrung in der aktenführenden Stelle.

Nach einer Einführungs- und Erprobungsphase wechseln seit 2010 mehr und mehr oberste Landesbehörden zu einer führenden eAkte in HeDok: in Papierform eingehende Dokumente werden in HeDok überführt und anschließend vernichtet; die Akten sind dort nur noch elektronisch vorhanden.

Ein weiterer Schritt, nämlich Dokumente dem Staatsarchiv elektronisch anbieten oder endgültig löschen zu können, steht noch aus. Hierfür müssen die technischen Voraussetzungen geschaffen werden: die Aussonderungsschnittstelle für HeDok muss programmiert werden.

3.3.1.2.2
Sachstand DIMAG und Aussonderungsschnittstelle für HeDok

Das Hessische Staatsarchiv selbst verwendet als Archivierungssystem DIMAG. Dieses System soll die aus HeDok ausgesonderten eAkten aufnehmen. Dabei handelt es sich um eine Eigenentwicklung des Landesarchivs Baden-Württemberg, die seit Januar 2011 in Hessen eingesetzt wird. Diese Software wird in einer Entwicklungspartnerschaft zwischen den staatlichen Archiven verschiedener Bundesländer (Baden-Württemberg, Hessen und Bayern) gepflegt und weiterentwickelt.

Ziel dieses gemeinsamen Projekts ist es, ein einheitliches Aussonderungsverfahren aus dem eingesetzten Dokumentenmanagementsystem zu definieren und so einerseits einen standardisierten

Prozess zu schaffen, andererseits aber natürlich auch Kosten zu sparen. Das gemeinsame Anforderungskonzept wurde bereits im Frühjahr 2011 fertig gestellt. Nach anfänglicher Skepsis beteiligte sich die Herstellerfirma des Dokumentenmanagementsystems sehr engagiert und zielstrebig an diesem Projekt, sodass sie im Juni 2011 ein erstes Umsetzungskonzept vorlegen konnte. Einzig offener Punkt war zu diesem Zeitpunkt noch die Spezifikation der Metadaten-Dateien, die in Absprache und Zusammenarbeit zwischen den Anwendern und der Herstellerfirma bis Mai 2012 abgeschlossen werden konnte.

Seit Ende des Jahres 2012 liegt den Bundesländern, die die Anforderungen an die Aussonderung aus dem eingesetzten Dokumentenmanagementsystem gemeinsam definiert haben, ein Angebot der Herstellerfirma zur Umsetzung vor. Nach Erteilung des Programmierauftrags hätte das Aussonderungsverfahren im folgenden Jahr umgesetzt und in Betrieb genommen werden sollen.

3.3.1.2.3
Rechtslage

Die Hessische Landesverwaltung verarbeitet innerhalb ihres breiten Aufgabenspektrums vielerlei Daten – auch solche, die personenbezogen sind.

Nach dem Hessischen Datenschutzgesetz sind personenbezogene Daten zu löschen, wenn sie für die mit ihnen erfüllten Zwecke nicht mehr erforderlich sind (§ 19 Abs. 3 HDSG).

§ 19 Abs. 3 HDSG

Personenbezogene Daten sind unverzüglich zu löschen, sobald feststeht, daß ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 weiterverarbeitet werden dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer auf Grund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Akten sind zur Aufgabenerfüllung nicht mehr erforderlich, wenn die Bearbeitung abgeschlossen ist und entweder spezialgesetzlich geregelte oder die für Schriftgut des Landes Hessen festgelegten Aufbewahrungsfristen abgelaufen sind. In den Anhängen zum Erlass der Landesregierung zur Aktenführung in den Dienststellen des Landes Hessen (Aktenführungserlass – AfE) vom 14. Dezember 2012 (StAnz. 2013 S. 3 ff.) sind einige allgemeine und besondere Aufbewahrungs-

fristen aufgeführt. Die Regelaufbewahrungsfrist beträgt für die federführende Stelle fünf Jahre (s. Anlage B zum AfE). Die meisten Dokumente werden dieser Aufbewahrungsfrist unterliegen.

Mit Ablauf der Aufbewahrungsfristen sind Akten auszusondern und dem zuständigen Archiv anzubieten, das innerhalb von sechs Monaten über die Archivwürdigkeit der angebotenen Unterlagen zu entscheiden hat (§ 8 Abs. 1 Satz 1 und 3 HArchivG).

§ 8 Abs. 1 Satz 1 und 3 HArchivG

Die in § 2 Abs. 3 und 6 genannten Stellen sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr benötigt werden und deren Aufbewahrungsfrist abgelaufen ist, unverzüglich auszusondern und dem zuständigen Archiv zur Archivierung anzubieten. … Das zuständige Archiv hat binnen sechs Monaten über die Archivwürdigkeit angebotener Unterlagen zu entscheiden.

Akten, die nicht archivwürdig sind, sind zu vernichten. Bei elektronischen Dokumenten bedeutet dies, dass sie zu löschen sind. Derzeit behilft sich die Landesverwaltung damit, dass die elektronischen Akten bestenfalls in die Langzeitarchivierung in HeDok übernommen werden. Damit sind sie jedoch immer noch im Zugriff der jeweiligen Behörde und weder ausgesondert noch gelöscht. Bei personenbezogenen Daten, die in der Mehrzahl der Akten der Landesverwaltung enthalten sind, bedeutet dies einen Verstoß gegen das Hessische Datenschutzgesetz.

3.3.1.2.4
Forderungen

Zur Umsetzung der eGovernment-Strategie des Landes Hessen gehört es auch, die für die Aussonderungsschnittstelle erforderlichen finanziellen Mittel zur Verfügung zu stellen.

Bei einer schnellen Weiterführung des Projektes kann im günstigsten Fall aus heutiger Sicht im Jahr 2015 mit der Anbietung und Aussonderung elektronischer Akten begonnen werden. Schon jetzt ist die Regelaufbewahrungsfrist weit überschritten. Bis zur Umsetzung der Schnittstelle zur Archivierung nimmt die Landesregierung das weitere Anwachsen von Datenschutzverstößen durch nicht rechtzeitiges Löschen nicht mehr erforderlicher personenbezogener Daten in Kauf.

Dies werde ich beanstanden müssen, wenn nicht zeitnah Aktivitäten zur Beendigung dieses Zustandes ergriffen werden.

3.3.2 Justiz, Strafvollzug und Ordnungswidrigkeiten

3.3.2.1
Umsetzung der Neuregelungen des Telekommunikationsgesetzes zur Bestandsdatenauskunft in Landesrecht

Der Landesgesetzgeber hat umfassend von seiner Kompetenz Gebrauch gemacht, den Sicherheitsbehörden einen Zugriff auf Bestandsdaten der Telekommunikationsanbieter zu ermöglichen.

Das Bundesverfassungsgericht hatte im Januar 2012 entschieden (1 BvR 1299/05, BVerwGE 130, 151), dass eine qualifizierte Rechtsgrundlage notwendig sei, um den Sicherheitsbehörden einen Auskunftsanspruch gegenüber den Telekommunikationsunternehmen, bezogen auf Bestandsdaten im Sinne des § 111 Telekommunikationsgesetz (TKG), einzuräumen.

§ 111 Absatz 1 TKG

Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. Die Verpflichtung zur unverzüglichen Speicherung nach Satz 1 gilt hinsichtlich der Daten nach Satz 1 Nr. 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Satz 1 Nr. 1 und 2 erhebt, wobei an die Stelle der Daten nach Satz 1 Nr. 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Satz 1 Nr. 2 der Inhaber des elektronischen Postfachs tritt. Wird dem Verpflichteten nach Satz 1 oder Satz 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat der nach Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung

der Daten ohne besonderen Aufwand möglich ist. Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

In seiner Entscheidung hatte das BVerfG das „Doppeltürmodell“ entwickelt. Danach ist zum einen eine konkrete Norm erforderlich, die die Übermittlung gestattet (erste Tür) sowie eine weitere Norm für die Rahmenbedingungen des Abrufs (zweite Tür). Weiterhin wurde entschieden, dass auch für die Nutzung dynamischer IP-Adressen in diesem Zusammenhang eine normenklare Regelung erforderlich ist, die den besonderen Anforderungen des Eingriffs in das Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG gerecht wird.

Die Ausgestaltung der ersten Tür hat der Bundesgesetzgeber mit dem Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (BGBl. I, S. 16029) geschaffen.
Die Verpflichtung der Telekommunikationsunternehmen zur Auskunftserteilung ergibt sich nunmehr aus § 113 TKG.

§ 113 TKG

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, darf nach Maßgabe des Absatzes 2 die nach den §§ 95 und 111 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen.
(2) Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt; an andere öffentliche und nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Bei Gefahr im Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen.
(3) Stellen im Sinne des Absatzes 1 sind

1. die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten zuständigen Behörden;
2. die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden;
3. die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst.

(4) Derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die zu beauskunftenden Daten unverzüglich und vollständig zu übermitteln. Über das Auskunftsersuchen und die Auskunftserteilung haben die Verpflichteten gegenüber den Betroffenen sowie Dritten Stillschweigen zu wahren.

(5) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen. Wer mehr als 100 000 Kunden hat, hat für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle nach Maßgabe der Technischen Richtlinie nach § 110 Absatz 3 bereitzuhalten, durch die auch die gegen die Kenntnisnahme der Daten durch Unbefugte gesicherte Übertragung gewährleistet ist. Dabei ist dafür Sorge zu tragen, dass jedes Auskunftsverlangen durch eine verantwortliche Fachkraft auf Einhaltung der in Absatz 2 genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird.

Für die Regelungen, die den Sicherheitsbehörden des Landes die zweite Tür öffnen, liegt die Gesetzgebungskompetenz beim Hessischen Landtag. Er hatte auch darüber zu entscheiden, in welchem Umfang von dieser Kompetenz Gebrauch gemacht werden sollte.

Ausgehend von der Rechtsprechung des BVerfG waren zur Zulässigkeit von Auskunftsbegehren drei Gruppen von Daten zu beurteilen:

– die Bestandsdaten gem. §§ 95 und 111 TKG,

– die sogenannten Zugangssicherungscodes gem. § 113 Absatz 1 Satz 2 TKG. Dabei handelt es sich um Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder auch hiervon räumlich getrennten Speichereinrichtungen geschützt wird. Dazu gehören z.B. PIN und PUK (Personal Identification Number and Personal Unblocking Key),

– die Dynamischen IP-Adressen, d.h. die zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adressen. Diese Daten sind nur durch eine Verknüpfung mit Verkehrsdaten einem bestimmten Nutzer zuzuordnen. Daher hatte das BVerfG dafür eine ausdrückliche gesetzliche Regelung verlangt, die den Anforderungen an einen Eingriff in das Telekommunikationsgeheimnis aus Art. 10 Abs. 1 GG gerecht wird.

Das Gesetzgebungsverfahren im Landtag wurde durch einen gemeinsamen Gesetzentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Gesetzes über das Landesamt für Verfassungsschutz vom 12. März 2013 eingeleitet (LTDrs. 18/7137). Dieser Entwurf war zeitlich vor den entscheidenden Beratungen im Bundestag vorgelegt worden. Er sollte den hessischen Sicherheitsbehörden einen umfassenden Zugriff auf diese Daten ermöglichen. In der vorgelegten Form wurde der Entwurf den verfassungsrechtlichen Anforderungen an einen Eingriff in das Recht auf informationelle Selbstbestimmung sowie das Telekommunikationsgeheimnis gem. Art. 10 GG jedoch nicht gerecht.

In einer Anhörung im Innenausschuss des Landtages hatte ich Gelegenheit, die Defizite des Gesetzesvorschlages aufzuzeigen.

Insbesondere für die Daten gem. § 113 Abs. 1 S. 2 TKG habe ich eine differenziertere Regelung gefordert. Zugangssicherungscodes (wie etwa Passwörter, PIN und PUK) selbst sind zwar Bestandsdaten im Sinne des TKG, sie haben jedoch einen höheren Schutzbedarf als die herkömmlichen Bestandsdaten, da mit ihrer Hilfe nicht nur der Umfang, sondern auch der Inhalt einer Kommunikationsbeziehung erschlossen werden kann. Insoweit entspricht der Eingriffsgehalt bei Auskünften solcher Daten eher dem einer Auskunft zu einer dynamischen IP-Adresse als zu sonstigen Bestandsdaten. Da in aller Regel solche Daten deshalb nur dann erforderlich sein können, wenn auch auf die durch sie erschließbaren Inhaltsdaten zugegriffen werden soll, war eine Beschränkung der Auskunftsmöglichkeiten erforderlich. So hatte auch der Bundesgesetzgeber – soweit er für die Sicherheitsbehörden des Bundes die Regelungen zur zweiten Tür gestaltet hat – eine zusätzliche Anforderung formuliert. Danach ist eine solche Datenerhebung nur zulässig, wenn auch die gesetzlichen Voraussetzungen für die Daten vorliegen, auf die mittels dieser Bestandsdaten zugegriffen werden kann. Dies entspricht auch der Rechtsprechung des BVerfG. Zugangssicherungscodes erfordern mit anderen Worten einen vorverlagerten Datenschutz.

Aus dem erhöhten Schutzbedarf der Zugangssicherungscodes folgt meines Erachtens zudem, dass diese Daten nicht – wie im Gesetzentwurf vorgesehen – von der Notwendigkeit einer richterlichen Anordnung ausgenommen werden können. Schließlich halte ich für diese Daten auch eine Benachrichtigung der Betroffenen für erforderlich.

Für die dynamischen IP-Adressen war nur im HSOG, nicht aber im LfV-Gesetz, eine differenzierte Regelung vorgesehen. Auch dies wurde den verfassungsrechtlichen Anforderungen insbesondere wegen des Eignriffs in das Telekommunikationsgeheimnis nicht gerecht.

Im Anschluss an die Anhörung im Innenausschuss des Hessischen Landtages erfolgte eine Überarbeitung des Gesetzentwurfes, die zumindest teilweise den – nicht nur von mir – geäußerten Bedenken Rechnung getragen hat.

Für die Tätigkeit der Polizei im Rahmen der Gefahrenabwehr wird nunmehr differenziert zwischen der Abfrage von reinen Bestandsdaten und den Zugangssicherungscodes. Diese dürfen nur erhoben werden, wenn auch die gesetzlichen Voraussetzungen für die Nutzung der Daten, die mit ihrer Hilfe erschließbar sind, vorliegen. Auch die notwendigen verfahrenssichernden Maßnahmen wurden getroffen.

§ 15a Absatz 2 HSOG

Unter den Voraussetzungen des Abs. 1 können die Polizeibehörden auch Auskunft über Verkehrsdaten nach § 96 Abs. 1 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 20. Juni 2013 (BGBl. I S. 1602), in einem zurückliegenden oder einem zukünftigen Zeitraum sowie über Inhalte verlangen, die innerhalb des Telekommunikationsnetzes in Speichereinrichtungen abgelegt sind. Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften. Auskunft über Bestandsdaten nach den §§ 95 und 111 des Telekommunikationsgesetzes können die Polizeibehörden von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, unter den Voraussetzungen des § 12 Abs. 1 Satz 1, Abs. 3 und 4 verlangen (§ 113 Abs. 1 Satz 1 und 3 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 3 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Die Auskunft über Bestandsdaten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse darf nur zur Abwehr einer gegenwärtigen erheblichen Gefahr verlangt werden. § 29 Abs. 6 gilt für Satz 4 und 5 entsprechend.

Im LfV-Gesetz wurden die Befugnisse differenzierter ausgestaltet.

§ 4a LfV-Gesetz

.....

(3) Das Landesamt für Verfassungsschutz darf, soweit dies zur Erfüllung seiner Aufgaben nach § 2 Abs. 2 erforderlich ist, von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 20. Juni 2013 (BGBl. I

S. 1602), erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 und 3 des Telekommunikationsgesetzes); dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes). Die Auskunft darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Abs. 1 Satz 3 des Telekommunikationsgesetzes). Die Auskunft darf nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

.....

(5) Auskünfte nach Abs. 3, soweit Daten nach § 113 Abs. 1 Satz 2 und 3 des Telekommunikationsgesetzes betroffen sind, und Auskünfte nach Abs. 4 dürfen nur auf Anordnung des für den Verfassungsschutz zuständigen Ministeriums eingeholt werden. Die Anordnung ist durch die Leiterin oder den Leiter des Landesamts für Verfassungsschutz oder seine Vertreterin oder seinen Vertreter schriftlich zu beantragen. Der Antrag ist zu begründen. Das Ministerium unterrichtet unverzüglich die G10-Kommission (§ 2 Abs. 1 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz vom 16. Dezember 1969 [GVBl. I S. 303], zuletzt geändert durch Gesetz vom 27. September 2012 [GVBl. S. 290]) über die Anordnung vor deren Vollzug. Bei Gefahr im Verzug kann das Ministerium den Vollzug der Anordnung auch bereits vor Unterrichtung der Kommission anordnen. Die G10-Kommission prüft von Amts wegen oder aufgrund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften. § 15 Abs. 5 des Artikel 10-Gesetzes ist entsprechend anzuwenden. Anordnungen, die die G10-Kommission für unzulässig oder nicht notwendig erklärt, hat das Ministerium unverzüglich aufzuheben. Für die Verarbeitung der erhobenen Daten nach Abs. 3, soweit Daten nach § 113 Abs. 1 Satz 2 und 3 des Telekommunikationsgesetzes betroffen sind, und für die Verarbeitung der nach Abs. 4 Nr. 1 bis 3 erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden. § 12 Abs. 1 und 3 des Artikel 10-Gesetzes findet entsprechende Anwendung.

3.3.2.2
Prüfung der HZD Hünfeld

In diesem Jahr habe ich geprüft, ob die HZD Hünfeld als Dienstleister der Hessischen Justiz Anforderungen erfüllt, die seitens der Justiz an sie gerichtet wurden. Trotz einiger Bereiche, in denen Anpassungen erforderlich sind, ergab sich ein positiver Gesamteindruck.

Mitte des Jahres habe ich die Umsetzung von Sicherheitsbelangen geprüft, die im Rahmen der von der HZD für die Hessische Justiz erbrachten Leistungen zu erfüllen sind. Gegenstand der Prüfung war neben räumlichen Sicherheitsmaßnahmen insbesondere die Umsetzung von Vorgaben

aus einem Netzkonzept hinsichtlich der Fernbetreuung von Nutzern sowie administrativer Zugriffe auf Benutzerverzeichnisse und E-Mail-Konten.

Die Anforderungen wurden bei den räumlichen Sicherungsmaßnahmen und bei der Fernbetreuung von Nutzern voll erfüllt.

Es gab aber einige Punkte, die geändert werden mussten:

– Es gab zu viele Personen mit (Domänen-) Administratorrechten.

  Durch diese weitgehenden Zugriffsrechte hatten Mitarbeiter potentiell die Möglichkeit, auf Daten zuzugreifen, auch wenn es nicht immer für ihre Aufgaben erforderlich war.

  Der HZD war dieser Umstand bewusst. Im Rahmen einer Neukonzeption soll die Anzahl der Personen mit Administratorrechten reduziert werden. Das Ziel ist es, die Anzahl auf weniger als ein Drittel zu senken.

– Die Tätigkeit von Administratoren der E-Mail-Plattform war nur eingeschränkt nachvollziehbar.

  Die Administration der E-Mail-Plattform der Justiz wird weitgehend durch die HZD Hünfeld durchgeführt. Zentrale Aufgaben, um die technische Infrastruktur lauffähig zu halten, werden auch durch die HZD in Wiesbaden durchgeführt. Eine Aufgabe von Administratoren ist die Vergabe von Zugriffsrechten auf Postfächer. Sie können potentiell jedem Nutzer der Plattform, auch sich selbst, den Zugriff auf ein beliebiges Postfach einräumen. Es ist festgelegt, dass ein Auftrag vorliegen muss, damit Zugriffsrechte geändert werden. Die entsprechenden Aufträge werden dokumentiert. Zum Zeitpunkt der Prüfung gab es aber kein Auswerteprogramm, mit dem die systemseitigen Protokolldaten daraufhin kontrolliert werden, ob ein Administrator der E-Mail-Plattform Zugriffsrechte auf ein Postfach geändert hat. Es würde daher nur zufällig erkannt, wenn ein Administrator sich oder anderen Nutzern ohne Auftrag Zugriff auf ein Postfach verschafft.

  Der HZD war der Umstand bekannt, und es war daher schon eine entsprechende Kontrollsoftware beschafft. Diese soll ab Anfang 2014 eingerichtet werden und den mit der Kontrolle beauftragten Mitarbeitern zur Verfügung stehen.

– Es war für einen Systemrevisor praktisch nicht möglich, eine Besitzübernahme durch Administratoren auf gesperrte persönliche Verzeichnisse, bspw. von Richtern, zu erkennen.

Nach dem Netzkonzept der Hessischen Justiz gibt es u.a. bei Gerichten die Funktion des Systemrevisors. Systemrevisoren sollen Systemprotokolle auswerten, um Auffälligkeiten festzustellen. Ein auffälliges Ereignis liegt bspw. vor, wenn sich ein Administrator Zugriffsrechte auf das persönliche Verzeichnis eines Richters einräumt. Dazu muss man folgendes wissen: Nach den vergebenen Zugriffsrechten haben Systemadministratoren der HZD kein Zugriffsrecht auf das persönliche Verzeichnis eines Richters. D.h. der Administrator kann bspw. keine Dateien lesen oder verändern. Allerdings könnte er sich Zugriffsrechte verschaffen. Als ersten Schritt müsste er eine sog. Besitzübernahme bei dem Verzeichnis vornehmen, um anschließend die Zugriffsrechte ändern zu können. Dann könnte er für sich oder andere Benutzer Lese- und Schreibrechte vergeben. Der Vorgang einer Besitzübernahme wird protokolliert und kann durch den Systemrevisor festgestellt werden.

Bedingt durch einen Softwarewechsel haben sich unerwartete Probleme ergeben. Es wurde entsprechend dem Netzkonzept der Zugriff auf Verzeichnisse protokolliert. Durch die neue Softwareversion wurden aber neben den Besitzübernahmen durch Administratoren auch systemseitige Zugriffe auf Verzeichnisse, bspw. im Rahmen der Datensicherung, unter identischen Ereignisnummern protokolliert. Durch die große Zahl von Protokolleinträgen war es damit einem Systemrevisor praktisch nicht mehr möglich, unberechtigte Besitzübernahmen zu erkennen.

Auch dieser Umstand wurde durch die HZD als änderungsbedürftig angesehen. Um die Anforderungen erfüllen zu können, wird nach einer besseren Software zur Protokollauswertung gesucht. Das Ergebnis stand bei Redaktionsschluss dieses Tätigkeitsberichts noch nicht fest.

– Es war nach Fertigstellung eines Auftrags nicht möglich, an Hand der Einträge im Ticketsystem zu erkennen, welcher Mitarbeiter den Auftrag ausgeführt hat.

Die HZD nutzt ein Ticketsystem, um Aufträge und deren Abarbeitung zu dokumentieren. Dazu wird bei Eingang eines Auftrages bzw. einer Fehlermeldung durch einen Mitarbeiter ein neuer Auftrag angelegt und der Fehler bzw. der Auftrag dokumentiert. Anschließend wird er an die zuständigen Bearbeiter weitergeleitet. Diese dokumentieren im Ticketsystem ihre Tätigkeit. Wenn mehrere Mitarbeiter an einem Auftrag arbeiten, beschreibt jeder seine Tätigkeiten. Nach Abschluss des Auftrags wird dieser im System als beendet gekennzeichnet.

Bei der HZD gibt es eine Anpassung, durch die bei Beendigung des Auftrags die Namen der beteiligten Mitarbeiter gelöscht werden. Es bleibt zwar die Beschreibung des Auftrags resp. des Fehlers und seine Bearbeitung als eine Art Wissensdatenbank erhalten, jedoch ist nicht mehr nachvollziehbar, wer was veranlasst hat.

Für die Nachvollziehbarkeit der Tätigkeit von Administratoren ist dies ein Problem. Nach § 10 Abs. 2 Ziff. 6 HDSG ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle). Durch das frühzeitige Löschen von Ticket-Ersteller und -bearbeiter ist schon ab Abschluss des Tickets nicht mehr nachvollziehbar, wer wie agiert hat. Da das Remedy-System Teil der Dokumentation ist, erfolgt die Anonymisierung zu früh.

Zu diesem Punkt steht eine Reaktion der HZD noch aus.

Die gefundenen Defizite betrafen vor allem die Nachvollziehbarkeit der Tätigkeit von Administratoren. Für den Nachweis, dass entsprechend den Vorgaben des Auftraggebers gearbeitet wurde und die Anforderungen von § 10 Abs. 2 Ziff. 6 HDSG (Auftragskontrolle) erfüllt sind, ist die Nachvollziehbarkeit unerlässlich.

Es zeigt sich, dass sich die HZD der Defizite in weiten Teilen bewusst war. Nicht in allen Bereichen ist es jedoch gelungen, zeitnah eine Abhilfe zu schaffen.

Ich habe das Justizministerium zeitgleich mit der HZD über die Ergebnisse meiner Prüfung in Kenntnis gesetzt. Nach meiner Einschätzung muss auch das Justizministerium die eigenen Maßnahmen zur Auftragskontrolle hinterfragen. In diesem Zusammenhang spielt die IT-Kontrollkommission der Justiz eine wesentliche Rolle, die nach § 3 des Gesetzes zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten vom 16. Dezember 2011 eingerichtet wurde. Die IT-Kontrollkommission prüft insbesondere die HZD in Hünfeld und hat im Rahmen ihrer Tätigkeit erste Ergebnisse erzielt. Ich gehe davon aus, dass die Qualität der Dienstleistung der HZD durch deren regelmäßige Überprüfungen verbessert wird.

§ 3 JITStG

(1) Soweit im Rahmen der Fachaufsicht nach § 2 Satz 2 Überprüfungen zum Schutz vor unbefugten Zugriffen durch Mitarbeiterinnen und Mitarbeiter der Hessischen Zentrale für Datenverarbeitung erfolgen sollen, wirkt eine einzurichtende IT-Kontrollkommission mit.

(2) Die IT-Kontrollkommission besteht aus
1. je einer Vertreterin oder einem Vertreter
   a) der IT-Stelle,
   b) jedes Bezirksrichterrats und des Richterrats des Hessischen Finanzgerichts zum Schutz der richterlichen Unabhängigkeit,

c) des Bezirksstaatsanwaltsrats zum Schutz des Legalitätsprinzips,

2. einer vom Hauptpersonalrat der Justiz zu benennenden Person, bei der oder dem es sich um eine Rechtspflegerin oder einen Rechtspfleger handeln muss, zum Schutz der sachlichen Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger.

3.3.2.3
Akteneinsicht im Justizvollzug

Zur Verfolgung von Ansprüchen ist es oftmals notwendig, Einsicht in Akten zu erhalten. Dieses Recht gilt jedoch nicht uneingeschränkt. Im Justizvollzug scheitert die Durchsetzung in vielen Fällen an einer unvollständigen Begründung des Antrages.

Es haben sich Eingaben gehäuft, bei denen sich Inhaftierte bei mir beschwert haben, dass sie keine oder nur unzureichende Einsicht in ihre Akten bei der jeweiligen Justizvollzugsanstalt erhalten haben. Dies betraf zum einen die Einsicht in die Gefangenenpersonalakte, zum anderen auch die Einsicht in die Gesundheitsakten der inhaftierten Personen.

In der Gefangenenpersonalakte befinden sich personenbezogene Daten, die für und während der Durchführung des Strafvollzugs über den Gefangenen erhoben werden. Informationen über ärztliche Behandlungen und Daten über den Gesundheitsstatus werden in der Gesundheitsakte gespeichert.

Jeder Gefangene hat gem. § 64 S. 1 des Hessischen Strafvollzugsgesetzes (HStVollzG) i.V.m. § 18 Abs. 3 bis 6 HDSG das Recht auf Aktenauskunft oder, soweit dies zur Wahrnehmung rechtlicher Interessen erforderlich ist, auch Einsicht in seine Gefangenpersonalakte und seine Gesundheitsakte.

§ 64 HStVollzG

Die Betroffenen erhalten nach Maßgabe des § 18 Abs. 3 bis 6 des Hessischen Datenschutzgesetzes Auskunft oder, soweit dies zur Wahrnehmung rechtlicher Interessen erforderlich ist, Akteneinsicht hinsichtlich der zu ihrer Person gespeicherten Daten. Eine Pflicht zur Benachrichtigung nach § 18 Abs. 1 des Hessischen Datenschutzgesetzes besteht nicht.

In einem Einzelfall, den ich hier stellvertretend für einige andere erläutern will, begehrte ein Strafgefangener Einsicht in die Einweisungsdokumentation als Bestandteil der Gefangenenpersonalakte und entsprechende Kopien aus der Akte. Er gab als Begründung hierfür an, er verfolge zivilrechtliche Interessen und brauche zum Zwecke der Schadensabwendung genaue Informationen

über das sog. Einweisungsverfahren. Aus seinem Recht auf informationelle Selbstbestimmung erwachse auch ohne Begründung ein Recht auf vollständige Akteneinsicht.

Diesem Wunsch auf Akteneinsicht wurde jedoch seitens der Justizvollzugsanstalt nicht nachgekommen. Begründet wurde dies damit, das Einsichtsverlangen sei zu unbestimmt, ohne weitere Begründung könnten weder Einsicht in die Akten noch Kopien daraus gewährt werden.

Wer als Gefangener Einsicht in seine Akten haben möchte, muss die Gründe hierfür konkret bezeichnen. Es ist gem. § 64 HStVollzG erforderlich, dass dargelegt und begründet wird, dass der Betroffene zur Wahrnehmung der rechtlichen Interessen auf die Einsichtnahme in die Akte angewiesen ist. Zur Geltendmachung des Rechts sind die Teile bzw. Angaben näher zu bezeichnen, auf die es zur Wahrung der Rechte ankommt. Die pauschale Begründung, man müsse Einsicht in alle Akten zur Verfolgung von Ansprüchen bekommen, genügt nicht. Es ist genauer darzulegen, welche Ansprüche verfolgt und welche Aktenteile hierfür gebraucht werden. Ansonsten ist der Antrag zu unspezifisch und kann abgelehnt werden. Oftmals scheitert das Auskunftsbegehren an dieser formalen Hürde, da nur formelhaft „Akteneinsicht“ verlangt wird.

Ich habe dem Petenten geraten, seinen Antrag zu spezifizieren und genau darzulegen, welche Aktenbestandteile er zu welchem Zweck benötige. Im vorliegenden Fall hat der Strafgefangene sich jedoch geweigert, sein Anliegen gegenüber der Justizvollzugsanstalt zu spezifizieren. Deshalb hat diese den Antrag zu Recht abgelehnt.

Auch in einem anderen Fall kam ich zu dem Ergebnis, dass die Einsicht in die Gesundheitsakte des Gefangenen zu Recht verweigert wurde. Der Strafgefangene beantragte pauschal Einsicht in ca. 14 Aktenordner und eine dicke Krankenakte mit vielen verschiedenen Gutachten zu seinem Gesundheitszustand. Als Begründung führte er lediglich an, er brauche alle Unterlagen zur Verfolgung rechtlicher Schritte. Damit hat er aber nicht dargelegt, weshalb er über die Auskunftserteilung hinaus auf die Einsichtnahme in alle Aktenbestandteile angewiesen ist bzw. in welche Aktenteile die Einsicht erforderlich ist, um seine genauer bezeichneten rechtlichen Interessen wahrzunehmen. Nötig wäre also eine genauere Begründung und damit einhergehend eine Präzisierung der gewünschten Aktenbestandteile. Da der Strafgefangene dieses nicht wollte, wurde auch hier zu Recht ein Anspruch auf Akteneinsicht abgelehnt.

Mein Fazit ist, dass es in den meisten Fällen an genaueren Begründungen und Angaben über die gewünschten Aktenteile fehlt. Ich habe die Betroffenen darüber aufgeklärt, dass das Recht auf Akteneinsicht nicht uneingeschränkt besteht und auch hierfür bestimmte Voraussetzungen erfüllt sein müssen. Es ist auch nicht meine Aufgabe, anstelle des Gefangenen Einsicht in die kompletten Unterlagen zu nehmen und dann anstelle der Justizvollzugsanstalt die Auskunft zu erteilen.

3.3.2.4
OWi21 – Neue Komponenten

Die ekom21 GmbH hat für das Verfahren OWi21 neue Komponenten entwickelt. Es handelt sich um ein Programm für Smartphones zur Erfassung von Ordnungswidrigkeiten (OWi21ToGo) sowie die Möglichkeit einer Online-Anhörung zum Ausfüllen des Anhörungsbogens über das Internet. Während die Komponente OWi21ToGo von der hessischen Polizei bereits genutzt wird, müssen bei der Online-Anhörung noch Fragen geklärt werden.

3.3.2.4.1
OWi21 – Allgemein

Für die Abwicklung von Ordnungswidrigkeitenverfahren hat die ekom21 GmbH das Verfahren OWi21 entwickelt. Mit diesem Verfahren wird die Durchführung von Ordnungswidrigkeitenverfahren als Workflow unterstützt. Bei Überlegungen zu einer technischen Weiterentwicklung hat man zwei Bereiche ins Auge gefasst. Zum einen die Erfassung der Ordnungswidrigkeit vor Ort und zum anderen die Äußerung des Angeschriebenen.

3.3.2.4.2
OWi21ToGo

3.3.2.4.2.1
Das Konzept

Die Erfassung von Tatbeständen vor Ort – insbesondere im Bereich der Verkehrsordnungswidrigkeiten – wurde von den beteiligten Stellen als aufwändig bzw. zu teuer empfunden. Da Smartphones technisch betrachtet geeignet sind, die Beamten vor Ort zu unterstützen, und günstiger sind als Spezialgeräte, hat die hessische Polizei zusammen mit der ekom21 GmbH Überlegungen angestellt, wie ein sinnvoller, rechtlich zulässiger Einsatz von Smartphones aussehen kann. In diesen Prozess war ich eingebunden.

Das Konzept sieht vor, dass mit einem Smartphone Fotos gemacht werden und dann die weiteren Daten zu einer Ordnungswidrigkeit erfasst werden. Diese Daten werden über das Internet an einen Server übertragen, der von der ekom21 GmbH betrieben wird. Hierzu hat die ekom21 GmbH eine

App (s.u.) programmiert, mit der die rechtlich zulässigen Daten erfasst werden können. Die Herausforderung bestand darin, eine Lösung zu entwickeln, die eine ausreichende Datensicherheit gewährleistet.

3.3.2.4.2.2
Datensicherheit

Es gab drei Elemente, die betrachtet wurden: der Server, die Übertragung und das Smartphone selbst.

3.3.2.4.2.2.1
Der Server

Der Server wird analog zu den anderen Webangeboten der ekom21 GmbH in einer DMZ betrieben. Sobald die Daten an den Server übertragen sind, werden sie automatisch vom Server heruntergeladen und der Fachanwendung zur Verfügung gestellt. Ist dieser Download erfolgreich verlaufen, werden die Daten auf dem Server gelöscht.

3.3.2.4.2.2.2
Die Übertragung

Die Daten werden verschlüsselt übertragen. Dabei wird seitens des Servers geprüft, ob die Datei von einem zugelassenen Gerät stammt. Die eingesetzten Algorithmen erfüllen die aktuellen Anforderungen.

3.3.2.4.2.2.3
Das Smartphone

Ein Smartphone bietet sehr viel mehr technische Möglichkeiten, als zu dem vorgesehenen Zweck benötigt werden. Es galt daher neben organisatorischen Vorgaben auf zwei Gebieten technische Sicherungen einzubauen.

Dienstanweisung

Die Polizei hat eine Dienstanweisung erlassen, die den Umgang mit dem Gerät reglementiert. Eine private Nutzung ist untersagt, und es dürfen außer der installierten App keine weiteren Apps geladen werden. Diese Vorgabe wird auch technisch kontrolliert.

App und Daten

Die App wurde für das Betriebssystem Android programmiert. Die ekom21 GmbH garantiert dabei die Funktionsfähigkeit für bestimmte Endgeräte. Die App selbst hat eine Benutzerverwaltung, und man kann sie nur starten, wenn eine Benutzerkennung und ein Passwort eingegeben sind. Die Passwortvorgaben richten sich nach den üblichen Anforderungen aus den Grundschutzkatalogen des BSI.

App (engl. Abk. für Application Software)

Bezieht sich auf jegliche Art von Anwendungssoftware. Wird im deutschen Sprachraum meist mit Anwendungen für Smartphones und Tablet-Computer gleichgesetzt.

Sobald die Daten erfasst sind, werden sie übertragen und nach erfolgreicher Übertragung gelöscht. Das sollte in der Regel nach wenigen Sekunden geschehen sein. Falls jedoch keine Verbindung zum Server der ekom21 GmbH besteht, müssen die Daten zwischengespeichert werden. Dies erfolgt immer verschlüsselt. Sobald die Verbindung wieder hergestellt ist, erfolgt die Übertragung mit anschließender Löschung. Auf dem Smartphone sollten sich daher im Normalfall keine Daten befinden, auf die zugegriffen werden könnte.

Konfiguration

Wie ich bereits in meinem 41. Tätigkeitsbericht, Ziff. 2.3.1 und einer Handreichung dargelegt habe, muss die Dienststelle die Kontrolle über das Endgerät haben. Zu diesem Zweck wird ein Mobile Device Management (MDM) eingesetzt. Durch entsprechende Einträge im MDM wird erzwungen, dass nur bestimmte Apps installiert werden können. Außerdem werden restriktive Vorgaben zu Schnittstellen, zur Ortung und zu Gerätepasswörtern umgesetzt. Ganz wichtig ist aber, dass bei Verlust das Gerät aus der Ferne gelöscht werden kann.

3.3.2.4.2.2.4
Fazit

Unter diesen Voraussetzungen habe ich keine Vorbehalte gegen den Einsatz. Das gilt sowohl für den Einsatz durch die Polizei als auch durch kommunale Ordnungsbehörden.

3.3.2.4.3
Online-Anhörung

Mit der Online-Anhörung soll Bürgern die Möglichkeit eröffnet werden, ohne großen Aufwand über das Internet einen Anhörungsbogenbogen auszufüllen.

Auch hier befindet sich der Server wieder in einer DMZ. Alle Datenübertragungen erfolgen verschlüsselt.

Ein Bürger kann sich auf den Server unter Eingabe des Aktenzeichens anmelden. Sobald er den Fragebogen ausgefüllt hat und den Inhalt bestätigt, werden die Daten für die weitere Bearbeitung oder Einsicht gesperrt. Die Daten werden dann automatisch heruntergeladen, dem Fachverfahren zur Verfügung gestellt und auf dem Server gelöscht.

Die Abläufe sind – technisch betrachtet – klar strukturiert und bieten wenig Anlass zu Kritik, wenn die Datensicherheit des Servers gegeben ist.

Vor der Umsetzung sind allerdings noch rechtliche Rahmenbedingungen zu regeln. Eine Online-Anhörung ist grundsätzlich im Rahmen der elektronischen Aktenführung gem. § 110b OWiG möglich.

§ 110b OWiG

(1) Die Verfahrensakten können elektronisch geführt werden. Die Bundesregierung und die Landesregierungen bestimmen für ihren Bereich durch Rechtsverordnung den Zeitpunkt, von dem an die Akten elektronisch geführt werden oder im behördlichen Verfahren geführt werden können sowie die hierfür geltenden organisatorisch-technischen Rahmenbedingungen für die Bildung, Führung und Aufbewahrung der elektronisch geführten Akten. Die Bundesregierung und die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die zuständigen Bundes- oder Landesministerien übertragen. Die Zulassung der elektronischen Aktenführung kann auf einzelne Behörden, Gerichte oder Verfahren beschränkt werden.

(2) Zu den elektronisch geführten Akten eingereichte und für eine Übertragung geeignete Schriftstücke und Gegenstände des Augenscheins (Urschriften) sind zur Ersetzung der Urschrift in ein elektronisches Dokument zu übertragen, soweit die Rechtsverordnung nach Absatz 1 nichts anderes bestimmt. Das elektronische Dokument muss den Vermerk enthalten, wann und durch wen die Urschrift übertragen worden ist. Die Urschriften sind bis zum Abschluss des Verfahrens so aufzubewahren, dass sie auf Anforderung innerhalb von einer Woche vorgelegt werden können.

(3) Elektronische Dokumente, die nach Absatz 2 hergestellt wurden, sind für das Verfahren zugrunde zu legen, soweit kein Anlass besteht, an der Übereinstimmung mit der Urschrift zu zweifeln.

(4) Enthält das nach Absatz 2 hergestellte elektronische Dokument zusätzlich zu dem Vermerk nach Absatz 2 Satz 2 einen mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen Vermerk darüber,

1. dass die Wiedergabe auf dem Bildschirm mit der Urschrift inhaltlich und bildlich übereinstimmt sowie
2. ob die Urschrift bei der Übertragung als Original oder in Abschrift vorgelegen hat,

kann die Urschrift bereits vor Abschluss des Verfahrens vernichtet werden. Dies gilt nicht für in Verwahrung zu nehmende oder in anderer Weise sicherzustellende Urschriften, die als Beweismittel von Bedeutung sind oder der Einziehung oder dem Verfall unterliegen (§§ 22 bis 29a, 46 dieses Gesetzes in Verbindung mit §§ 94, 111b bis 111n der Strafprozessordnung). Verfahrensinterne Erklärungen des Betroffenen und Dritter sowie ihnen beigefügte einfache Abschriften können unter den Voraussetzungen von Satz 1 vernichtet werden. In der Rechtsverordnung nach Absatz 1 kann abweichend von den Sätzen 1 und 3 bestimmt werden, dass die Urschriften weiter aufzubewahren sind.

Details dazu sind in einer Rechtsverordnung festzulegen. Die derzeit gültige Verordnung über die elektronische Aktenführung bei Verwaltungsbehörden in Bußgeldverfahren vom 23. Juli 2010 (GVBl. I S. 254) regelt zwar grundsätzlich, dass die Bußgeldakten elektronisch geführt werden können und welcher technische Standard einzuhalten ist, wenn zwischen Verwaltungsbehörden und mit der Staatsanwaltschaft Akten auszutauschen sind. Es gibt jedoch noch keine Regelungen zur Ausgestaltung der elektronischen Einreichung von Dokumenten durch Betroffene.

Dabei ist auch § 110a OWiG zu berücksichtigen. Danach gilt grundsätzlich, dass Dokumente, die ausdrücklich schriftlich einzureichen sind, qualifiziert zu signieren oder in einem andern sicheren

Verfahren, das die Authentizität und die Integrität des übermittelten Dokuments sicherstellt, zu übertragen sind. Zwar gehört der Anhörungsbogen nicht zu den Dokumenten, für die das OWiG zwingend die schriftliche Einreichung verlangt. Dies ändert jedoch nichts daran, dass für diese neue Art der Kommunikation in Bußgeldverfahren technische Rahmenbedingungen zu definieren sind, vergleichbar der Möglichkeit des elektronischen Rechtsverkehrs mit den Gerichten.

Mir wurde zugesagt, dass ein Entwurf für eine entsprechende Rechtsverordnung vorgelegt wird. Derzeit ist er mir noch nicht bekannt.

3.3.3 Verfassungsschutz

3.3.3.1
Neuordnung der parlamentarischen Kontrolle des Verfassungsschutzes

Die Ereignisse um die Morde der rechtsextremistischen Terrorzelle NSU haben auch in Hessen zu ausführlichen Diskussionen über den Verfassungsschutz – insbesondere zur parlamentarischen Kontrolle – geführt. Zu einer umfassenden Neugestaltung der gesetzlichen Grundlagen ist es jedoch nicht gekommen.

Schon im vergangenen Jahr hatte der Landtag über mehrere Gesetzentwürfe zu beraten, die alle an die Diskussion der Ereignisse rund um die NSU-Morde anknüpften. Schwerpunkt dabei war u.a. die Verstärkung der parlamentarischen Kontrolle.

Beraten wurden gleichzeitig drei alternative Vorschläge:

– Gesetzentwurf der Fraktionen der CDU und der FDP für ein Gesetz über das Landesamt für Verfassungsschutz (LTDrucks. 18/6193):

  Dieser hatte im Wesentlichen nur die Arbeit der parlamentarischen Kontrollkommission zum Gegenstand.

– Dringlicher Gesetzentwurf der Fraktion der SPD für ein Gesetz zur Stärkung der Parlamentarischen Kontrolle gegenüber der Tätigkeit des Landesamtes für den Verfassungsschutz (LTDrucks. 18/5061):

  Dieser bestand aus einem Vorschlag mit Änderungen im Bereich der Befugnisse des Landes-

amtes für Verfassungsschutz sowie einem separaten Gesetz zur Arbeit der parlamentarischen Kontrollkommission.

– Gesetzentwurf der Fraktion DIE LINKE für ein Hessisches Gesetz zur Neuordnung der Aufgaben zum Schutz der Verfassung und zur Auflösung des Landesamtes für Verfassungsschutz (LTDrucks. 18/6179):

  Gegenstand dieses Gesetzentwurfs war, das Landesamt für Verfassungsschutz und damit verbunden auch die Informationsbeschaffung durch nachrichtendienstliche Mittel abzuschaffen. Anstelle dessen sollte eine neue Institution geschaffen werden, die schwerpunktmäßig der Dokumentation und Information über neonazistische und andere gegen die Grundsätze der Verfassung gerichtete Aktivitäten dienen sollte. Daneben sollte diese für die Aufgaben zuständig sein, die durch Vorgaben des Bundesverfassungsschutzgesetzes (BVerfSchG) zwingend durch die Länder wahrzunehmen sind.

Alle drei Entwürfe waren auch Gegenstand einer Anhörung im Innenausschuss des Landtages, an der ich teilgenommen habe.

Das Ziel der genannten Gesetzentwürfe - die Vorschriften zur Kontrolle der Tätigkeit des Landesamtes für Verfassungsschutz durch das Parlamentarische Kontrollgremium in Abwägung der notwendigen Vertraulichkeitsregelungen und des informationellen Selbstbestimmungsrecht der Betroffenen zu überarbeiten – trage ich mit. Dabei möchte ich insbesondere drei Aspekte hervorheben.

3.3.3.1.1
Zugang zu den erforderlichen Unterlagen – Wahrung der Vertraulichkeit

Eine sinnvolle Kontrolltätigkeit, die dem verfassungsrechtlichen Auftrag der parlamentarischen Kontrolle der Exekutive und der Stellung der Abgeordneten gerecht wird, setzt voraus, dass die Abgeordneten Zugang zu den Unterlagen bekommen, die aus ihrer Sicht zur Erfüllung ihres Kontrollauftrags erforderlich sind.

Datenschutzrechtliche Grundsätze stehen einer Regelung nicht entgegen, wonach dem Kontrollgremium auch Unterlagen direkt zur Verfügung gestellt werden und nicht nur eine Einsicht in den Räumen des Landesamtes erfolgen kann. Die Richtlinien für den Umgang mit Verschlusssachen des Hessischen Landtages sehen grundsätzlich schon Möglichkeiten zum Umgang mit sensiblen Unterlagen vor. Ausgehend von den dortigen Regelungen zur Behandlung von Angelegenheiten, die als „Streng geheim“ eingestuft sind, ist auch eine Geschäftsordnungsvorgabe für die Parlamen-

tarische Kontrollkommission möglich. Der Landesregierung muss allerdings die Möglichkeit verbleiben, in begründeten Fällen „nur“ ein Einsichtsrecht in den Räumen des Landesamtes zu gewähren.

Neben dem Schutz der Vertraulichkeit der Unterlagen ist selbstverständlich auch die Vertraulichkeit der Sitzungen sicherzustellen. Dazu ist es nicht nötig, die Nutzung jeglicher Geräte der Informationstechnik während der Sitzung zu untersagen. Bei allem Verständnis für ein Unbehagen bezogen auf die Abschöpfungsmöglichkeiten von Handys und ähnlichen Geräten halte ich es doch für zu weit gehend, jegliche Nutzung von elektronischen Geräten während der Sitzung zu untersagen, wie es der CDU/FDP-Entwurf vorsah. Sinnvoller erscheint es mir, für einen Sitzungsraum zu sorgen, der entsprechend technisch abhörsicher ausgestattet ist. Die Mehrheit des Landtages hat sich in diesem Punkt jedoch dem restriktiven Vorschlag des CDU/FDP-Entwurfes angeschlossen.

3.3.3.1.2
Dokumentation der Beratungen

Eine effektive Kontrolltätigkeit erfordert, dass der Gegenstand der Erörterung in der Parlamentarischen Kontrollkommission nachträglich eindeutig bestimmt werden kann und dass zu einem späteren Zeitpunkt die Möglichkeit besteht, zu prüfen, ob Konsequenzen aus der Beratung gezogen worden sind.

Die Frage, ob die Landesregierung ihre Unterrichtungspflicht im notwendigen Maße zum jeweiligen Zeitpunkt erfüllt hat, erfordert ein Protokoll, das mehr als die Benennung des Beratungsgegenstandes zum Inhalt hat, was der CDU/FDP-Entwurf vorsah.

Sollen sich die Mitglieder der Parlamentarischen Kontrollkommission ernsthaft mit ihrer Kontrollaufgabe auseinandersetzen, muss es ihnen zudem auch möglich sein, Notizen zum Gebrauch über die jeweilige Sitzung hinaus zu fertigen. Daher wäre es ein Eingriff in die freie Mandatsausübung der Abgeordneten, wenn Notizen zum Ende einer Sitzung eingesammelt und dann vernichtet würden.

Seit der Erfindung der Schrift ist es überholt, sich allein auf das Gedächtnis zu verlassen. Zur Wahrung der Vertraulichkeit der Beratungsgegenstände ist eine Regelung denkbar, wie sie für die Behandlung der Verschlusssachen gilt: Die Aufbewahrung im verschlossenen Umschlag und Zugang lediglich in den Räumen der für Verschlusssachen zuständigen Stelle des Landtages. So kann die Arbeit der Abgeordneten sinnvoll unterstützt werden und gleichzeitig die Vertraulichkeit solcher

Notizen gewahrt werden. Meinem Vorschlag zum Umgang mit solchen Notizen wurde dann letztlich auch gefolgt.

3.3.3.1.3
Fachliche Unterstützung

Dem parlamentarischen Kontrollgremium und auch den einzelnen Mitgliedern sollte zudem eine sachkundige Unterstützung möglich sein.

Für komplexere Fragestellungen ist die Unterstützung durch eigene Mitarbeiter nicht nur möglich, sondern geboten. Hierfür sollten Regelungen sowohl zu den Voraussetzungen als auch zur Sicherstellung der Vertraulichkeit für derartige Tätigkeiten geschaffen werden, wie es sie auf Bundesebene und in anderen Bundesländern gibt. Eine solche Regelung fand leider keine Mehrheit im Parlament.

Auch die Unterstützung durch Sachverständige halte ich grundsätzlich für zulässig. Es versteht sich von selbst, dass die Anforderungen an die Vertraulichkeit auch in diesem Zusammenhang zu wahren sind. Folglich bedarf es einer Regelung, welche Informationen Sachverständigen zugänglich sind, wie die Informationen zugänglich gemacht werden, in welcher Form der Sachverständigenbericht abzufassen ist und schließlich wie die Parlamentarische Kontrollkommission bzw. ihre Mitglieder mit dem vorgelegten Bericht umzugehen haben. Die dazu nunmehr realisierte Regelung bleibt in ihrem Gehalt leider deutlich dahinter zurück.

Begrüßt habe ich, dass schon in den Entwürfen vorgesehen war, dem Kontrollgremium die Möglichkeit zu eröffnen, auch den Hessischen Datenschutzbeauftragten um Stellungnahmen zu bitten. Die nunmehr gefundene Regelung ist allerdings nicht sehr konkret.

3.3.3.1.4
Ergebnis der parlamentarischen Beratung

Da das Gesetz in der vorherigen Fassung bis zum 31. Dezember 2012 befristet war, bestand die Notwendigkeit, rechtzeitig eine Novellierung zu beschließen. Daher blieb die Diskussion über eine Neuausrichtung der Arbeit des Verfassungsschutzes insgesamt im Wesentlichen aus. Es wurden zu den genannten Punkten durch die Mehrheit des Landtages auch nur wenige Änderungen vorgenommen. Das Gesetz zur Änderung des Gesetzes über das Landesamt für Verfassungsschutz wurde am 12. Dezember 2012 (GVBl. 2012 S. 578 bis 580) verkündet. Neben den Ergänzungen

zur Tätigkeit der Parlamentarischen Kontrollkommission gab es Änderungen durch eine Neustrukturierung der Befugnisse des Landesamtes für Verfassungsschutz zu den besonderen Auskunftsersuchen.

3.3.3.1.5
Erneutes Novellierungsvorhaben

Im laufenden Jahr wurde durch die SPD-Fraktion ein weiterer Gesetzentwurf zur Neuausrichtung des Verfassungsschutzes in Hessen und zur Stärkung der parlamentarischen Kontrolle (LTDrucks. 18/7352) eingebracht. Zielsetzung dieses Gesetzentwurfs war erneut zum einen eine Erweiterung der Befugnisse der Kontrollkommission ergänzt um die Möglichkeit für die Kommissionsmitglieder, sich durch Zuarbeit von Beschäftigten unterstützen zu lassen. Zum anderen sollten bestimmte Sachverhalte auch parlamentsöffentlich diskutiert werden können. Gleichzeitig sollten die Aufgaben und Arbeitsweisen des Landesamtes für Verfassungsschutz neu strukturiert werden. Die Kritik aus dem vorangegangenen Gesetzgebungsverfahren war in diesem Entwurf größtenteils berücksichtigt worden.

Ausdrücklich zu begrüßen in diesem Zusammenhang war das Anliegen, im Gesetz die Anwendungsmöglichkeiten für nachrichtendienstliche Mittel näher zu präzisieren. Darüber hinaus sollten im Interesse der Zusammenarbeit mit den Verfassungsschutzbehörden des Bundes und der Länder auch die Regelungen zum Informationsaustausch konkretisiert werden.

Zu diesem Gesetzentwurf fand zwar ebenfalls eine Anhörung durch den Innenausschuss statt. Eine Auswertung dieser Anhörung und eine Entscheidung des Parlaments hat es in der abgelaufenen Legislatur jedoch nicht mehr gegeben.

3.3.4 Ausländerwesen

3.3.4.1
Ausschreibung im Schengener Informationssystem zur Einreiseverweigerung und Befristung der Wirkung der Ausweisung

Eine nach deutschem Recht unbefristete Ausweisungsverfügung steht der Löschung einer Ausschreibung im Schengener Informationssystem entgegen. Nach neuer Rechtsprechung hat jedoch

ein Ausländer oder eine Ausländerin aus einem Drittstaat einen grundsätzlichen Anspruch auf eine Befristung der Sperrwirkung, was sich auf die Dauer dieser Ausschreibung auswirkt.

3.3.4.1.1
Sachverhalt

Ein Drittausländer wurde durch die Ausländerbehörde eines hessischen Landkreises im Jahr 1994 aufgrund besonderer Gefährlichkeit ausgewiesen und abgeschoben. Seitdem reiste er erneut mehrfach illegal in das Bundesgebiet ein und beging während dieser Zeit erneut Straftaten. 2010 wurde er letztmalig abgeschoben. Zudem erfolgte eine Ausschreibung im Schengener Informationssystem (SIS). Der Betroffene hat im April 2013 die nachträgliche Befristung der Wirkung der Abschiebung beantragt.

Die Ausländerbehörde teilte auf Nachfrage mit, dass regelmäßig geprüft werde, ob die SIS-Ausschreibung des Ausländers gelöscht werden könne. Bisher habe sie jedoch an der SIS-Ausschreibung festhalten müssen, da die Wirkung der Ausweisung noch nicht befristet wurde. Der betroffene Drittausländer wandte sich an mich, da nach seiner Auffassung eine Verlängerung der SIS-Ausschreibung nicht rechtmäßig sei.

3.3.4.1.2
Rechtliche Beurteilung

Gemäß § 11 Abs. 1 Satz 1 AufenthG darf ein Ausländer, der ausgewiesen, zurückgeschoben oder abgeschoben worden ist, nicht erneut in das Bundesgebiet einreisen und sich darin aufhalten (gesetzliche Sperrwirkung). Zugleich führt der Vollzug dieser Maßnahmen i.d.R. dazu, dass der Ausländer im SIS gem. Art. 24 Abs. 3 der Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) zur Einreiseverweigerung ausgeschrieben wird mit der Folge, dass dieses Einreiseverbot für das gesamte Schengen-Gebiet gilt.

Art. 24 Abs. 1 und 3 SIS II-Verordnung

(1) Die Daten zu Drittstaatsangehörigen, die zur Einreise oder Aufenthaltsverweigerung ausgeschrieben sind, werden aufgrund einer nationalen Ausschreibung eingegeben, die auf einer Entscheidung der zuständigen Verwaltungsbehörden oder Gerichte beruht, wobei die Verfahrensregeln des nationalen Rechts zu beachten sind; diese Entscheidung darf nur auf der Grundlage einer

individuellen Bewertung ergehen. Rechtsbehelfe gegen diese Entscheidungen richten sich nach den nationalen Rechtsvorschriften.

(3) Eine Ausschreibung kann auch eingegeben werden, wenn die Entscheidung nach Absatz 1 darauf beruht, dass der Drittstaatsangehörige ausgewiesen, zurückgewiesen oder abgeschoben worden ist, wobei die Maßnahme nicht aufgehoben oder ausgesetzt worden sein darf, ein Verbot der Einreise oder gegebenenfalls ein Verbot des Aufenthalts enthalten oder davon begleitet sein muss und auf der Nichtbeachtung der nationalen Rechtsvorschriften über die Einreise oder den Aufenthalt von Drittstaatsangehörigen beruhen muss.

Die gesetzliche Sperrwirkung, d.h. das unbefristete Einreise- und Aufenthaltsverbot des § 11 Abs. 1 AufenthG, trat bei dem betroffenen Drittstaatsangehörigen ein, da die Abschiebung tatsächlich vollzogen worden war. Der Vollzug hat zudem bewirkt, dass er im SIS zur Einreiseverweigerung ausgeschrieben wurde. Artikel 29 der SIS II-Verordnung regelt, wie lange eine Ausschreibung im SIS erfolgt.

Artikel 29 Abs. 1, 2 und 4 SIS II-Verordnung

(1) Die gemäß dieser Verordnung in das SIS II eingegebenen Ausschreibungen werden nicht länger als für den verfolgten Zweck erforderlich gespeichert.

(2) Der ausschreibende Mitgliedstaat prüft innerhalb von drei Jahren nach Eingabe einer solchen Ausschreibung in das SIS II die Erforderlichkeit der weiteren Speicherung.

(4) Innerhalb der Prüffrist kann der ausschreibende Mitgliedstaat nach einer umfassenden individuellen Bewertung, die zu protokollieren ist, beschließen, die Ausschreibung noch beizubehalten, wenn dies für den der Ausschreibung zugrunde liegenden Zweck erforderlich ist. In diesem Fall gilt Abs. 2 auch für die Verlängerung.

Nach geltender Rechtslage ist also alle drei Jahre zu prüfen, ob die Ausschreibung noch erforderlich ist. Solange jedoch die Sperrwirkung des § 11 Abs. 1 AufenthG besteht, ist die Ausschreibung noch als erforderlich im Sinne des Artikels 29 Abs. 1, 2 und 4 der SIS II-Verordnung anzusehen. Die in dieser Vorschrift genannten Überprüfungsfristen haben keinen Einfluss auf die Sperrwirkung des § 11 Abs. 1 AufenthG. Vielmehr richtet sich die Dauer der SIS-Ausschreibung danach, wie lange die Sperrwirkung besteht.

Daher ist zunächst die Sperrwirkung zu befristen, wenn sich der Betroffene gegen die fortgesetzte SIS-Ausschreibung wenden möchte. Eine solche Befristung ermöglicht ihm § 11 Abs. 1 Satz 3 AufenthG.

§ 11 Abs. 1 Satz 1 bis 3 AufenthG

Ein Ausländer, der ausgewiesen, zurückgeschoben oder abgeschoben worden ist, darf nicht erneut in das Bundesgebiet einreisen und sich darin aufhalten. Ihm wird auch bei Vorliegen der Voraussetzungen eines Anspruchs nach diesem Gesetz kein Aufenthaltstitel erteilt. Die in den Sätzen 1 und 2 bezeichneten Wirkungen werden auf Antrag befristet.

Der Drittausländer hat vorliegend einen solchen Antrag auf Befristung der Wirkungen der Ausweisung gestellt, über den allerdings noch nicht entschieden wurde.

In der Zukunft könnte sich an der dargestellten Rechtslage etwas ändern durch eine Entscheidung des Bundesverwaltungsgerichts aus dem Jahr 2012 (BVerwG, 1C 19/11, NVwZ 2013, 365). Das höchste Verwaltungsgericht hat entschieden, dass Ausländer grundsätzlich einen Anspruch darauf haben, dass die Ausländerbehörde mit der Ausweisung zugleich die Sperrwirkung, also das daran geknüpfte Einreise- und Aufenthaltsverbot, befristet. Bei der Bemessung der Frist sollen zukünftig die individuellen Umstände des Einzelfalls maßgebend sein. Eine von vorneherein befristete Ausweisungsverfügung hat dann auch Auswirkungen auf die Dauer der SIS-Ausschreibung.

3.3.4.2
Einverständniserklärung im Einbürgerungsverfahren – Anforderungen an Verständlichkeit und Vollständigkeit

Die Einverständniserklärung von Personen, die sich um eine Einbürgerung bewerben, mit der die Einbürgerungsbehörde Informationen bei öffentlichen Leistungsträgern (z.B. Jobcentern) einholt, muss für Betroffene verständlich sein und sie vollständig über den Zweck und den Umfang der Datenerhebung unterrichten.

Im Rahmen des Einbürgerungsverfahrens holen die Regierungspräsidien als zuständige Einbürgerungsbehörden eine Reihe von Informationen über Personen, die sich um die Einbürgerung bewerben, bei verschiedenen öffentlichen Stellen ein. Rechtsgrundlage hierfür sind die nach unterschiedlichen Arten der Einbürgerung differenzierenden Vorschriften des Staatsangehörigkeitsgesetzes (StAG). Regelmäßig ist auch die Auskunft über die finanzielle Situation einer Person, die sich um die Einbürgerung bewirbt, vorgesehen:

§ 10 Abs. 1 Nr. 3 StAG

Ein Ausländer, der seit acht Jahren rechtmäßig seinen gewöhnlichen Aufenthalt im Inland hat und handlungsfähig nach Maßgabe des § 80 des Aufenthaltsgesetzes oder gesetzlich vertreten ist, ist auf Antrag einzubürgern, wenn er

...

3. den Lebensunterhalt für sich und seine unterhaltsberechtigten Familienangehörigen ohne Inanspruchnahme von Leistungen nach dem Zweiten oder Zwölften Buch Sozialgesetzbuch bestreiten kann oder deren Inanspruchnahme nicht zu vertreten hat.

Daraus folgt, dass die Person, die sich um die Einbürgerung bewirbt, in bestimmten Fällen einen Nachweis zu erbringen hat, dass sie unverschuldet öffentliche Leistungen empfängt. In der Praxis sieht das Verfahren so aus, dass die Person schriftlich ihr Einverständnis erklärt, dass die Einbürgerungsbehörde Auskünfte beim zuständigen Leistungsträger einholen kann.

Für diese Einverständniserklärung haben die Behörden ein Formular verwendet, das von Einbürgerungswilligen auszufüllen war.

Die Formulierung dieser Erklärung wurde von einigen Leistungsträgern kritisiert. Das Regierungspräsidium Darmstadt bat insofern um meine Einschätzung. Eine Übermittlung von Sozialdaten bestimmt sich nach § 35 Abs. 2 SGB I i.V.m. § 67b SGB X.

§ 35 Abs. 2 SGB I

Eine Erhebung, Verarbeitung und Nutzung von Sozialdaten ist nur unter den Voraussetzungen des Zweiten Kapitels des Zehnten Buches zulässig.

§ 67b SGB X

(1) Die Verarbeitung von Sozialdaten und deren Nutzung sind nur zulässig, soweit die nachfolgenden Vorschriften oder eine andere Rechtsvorschrift in diesem Gesetzbuch es erlauben oder anordnen oder soweit der Betroffene eingewilligt hat.

(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der vorgesehenen Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf dessen freier Entscheidung beruht.

Die Einwilligung und der Hinweis bedürfen der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Nach ihrem Wortlaut beinhaltete die von den Behörden verwandte Einverständniserklärung lediglich, dass zur Prüfung der wirtschaftlichen Voraussetzungen Auskünfte über den Bezug von Leistungen nach dem SGB II bei der Agentur für Arbeit bzw. den für die Leistungserteilung zuständigen kommunalen Trägern eingeholt werden.

Für Personen, die sich um die Einbürgerung bewerben, ist aus dieser vorformulierten Einverständniserklärung nicht ersichtlich, dass mit den erhobenen Informationen geklärt werden soll, ob sie die Hilfebedürftigkeit zu vertreten haben (Klärung der Verschuldensfrage). Daher ist eine Datenübermittlung nicht von der Einverständniserklärung gedeckt.

Die Regierungspräsidien haben daher den Vordruck für die Einverständniserklärung überarbeitet. Aus dem neuen Formular geht ausdrücklich hervor, dass die Informationen bei den Leistungsträgern zur Klärung der Verschuldensfrage erhoben werden. Zusätzlich wird Personen, die sich um die Einbürgerung bewerben, die Möglichkeit gegeben, den Fragebogen, den die Einbürgerungsbehörde an den Leistungsträger übersendet, vor Unterzeichnung der Einverständniserklärung einzusehen.

3.3.4.3
Übermittlung von Lichtbildern durch Ausländerbehörden an Bußgeldstellen

Die Zulässigkeit der Übermittlung von Lichtbildern bzw. Ablichtungen von Ausweisdokumenten durch Ausländerbehörden an Bußgeldstellen kann nicht generell, sondern nur im Einzelfall beurteilt werden.

Verkehrsordnungswidrigkeiten werden in vielen Fällen durch stationäre Rotlichtüberwachungen bzw. Radarmessgeräte festgestellt, wobei ein Lichtbild des Fahrers oder der Fahrerin erzeugt wird. Sofern sich Betroffene im Bußgeldverfahren nicht zur Sache einlassen oder die Tat bestreiten, kann die Feststellung der Identität des Fahrer bzw. der Fahrerin durch einen Lichtbildabgleich erfolgen. Dazu fordert die Bußgeldstelle eine Ablichtung des Personalausweises oder Passes von den zuständigen Behörden an. Während für deutsche Staatsbürger das Passgesetz bzw. Personalausweisgesetz eindeutige Übermittlungsvorschriften für diese Fälle bereit hält, stellt sich die Situation für ausländische Staatsangehörige komplizierter dar. Die Ausländerbehörde einer hessi-

schen Stadt trat an mich heran, um die einschlägigen Rechtsgrundlagen für die Übermittlung von Ausweisdokumenten zu erörtern.

Im konkreten Fall bat eine Bußgeldstelle in Baden-Württemberg die Ausländerbehörde um Übersendung eines Lichtbildes des Vaters des ermittelten Halters. Die Bußgeldstelle verwies als Rechtsgrundlage auf die Vorschriften der §§ 161 Abs. 1 StPO i.V.m. § 46 Abs. 1 OWiG.

§ 46 Abs. 1 OWiG

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.

§ 161 Abs. 1 S. 1 StPO

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

Das in diesen Vorschriften verankerte Auskunftsrecht der Bußgeldstellen steht der eingeschränkten Befugnis zur Übermittlung personenbezogener Daten der Ausländerbehörde, bei der Lichtbilder hinterlegt sind, entgegen. Eine Übermittlungsbefugnis bzw. -verpflichtung kann zwar nicht auf bereichsspezifische Übermittlungsregelungen des Aufenthaltsgesetzes (§§ 90 ff.) gestützt werden, da sie nicht einschlägig sind. Herangezogen werden können aber die allgemeinen Datenübermittlungsvorschriften nach §§ 11 ff. HDSG. Nach § 13 Abs. 2 i.V.m. § 12 Abs. 2 Nr. 4 HDSG können Daten (Lichtbilder) unter Änderung des Zwecks der ursprünglichen Datenerhebung verarbeitet (übermittelt) werden, wenn sich bei der übermittelnden Behörde Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben.

§ 13 Abs. 2 HDSG

Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.

§ 12 Abs. 2 Nr. 4 HDSG

Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn
...
4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
...

Die Ausländerbehörde als übermittelnde Stelle hat dabei gemäß § 14 HDSG die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Bei Rotlichtverstößen oder Geschwindigkeitsüberschreitungen ist die Bußgeldstelle zumeist nur durch einen Lichtbildabgleich in der Lage, den Täter zu identifizieren, sodass die Schlüssigkeit zu bejahen ist. Bei dem bloßen Hinweis auf das Vorliegen einer nicht näher bezeichneten Ordnungswidrigkeit kann die Ausländerbehörde die Schlüssigkeit der Datenübermittlung jedoch nicht überprüfen. Gleiches gilt für das Anfordern von Lichtbildern von Personen, die nicht mit dem Halter übereinstimmen. Sofern nicht nachvollziehbar ist, weshalb ein Lichtbild angefordert wird, verbietet sich eine Datenübermittlung. Hier muss die Ausländerbehörde zunächst weitere Informationen einholen. So muss sie zum Beispiel klären, um welche Ordnungswidrigkeit es sich handelt oder in welchem Verhältnis eine Person, die an der Ordnungswidrigkeit nicht unmittelbar beteiligt ist, deren Lichtbild aber angefordert wird, zu dem Täter steht. Erst durch eine Überprüfung der Einzelfallumstände kann die Zulässigkeit der Datenübermittlung beurteilt werden.

3.3.5 Schulen, Schulverwaltung, Hochschulen

3.3.5.1
Online-Bewerbungsverfahren für Wohnraum des Studentenwerks Darmstadt

Bislang wurde das Verfahren, mit dem sich an den Universitäten und Hochschulen in Darmstadt Studierende für vom Studentenwerk Darmstadt zu vermietenden Wohnraum bewerben konnten, in Papierform abgewickelt. Im Berichtsjahr wurde dieses Verfahren durch ein Online-Verfahren ersetzt. Bei der datenschutzgerechten Gestaltung des Verfahrens habe ich das Studentenwerk beraten.

3.3.5.1.1
Funktion des Verfahrens

Das Studentenwerk in Darmstadt verwaltet und vermietet einen umfangreichen Bestand an Wohnungen und Zimmern für die an den Universitäten und Hochschulen in Darmstadt Studierenden. Potenzielle Interessenten für eine Wohnung oder ein Zimmer können auf der Internetseite des Studentenwerks eine Seite aufrufen, die zu einem Online-Bewerbungsportal führt. Dort ist ein Aufnahmeantrag hinterlegt, welcher von der Bewerberin oder dem Bewerber ausgefüllt und abgeschickt werden muss. Der Online-Antrag wird auf einem vom Studentenwerk betriebenen Web-Server abgelegt. Erfolgt die Bewerbung nicht korrekt, erhält der bzw. die Betroffene einen Hinweis und hat die Möglichkeit, den Antrag erneut auszufüllen oder zu korrigieren. Ist der Antrag korrekt ausgefüllt, erhält der Bewerber bzw. die Bewerberin automatisch eine E-Mail zugesandt, welche er bzw. sie über einen Link bestätigen muss. Wird die E-Mail nicht bestätigt, so wird die Bewerbung nicht aktiv. Im anderen Fall wird die E-Mail-Adresse aktiviert und die Bewerbung mit den im Online-Antrag hinterlegten Daten vom Web-Server auf einen Datenbankserver des Studentenwerks übernommen. Alle auf dem Datenbankserver hinterlegten Bewerberanträge werden von den hierfür zuständigen Beschäftigten des Studentenwerks abgerufen, um eine Überprüfung der Bewerbung auf Vollständigkeit und inhaltlicher Plausibilität durchzuführen. Ergibt diese, dass die Bewerbung durch die Sachbearbeitung inhaltlich nicht weiter bearbeitet werden kann, so erfolgt zum einen eine Absage an den Bewerber bzw. die Bewerberin, zum anderen die Löschung der Bewerbung aus dem System, denn der Antrag ist ggf. neu oder in korrigierter Form zu stellen und wird dann neu eingespeist. Erfolgt die Übernahme der Bewerbung, so wird diese in eine Warteschlange weitergeleitet, welche alle vorgeprüften Bewerbungen in einem Rhythmus von 15 Minuten zu einem zweiten Server überträgt. Aus diesem werden die Daten entnommen und die gewünschte Wohnung mit dem bestehenden Angebot abgeglichen.

Systemseitig werden der Antragssachbearbeitung alle freien Wohnobjekte angezeigt. In einem weiteren Lauf wird deren Verfügbarkeit überprüft. Danach werden die Bewerbergruppen den von diesen nachgefragten Objekten zugeordnet. Im Anschluss daran wird eine Sortierung nach dem zeitlichen Eingang der Bewerbung vorgenommen. Dem Bewerber bzw. der Bewerberin wird im weiteren Verfahrensablauf eine E-Mail mit einem Mietvertragsangebot übermittelt. Der oder die Betroffene bestätigt das Mietvertragsangebot durch die Überweisung der Kaution. Wird der Mietvertrag nicht bestätigt, geht die Bewerbung zurück in die Bewerbergruppe und wird zunächst an den letzten Platz gesetzt, um zu einem späteren Zeitpunkt erneut bearbeitet zu werden.

3.3.5.1.2
Technische Verarbeitung und Sicherheitsmaßnahmen

Ursprünglich wollte das Studentenwerk Darmstadt einen externen Dienstleister im Wege einer Auftragsdatenverarbeitung nach § 4 HDSG mit der technischen Gestaltung und Abwicklung des Verfahrens betrauen. Schließlich entschied man sich aber für eine interne Lösung. Die Webseite für die Online-Bewerbung liegt jetzt auf einem Webserver im Serverraum des Studentenwerks Darmstadt. Der Server ist durch eine Firewall gesichert. Der Zugriff von außen ist nur auf einen bestimmten Port (https) erlaubt. Das hat zur Konsequenz, dass ausschließlich eine verschlüsselte Kommunikation zwischen Bewerber bzw. Bewerberin und dem Studentenwerk stattfindet. Hierfür wird ein Domänen-Zertifikat der Firma Globalsign mit 2048 Bit verwendet. Der Datenbankserver, auf den die Bewerberdaten übernommen werden, ist durch zwei Firewalls gesichert.

3.3.5.1.3
Datenschutzrechtliche Problempunkte

Das Studentenwerk hatte mich bei der Entwicklung des Online-Verfahrens um Beratung gebeten. Erste Fragestellungen betrafen die inhaltlichen Daten, welche die Bewerber in dem Online-Fragebogen eintragen sollten. Richtig ist, dass die zuständigen Stellen des Studentenwerks alle Daten an die Hand bekommen sollen, die benötigt werden, um das Vergabeverfahren nach den tatsächlichen Bedürfnissen der Studierenden ausgerichtet zu steuern. Fragen nach der gewünschten Wohnform, der Hochschule, der Mietobergrenze oder den klassischen Personendaten wie Name, Vorname, Geschlecht, Familienstand, Anzahl der Kinder oder Telefonnummer sind da selbstverständlich. Allerdings gab es in der Bewerber-Warteschlange, also nach Annahme des Antrags, einen Vorgang, bei dem die Sachbearbeiter eine „Prüfung der Bewerber auf Gründe für eine besondere Aufnahme (Behinderung)“ vornehmen sollten. Dabei handelt es sich um ein Datum nach § 7 Abs. 4 HDSG.

§ 7 Abs. 4 HDSG

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

Bei derartigen Daten handelt es sich nachvollziehbar um besonders sensible Personendaten, deren Verarbeitung grundsätzlich untersagt ist, soweit nicht eine Rechtsvorschrift dies vorsieht oder aber zwingend voraussetzt. Eine derartige Fallkonstellation ist jedoch offensichtlich nicht gegeben. Das Studentenwerk hat in der Folge auf die Erhebung derartiger Merkmale verzichtet.

Wesentliche Punkte zum technischen und organisatorischen Datenschutz nach § 10 Abs. 2 HDSG waren nicht oder nicht hinreichend beschrieben.

§ 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).

Informationen über die Zutritts-, Benutzer-, Zugriffs-, Datenverarbeitungs-, Verantwortlichkeits- und Auftragskontrolle mussten vom Studentenwerk konkretisiert werden. Danach wurde deutlich, dass der Zutritt zum Serverraum reglementiert und bis auf einige wenige Funktionsträger beschränkt ist.

Die konkretisierten Angaben zur Benutzerkontrolle machten deutlich, dass mit Benutzer-ID und einem achtstelligen Passwort (Groß-/Kleinbuchstabe, Zahl und Sonderzeichen) drei von vier möglichen Kriterien nach dem BSI-Standard entsprochen war.

In punkto Rollenkonzept lieferte die IT-Abteilung des Studentenwerks eine dezidierte Beschreibung der Vergabe von Rechten an einzelne Funktionsträger. Damit ist sichergestellt, dass nur Personen entsprechend ihrer Funktion lesenden, schreibenden oder gar Zugriffe erhalten, die ein Verändern der Daten oder deren Löschung ermöglichen.

Schließlich musste das Thema Löschung der personenbezogenen Daten eingehend erörtert werden.

§ 19 Abs. 3 HDSG

Personenbezogene Daten sind unverzüglich zu löschen, sobald feststeht, daß ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 weiterverarbeitet werden dürfen. Wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer auf Grund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht. Satz 1 findet keine Anwendung, wenn Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Da eine bereichsspezifische Regelung für die Löschung der personenbezogenen Daten fehlt, muss sich die Daten verarbeitende Stelle an den hierzu im HDSG getroffenen festgelegten Maßstäben orientieren. Die Löschung der Personendaten hat nach § 19 Abs. 3 HDSG unverzüglich zu erfolgen, soweit diese zur Aufgabenerfüllung des Datenverarbeiters nicht mehr erforderlich sind. In das Löschkonzept des Studentenwerks wurde mit meiner Hilfe ein abgestuftes Verfahren implementiert, welches sowohl den Belangen der Bewerber selbst als auch denen des Studentenwerks

Rechnung trägt. Die Daten auf dem Webserver, also das ausgefüllte Online-Formular, werden nach der E-Mail-Bestätigung des Bewerbers gelöscht. Die Daten, die auf den Datenbankserver übertragen wurden (vollständig und korrekt ausgefüllte Bewerbung), werden nach Ablauf von sechs Monaten gelöscht, wenn kein Mietvertrag zustande kommt. Daten der Mieter, die auf dem Datenbankserver hinterlegt sind, werden nach dem Ablauf von 36 Monaten nach Beendigung des Mietverhältnisses gelöscht.

3.3.5.1.4
Fazit

Für das Online-Bewerbungsverfahren des Studentenwerks Darmstadt konnte eine allgemein akzeptierte und datenschutzgerechte Verfahrensweise erarbeitet werden. Hilfreich war vor allem, dass der Betreiber des Verfahrens vor der Inbetriebnahme des Systems den Kontakt zu den zuständigen Mitarbeiterinnen und Mitarbeitern meines Hauses gesucht hat. Dadurch war es möglich, datenschutzrechtliche Disparitäten im Vorfeld zu erkennen, zu diskutieren und im Nachgang die Schwachstellen zu beseitigen.

3.3.5.2
Videoüberwachung an Schulen bleibt ein Dauerthema

Das Thema Videoüberwachung an Schulen hat sich zu einem Dauerbrenner entwickelt. Auch im abgelaufenen Berichtsjahr ist es zu einer nicht unerheblichen Anzahl von Anfragen gekommen. Breiten Raum nahm die Diskussion um die Überwachung an Schulen im Landkreis Hersfeld-Rotenburg ein.

Der Einsatz von Videokameras ist nichts anderes als eine automatisierte Form der Verarbeitung personenbezogener (Bild)-Daten. Eine spezifische rechtliche Grundlage für deren Einsatz in Schulen etwa im Schulgesetz oder in den einschlägigen Verordnungen zur Datenverarbeitung in Schulen gibt es nicht. Auch das Hessische Datenschutzgesetz hilft in diesem Fall nicht weiter. So bleibt bis auf Weiteres einzig das Hessische Gesetz über die Sicherheit und Ordnung (HSOG) vom 14. Januar 2005 (GVBl. I S. 14), um hilfsweise den Betrieb einer Überwachungsanlage in Schulen rechtfertigen zu können.

§ 14 Abs. 1, 3 und 4 HSOG

(1) Die Polizeibehörden können personenbezogene Daten auch über andere als die in den §§ 6 und 7 genannten Personen bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass bei oder im Zusammenhang mit der Veranstaltung oder Ansammlung Straftaten oder nicht geringfügige Ordnungswidrigkeiten drohen. Die Unterlagen sind spätestens zwei Monate nach Beendigung der Veranstaltung oder Ansammlung zu vernichten, soweit sie nicht zur Abwehr einer Gefahr, zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden. Eine Verarbeitung für andere Zwecke ist unzulässig. § 20 Abs. 7 bleibt unberührt.

(3) Die Polizeibehörden können zur Abwehr einer Gefahr oder wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, öffentlich zugängliche Orte mittels Bildübertragung offen beobachten und aufzeichnen. Der Umstand der Überwachung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Fest installierte Anlagen dürfen unabhängig davon, ob die Voraussetzungen für ihre Errichtung nach Satz 1 noch vorliegen, zwei Jahre lang betrieben werden; die Frist verlängert sich entsprechend, wenn die Voraussetzungen weiterhin vorliegen. Abs. 1 Satz 2 und 3 sowie 15 des Hessischen Datenschutzgesetzes gelten entsprechend.

(4) Die Gefahrenabwehrbehörden können mittels Bildübertragung offen beobachten und aufzeichnen

1. zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,

2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,

3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.

Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechts. Abs. 1 Satz 2 und 3, Abs. 3 Satz 2 und 3 sowie § 15 Hessisches Datenschutzgesetz gelten entsprechend.

3.3.5.2.1
Videoüberwachung an Schulen im Landkreis-Hersfeld-Rotenburg

Bereits im Zusammenhang mit der Vorstellung meines 41. Tätigkeitsberichts im Frühjahr vergangenen Jahres hatte das Thema Videoüberwachung an Schulen breiten Raum eingenommen, obwohl ich keine Einzelfälle geschildert, sondern nur unter der Ziff. 3.3.3.3 ausführliche Erläuterun-

gen zu den rechtlichen Rahmenbedingungen für derartige Maßnahmen abgegeben hatte. Zu diesem Zeitpunkt hatte mich gerade die Anfrage der Ersten Kreisbeigeordneten und Schuldezernentin des Landkreises Hersfeld-Rotenburg hinsichtlich der datenschutzrechtlichen Zulässigkeit des Einsatzes von Videotechnik an fünf Schulen erreicht, die eine umfangreiche Diskussion auslöste, an der sich auch Presse, Rundfunk und Fernsehen intensiv beteiligten.

3.3.5.2.1.1
Umfang der an den Schulen eingesetzten Videotechnik

Die auf die Anfrage hin eingeleiteten Recherchen meines Mitarbeiters förderten Erstaunliches zu Tage. Von den 49 Schulen im Landkreis Hersfeld-Rotenburg waren an fünf Schulen Kameras installiert. Bemerkenswert war dabei nicht nur der Umstand, dass es sich um vermeintlich kleine und überschaubare Einrichtungen, wie z.B. eine Grundschule mit 160 Kindern, handelte. Gleichermaßen auffällig war die unterschiedliche Ausgestaltung hinsichtlich der Anzahl der installierten Kameras sowie der überwachten Räume und Eingänge bzw. des Außengeländes.

3.3.5.2.1.1.1
Gesamtschule Schenklengsfeld

In der Gesamtschule Schenklengsfeld mit ihren 500 Schülerinnen und Schülern sind seit dem Jahr 2010 etwa 22 Kameras installiert, welche die Eingangstüren sowie die ebenerdigen Fensterfronten (mit Ausnahme des Lehrerzimmers) überwachen. Im Innenbereich werden alle Flure in beiden Etagen (Erdgeschoss und Obergeschoss) sowie das Foyer und der Aufenthaltsbereich der Schüler erfasst. Ebenfalls je eine Kamera ist in allen Schülertoiletten installiert. Diese zeichnen die Aktivitäten im Vorraum (Waschraum) der eigentlichen Toilettenanlage auf.

3.3.5.2.1.1.2
Gesamtschule Niederaula

In der Gesamtschule Niederaula (600 Schülerinnen und Schüler) wurden Kameras nach der Sanierung des Gebäudes installiert. Dabei handelt es sich um 16 Kameras sowie drei Attrappen. Diese sind im Außenbereich an den Eingängen installiert bzw. decken den Bereich des Schulhofs sowie die Außenwände ab. Im Innenbereich werden die Flure aller drei Etagen sowie das Foyer abgedeckt. Die Toilettenvorräume werden ebenfalls überwacht.

3.3.5.2.1.1.3
Gesamtschule Bebra

Hier zählt die Schülerzahl ca. 360 Köpfe. Im Jahr 2004, also vor fast zehn Jahren(!) wurde eine Videoanlage mit vier Einheiten installiert. Die Toilettenräume, der Aufenthaltsraum und der Haupteingang sind im Aufnahmefeld. Mit Kameraattrappen wird der Eindruck erweckt, als würde auch die hintere, dem Haupteingang gegenüber liegende Seite überwacht.

3.3.5.2.1.1.4
Konrad-Duden-Schule Bad Hersfeld

Die von 600 Schülerinnen und Schülern besuchte Gesamtschule hat ausschließlich im Außenbereich Kameras installiert. Überwacht werden der Schulhof sowie Vorder- und Hintereingang. Die Maßnahme wurde im Jahr 2012 realisiert.

3.3.5.2.1.1.5
Grundschule „An der Sommerseite“ Bad Hersfeld

Etwa 130 Kinder besuchen diese Schule. Nur der Außenbereich wird von fünf Kameras überwacht. Hierzu zählen u.a. die Treppe zum Haupteingang, der Eingang selbst sowie die vordere Fassade eines Neubaues. Hinzu kommt der Schulhof.

3.3.5.2.1.2
Technische Maßnahmen zur Umsetzung der Videoüberwachung

Die vorgenommenen technischen Maßnahmen sind in fast allen Fällen ähnlich realisiert. Es werden keine durchlaufenden Bilder erzeugt. Vielmehr findet eine Speicherung der Bilddaten statt. Das Aufzeichnungsgerät steht in der Regel in einem Raum, der vom Hausmeister der Schule genutzt wird. Bis zum Zeitpunkt der Anfrage an mein Haus war der Zugriff auf die Aufzeichnungen dem Hausmeister, der Schulleitung und in einigen Fällen bestimmten Lehrern möglich. Im weiteren Verlauf wurde der Zugriff auf dem Rekorder passwortgeschützt. Hausmeister und Schulleitung hatten je einen Teil des Passwortes, sodass ein Vier-Augen-Prinzip realisiert war. In einigen Fällen waren die Kameras mit einem Bewegungsmelder verbunden, zeichneten also nur dann auf, wenn

über den Melder der Eintritt einer Person in eine bestimmte Zone angezeigt wurde. Hinweise über die Videoüberwachung wurden in allen Schulen angebracht. Die Überwachung ist zeitlich nicht begrenzt und fand bis in den September vergangenen Jahres rund um die Uhr, also auch während des laufenden Schulbetriebs statt.

3.3.5.2.1.3
Motive für die Videoüberwachung

Bekanntermaßen sind insbesondere Schulen immer wieder das Ziel von Einbrüchen, sehen sich aber auch mit den unterschiedlichsten Formen von Vandalismus konfrontiert. Im Fall der in Rede stehenden Schulen kam es in der Vergangenheit auch immer wieder zu gravierenden Beschädigungen der Toilettenanlagen. Aber auch Außenwände wurden wiederholt in Mitleidenschaft gezogen, sodass sowohl der Schulträger, also der Landkreis Hersfeld-Rotenburg, als auch in der Mehrzahl die Schulleiterinnen oder Schulleiter es als ebenso probates wie legitimes Mittel ansahen, das Problem durch die Installierung von Kameras auch und insbesondere im Toilettenbereich in den Griff zu bekommen. Der Erfolg gab den Initiatoren vermeintlich Recht. Die Verschmutzung bzw. Beschädigung der Toilettenanlagen ging drastisch zurück, vermeintliche oder tatsächliche Verursacher wurden unter Zuhilfenahme der aufgezeichneten Bilder zur Verantwortung gezogen. Vom Ergebnis her kann der Schulträger eine nicht unbeträchtliche Summe von Renovierungskosten einsparen, die Reinigungskräfte sind nicht mehr mit teilweise übelster Form von Verunreinigung konfrontiert und Kinder sowie Jugendliche können saubere Toiletten benutzen.

3.3.5.2.1.4
Rechtliche und tatsächliche Gründe gegen die Videoüberwachung

Um es vorweg zu nehmen: Selbstverständlich will der Datenschutz nicht die Bemühungen derjenigen konterkarieren, die sich für saubere Schultoiletten und eine möglichst vandalismusfreie Schule exponieren. Auch ist es nicht hinnehmbar, wenn Kinder in der Schulzeit den Gang auf verschmutzte Toiletten meiden und deshalb z.B. die Einnahme von Flüssigkeit unterlassen. Dass es sich bei Vandalismus um kein Kavaliersdelikt handelt, ist klar. Dennoch müssen sich Schulträger und Schulleitungen an bestehendes Recht und Gesetz halten. So ist schon die Installation einer Videoüberwachung (nicht nur) an Schulen an Bedingungen geknüpft. In Ermangelung einer allgemeinen Rechtsgrundlage im HDSG kann in diesen Fällen die Videoüberwachung nur auf die engen Voraussetzungen des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) gestützt werden. So ist nach § 14 Abs. 4 Nr. 2 HSOG die Videoüberwachung nur zum Schutz einer **besonders gefährdeten öffentlichen Einrichtung** erlaubt. Schulen sind nicht von vorneherein

besonders gefährdete öffentliche Einrichtungen im Sinne des HSOG. Kriterien für die besondere Gefährdung sind die Eintrittswahrscheinlichkeit und die Größe des Schadens. Es reicht also nicht aus, wenn es einmal zu einem Vandalismusschaden gekommen ist. Ebenso sind verschmutzte oder beschädigte Toilettenanlagen unabhängig von dem Ärgernis kein Kriterium, welches die Installation von Videokameras rechtfertigen könnte. Vielmehr müssen derart schwerwiegende Beeinträchtigungen vorliegen, dass der Einsatz von Videotechnik zum Schutz der Einrichtung oder von Personen erforderlich ist und in Abwägung mit dem Rechtseingriff bei den Personen, deren Verhalten aufgezeichnet wird, verhältnismäßig erscheint.

Konkret bedeutet das die Möglichkeit zum Einsatz der Technik dann, wenn schwere Sachbeschädigungen in dem zur Überwachung vorgeschriebenen Bereich aufgetreten sind oder aber gehäuft tätliche Angriffe gegen Dritte zu verzeichnen sind. Ebenso kann man damit besonders schweren oder häufigen Straftaten (z.B. Drogenkriminalität) entgegenwirken. Das Bundesverwaltungsgericht hat in seinem Urteil vom 25. Januar 2012 (BVerwGE 141, 329) hierfür Kriterien entwickelt. Für die Beurteilung der Verhältnismäßigkeit spielt die Tiefe des Eingriffs in das Persönlichkeitsrecht der Betroffenen eine entscheidende Rolle. Der Rechtseingriff ist relativ gering, wenn z.B. die Kameras mit einer Einbruchmeldeanlage gekoppelt sind und eine Scharfschaltung außerhalb des Schulbetriebs erfolgt, in den Ferien oder aber nur nachts in Betrieb genommen wird.

Wie schwierig es ist, mit den aktuellen rechtlichen Instrumenten die Videoüberwachung im Schulbereich zu rechtfertigen, ergibt sich auch aus der Regelung des § 14 Abs. 4 HSOG. Danach ist der Videoeinsatz den Gefahrenabwehrbehörden vorbehalten. Nach Satz 2 zählt dazu auch der Inhaber des Hausrechts, in diesem Fall also der Schulträger. Ob dieser das Hausrecht für die Unterrichtszeit an den Schulleiter abtreten kann, ist strittig. Hinsichtlich der Frage der Zulässigkeit ist dies jedoch unerheblich. Unter dem Strich handelt es sich jedenfalls um eine Hilfskonstruktion, die meine Dienststelle für besondere Ausnahmefälle akzeptiert hat.

So muss am Ende der rechtlichen Bewertung der mit Videoüberwachungstechnik ausgestatteten Schulen im Landkreis Hersfeld-Rotenburg das Fazit gezogen werden, dass der Technikeinsatz unter den angetroffenen Verhältnissen so nicht zulässig ist. Die Nutzung der Kameras während des laufenden Schulbetriebs ist ausgeschlossen. Völlig inakzeptabel ist die Überwachungsmaßnahme im Bereich der Toiletten. Hier wurde dem Grundsatz der Verhältnismäßigkeit keinerlei Beachtung geschenkt, der Zweck heiligte offensichtlich die Mittel. Um es an dieser Stelle zu wiederholen: verstopfte oder verschmierte Sanitäranlagen sowie Vandalismus sind unakzeptabel. Auch die Kosten für die Beseitigung mutwillig verursachter Schäden haben i.d.R. beträchtliche Ausmaße. Dass man den Verursachern auf die Spur zu kommen versucht, um sie für die Schäden haftbar zu machen, ist nachvollziehbar und begrüßenswert. Dies jedoch mit Mitteln zu realisieren, welche der Gefahrenabwehr vorbehalten sind, verstößt gegen das Übermaßverbot.

Im Gegenteil stellt sich die Frage, warum das Fehlverhalten einer verschwindend geringen Minderheit dazu führt, die große Mehrheit derer, die sich innerhalb des Wertesystems korrekt verhalten, einem repressiv angelegten Überwachungsinstrumentarium auszusetzen. Nicht zuletzt steht dem auch der pädagogische Ansatz entgegen. Neben dem Bildungsauftrag als einer der Kernkompetenzen der Schule steht der erzieherische Aspekt zu aufgeklärten, mündigen und kritischen Schülerinnen und Schülern im Blickpunkt schulischen Handelns. Die dauerhafte Überwachung während der Schulzeit kommt einer Misstrauenserklärung gegenüber Schülerinnen und Schülern gleich. Eine Steigerung erfährt das Ganze durch die Überwachung der Toiletten. Hier wird der Intimbereich der Betroffenen berührt, die sich bei nächster Gelegenheit vielleicht noch vorhalten lassen müssten, nach dem Toilettengang nicht die Hände gereinigt zu haben.

3.3.5.2.1.5
Ergebnis der Prüfung und Bewertung

Die zuständigen Stellen innerhalb der Kreisverwaltung haben sich im Rahmen meiner Überprüfungen kooperativ und konstruktiv gezeigt. Das schließt einen Dissens im Rahmen meiner Bewertung natürlich nicht aus. Über die Tatsache der Überwachungsmaßnahmen selbst hinaus hatte der Kreis einige formale und inhaltliche Erfordernisse für eine Überwachung nicht beachtet:

– Zugriffs- bzw. Auswertungsregelungen auf das Bildmaterial waren nicht festgelegt,
– Einheitliche Regelungen für die Speicherung der Bilddaten fehlten,
– Die erforderlichen Verfahrensverzeichnisse nach § 28 HSOG fehlten,
– Eine Überprüfung auf die Erforderlichkeit der getroffenen Maßnahmen (also die Notwendigkeit des weiteren Betriebs der Kameras gem. § 14 Abs. 4 Satz 3 i.V.m. Abs. 3 Satz 3) erfolgte nicht. Dies hat alle zwei Jahre zu erfolgen und ist schriftlich zu dokumentieren.

In einem Brief an den Landrat des Kreises Hersfeld-Rotenburg habe ich meine Rechtsposition dargelegt und zunächst die Abschaltung der Kameras während des Schulbetriebs gefordert. Die Kameras in den Toiletten müssen abgebaut werden. Mittlerweile hat mir der Kreis versichert, dass während der Schulzeit die Kameras abgeschaltet sind.

3.3.5.2.2
Weitere Fälle der Videoüberwachung in Schulen

Der Landkreis Hersfeld-Rotenburg ist kein Einzelfall, aber in den geschilderten Auswüchsen nach meinem derzeitigen Kenntnisstand mit einem Alleinstellungsmerkmal versehen. Dennoch suchen einzelne Schulen, aber auch die Schulträger selbst nach Möglichkeiten, Vandalismus und Einbruch zu bekämpfen. Hier taucht immer wieder als Lösungsansatz der Einsatz von Videotechnik auf. So strebte der Schwalm-Eder-Kreis die Überwachung von zwei Schulen an. In diesem Fall zog man aber frühzeitig meine Behörde hinzu und ließ sich ebenfalls von der örtlichen Kriminalpolizei beraten. Das Ergebnis war, die Überwachung an einer Schule an neuralgischen Stellen zuzulassen, wenn die Kameras nur außerhalb der Schulzeit und mit einer Einbruchmeldeanlage gekoppelt betrieben werden. In dem anderen Fall konnte der Schulleiter überzeugt werden, auf das Instrument zu verzichten und stattdessen das konkrete Problem (Einnahme von Alkohol auf dem offen zugänglichen Schulgelände und daraus resultierende Verunreinigungen) in Zusammenarbeit mit der örtlichen Polizei in den Griff zu bekommen.

Weitere Anfragen erreichen mich in regelmäßigen Abständen und müssen dem konkreten Einzellfall geschuldet unterschiedlich entschieden werden.

3.3.5.2.3
Notwendigkeit einer Regelung der Videoüberwachung im HDSG

Die Erfahrungen der letzten Jahre haben gezeigt, dass immer mehr Schulträger wie auch Schulleiter zu der Überzeugung gelangen, mit Hilfe der Videotechnik Einbrüche und Sachbeschädigungen eindämmen zu können. Aus dem Blick gerät hierbei jedoch, dass es für derartige Maßnahmen an einer Regelung fehlt. Die Mängel der derzeitigen Regelung habe ich in diesem Beitrag aufgezeigt. Es sollte deshalb im HDSG eine Vorschrift geschaffen werden, die die Voraussetzungen und Schranken der Videoüberwachung durch öffentliche Stellen regelt. Damit sollte öffentlichen Stellen eine Videoüberwachung in engen Grenzen auch außerhalb der reinen Gefahrenabwehr eröffnet werden. Gerne bin ich bereit, bei der Gesetzesformulierung zu beraten. Mein Anliegen ist dabei, an einer interessengerechten und die Grundrechte wahrenden Regelung mitzuwirken mit dem Ziel, die Videoüberwachung nur ausnahmsweise einzusetzen und sie nicht zur Regel werden zu lassen.

3.3.5.3
Einführung von elektronischen Klassenbüchern in Schulen

Die beabsichtigte Einführung von elektronischen Klassenbüchern in hessischen Schulen war im Berichtsjahr ein zentrales Thema im Zusammenhang mit der Automatisierung von Verwaltungsprozessen in diesem Bereich. Bundesweit sind einige Projekte hierzu angestoßen worden. Auch in Hessen laufen derzeit einige Pilotprojekte, welche im Anschluss an die Erprobungsphase einer Evaluierung bedürfen. Auch datenschutzrechtliche Fragestellungen sind noch nicht endgültig geklärt.

3.3.5.3.1
Was enthält ein Klassenbuch?

Das Klassenbuch ist ein schulisches Dokument, in dem der behandelte Unterrichtsstoff, die Fehlstunden eines Schülers/einer Schülerin, die Hausaufgaben, auffälliges Verhalten und weitere wichtige Daten festgehalten werden. In einem Klassenbuch sind außerdem ein Schülerverzeichnis, Stundenpläne, Lehrerübersichten u.a. enthalten. In Hessen sind die Inhalte von Klassenbüchern in Anlage 1 Buchstabe A Ziff. 5 der Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen an Schulen vom 4. Februar 2009 (ABl. 2009, S. 131) geregelt.

3.3.5.3.2
Wie wird ein Klassenbuch im Schulalltag geführt?

Der sog. Klassenbuchführer ist i.d.R. für die Führung, den Zustand und die Aufbewahrung des Klassenbuchs verantwortlich. Er beschriftet z.B. zu Anfang des Schuljahres das Buch und trägt den Stundenplan ein. Kommt es zu Änderungen im Stundenplan, muss dies ebenso eingetragen werden. Hinzu kommt die Verantwortung über die Verfügbarkeit des Buches. Außerdem werden darin die gestellten Aufgaben und das Datum, zu welchem Zeitpunkt diese erfüllt sein müssen, vermerkt. Der Lehrer trägt die fehlenden Schüler/Schülerinnen ebenso ins Klassenbuch ein wie jene, die zu spät zum Unterricht kommen. Die Richtigkeit der Eintragungen wird mit einem Handzeichen des Lehrers bestätigt. Notwendige Maßnahmen z.B. in Form von Briefen an die Eltern, weil der Schüler zu häufig fehlt oder sich verspätet, müssen daraus herausgelesen werden.

3.3.5.3.3
Neue Möglichkeiten durch den Einsatz automatisierter Datenverarbeitung

Der Einsatz sog. elektronischer Klassenbücher soll in der Zukunft die Verwaltungsarbeit der Lehrer erleichtern und die Kommunikation mit den Eltern verbessern. Das, was bislang im Klassenbuch in Papierform abgebildet und für die Eltern grundsätzlich nicht einsehbar war, soll in Zukunft als Information für die Betroffenen jederzeit zugänglich sein. Eltern oder bei Berufsschülern der Arbeitgeber können sich taggenau darüber informieren, ob ihr Kind in der Schule bzw. der Auszubildende in der Berufsschule war oder ob die Betroffenen zu spät gekommen sind. Auch können sich Schüler über Unterrichtsinhalte informieren und Hausaufgaben zur Kenntnis nehmen. In Testversuchen anderer Bundesländer werden SMS an die Eltern verschickt, wenn das Kind nicht am Unterricht teilnimmt. In welcher Form und in welchem Umfang dieses in Softwareprodukten auch als „Fehlzeitenmanagement“ bezeichnete Verfahren dann tatsächlich zum Einsatz kommt, hängt von dem Produkt selbst bzw. der Leistungsanforderung des Anwenders, also der Schule, ab. Der Zugriff auf die Datenbank erfolgt online. Dienstleister sind in vielen Fällen private Anbieter, die sich dritter Unternehmen bedienen, welche die technischen Ressourcen eines Rechenzentrums zur Verfügung stellen. Datenschutzrechtliche Problemstellungen ergeben sich in der rechtlichen und technischen Bewertung der Prozesse. So ist eine Online-Nutzung von Schulverwaltungsdaten weder im Schulgesetz noch in den Rechtsverordnungen und Erlassen hierzu geregelt. Auch ergibt sich eine neue Qualität im Datenverarbeitungsprozess, der nicht mehr lokal in der Schule selbst oder beim Schulträger über ggf. geschützte Netze stattfindet. Vielmehr werden personenbezogene Verwaltungsdaten über das offene Netz transportiert und von einer Vielzahl externer Nutzer zur Kenntnis genommen. Hier stellen sich Fragen wie die Sicherstellung eines autorisierten Zugriffs hierzu berechtigter Personen, die Verschlüsselung der Inhalte sowie Sicherstellung der Segmentierung der Datenbestände für die unterschiedlichen Nutzer in Form eines Rollenkonzepts. Schließlich sollen am Ende Schulleitung, Lehrer, Schüler, Eltern und Arbeitgeber ein solches System nutzen und die einschlägigen Informationen daraus erhalten.

3.3.5.3.4
Weitere Nutzungsmöglichkeiten

Die Verwaltung von Fehlzeiten ist aber nur eine von vielen weiteren Nutzungsmöglichkeiten. Notenverwaltung, Stundenplangestaltung, Lehrervertretung u.a. können mit einem derartigen Instrument abgedeckt werden und die Verwaltungsarbeit der Lehrer erleichtern, die Kommunikation zwischen den betroffenen Stellen optimieren und erhebliche Zeitersparnis ermöglichen. Doch die Gefahr eines „gläsernen Schülers“ ist hierbei nur eine mögliche Gefahrenquelle für das Persönlichkeitsrecht der Betroffenen. So ist durch das Kultusministerium und das Landesschulamt die rechtli-

che Frage zu klären, ob Verwaltungsdaten außerhalb der Schule selbst verarbeitet werden dürfen. Nach meiner Einschätzung gibt dies die derzeitige Rechtslage ebenso wenig her wie die Frage zu stellen ist, wie sichergestellt wird, dass die hessenweit für alle öffentlichen Schulen maßgebliche Lehrer- und Schülerdatenbank (LUSD) auch dann hinsichtlich ihrer Datenbestände aktuell bleibt, wenn zumindest nicht unwesentliche Bereiche der Schulverwaltung über private Dienstleister administriert werden.

3.3.5.3.5
Erste Aktivitäten zur Begleitung derartiger Anwendungen

Der Einsatz von Verwaltungsplattformen im Schulbereich eröffnet eine Fülle von Funktionalitäten, die über jene des Klassenbuchs herkömmlicher Prägung deutlich hinaus gehen. Bereits das Modul „Fehlzeitenmanagement" für sich genommen beinhaltet durch den Online-Zugriff unterschiedlicher Nutzergruppen eine neue Qualität der Datenverarbeitung und Kommunikation. Es ist deshalb zwingend erforderlich, einen rechtlichen und technischen Rahmen unter Berücksichtigung der Art der verarbeiteten Daten zu schaffen. Hierzu erstellen meine Mitarbeiter derzeit ein Papier, welches mit dem Kultusministerium und dem Landesschulamt abgestimmt werden soll und in einen Erlass münden könnte, der allgemeinverbindlich den Einsatz dieser Produkte regelt. Die Nutzungsmöglichkeiten erscheinen aus Sicht der Anwender zunächst attraktiv und hinsichtlich des bisher erforderlichen Aufwandes wünschenswert zu sein. Auf der anderen Seite steht die Verarbeitung personenbezogener, teilweise sensibler Daten von Schülern und Lehrern, die externe Dienstleister über das Internet anbieten. Diese Daten werden angreifbar, könnten durch unbefugte Dritte abgeschöpft oder verfälscht werden. Deshalb muss die Kommunikation nach den derzeitigen technischen Standards sicher gemacht werden; ggf. können bestimmte Datenarten in dieser Form grundsätzlich nicht verarbeitet werden. Erste Pilotanwendungen verschiedener Produkte an wenigen, ausgesuchten hessischen Schulen sollen bis zum nächsten Bericht evaluiert und datenschutzrechtlich bewertet werden.

3.3.5.4
Änderung des Kandidatenverfahrens der LUSD

Das bisher bei einem Schulwechsel vorgesehene sog. Kandidatenverfahren, mit dem der aufnehmenden Schule die Übernahme der für die Schuljahresplanung erforderlichen Schülerdaten aus der zentralen Lehrer- und Schülerdatenbank LUSD ermöglicht wurde, hat sich in der Praxis in Fällen eines zwischenzeitlichen Umzugs des Schülers oder der Schülerin als untauglich erwiesen. Die

Projektzuständigen im Hessischen Kultusministerium habe ich bei der Erarbeitung einer besser praxistauglichen, aber gleichwohl datenschutzgerechten Lösung beraten.

Einige hessische Schulen sind mit der Bitte an mich herangetreten zu prüfen, ob eine Änderung des sogenannten Kandidatenverfahrens in der landesweiten, zentralen Lehrer- und Schülerdatenbank LUSD unter Wahrung datenschutzrechtlicher Belange möglich sei.

Bei der Einführung der LUSD wurde darauf Wert gelegt, dass alle im Verfahren anfallenden Daten durch das Rollen- und Berechtigungskonzept nur im Zugriff der jeweils Daten verarbeitenden Schule liegen. An der datenschutzrechtlichen Einordnung sollte sich in diesem Punkt mit der Zentralisierung gegenüber dem Altverfahren mit dezentralen Dateien nichts ändern.

Andererseits war es ein naheliegendes Ziel des landesweiten Modells, eine Übergabe der Daten für einen Schulwechsel zu ermöglichen. Dafür wurde ein gesondert berechtigtes Modul, das „Kandidatenverfahren“, programmiert, das bei Eingabe des richtigen Namens, Vornamens und Geburtstages alle Schüler in Hessen auflistet, auf die die Suchkriterien zutreffen. Um im Verfahren zum nächsten Schritt zu kommen, ist bisher die Eingabe des Straßennamens der im System LUSD hinterlegten Wohnadresse erforderlich. Erst danach werden der aufnehmenden Schule weitere Informationen zu der Person zugänglich, und die Daten der ausgewählten Schülerin oder des ausgewählten Schülers können für die Übernahme im System markiert werden. Ab diesem Zeitpunkt stehen der aufnehmenden Schule wenige Eckdaten zur Verfügung, die aber z.B. für die Planung des nächsten Schuljahres unbedingt gebraucht werden.

Mit diesem aufwändigen Verfahren sollte ausgeschlossen werden, dass über eine unbefugte Suche hessenweit der Aufenthaltsort bzw. die besuchte Schule zu einer beliebigen Person ermittelt werden kann. Nur wer den Straßennamen aus der im System hinterlegten Adresse bereits kennt, erhält Zugriff auf die Daten, erfährt in den folgenden Schritten des Verfahrens aber keine wesentlichen Zusatzinformationen über die ausgewählten Schüler bzw. Schülerinnen.

Die noch zuständige Schule bekommt danach den Hinweis, dass ein Schüler bzw. eine Schülerin für die Übernahme durch eine andere Schule markiert ist, und gibt die Daten der die Schule wechselnden Person nach einer Plausibilitätsprüfung für die aufnehmende Schule frei.

Das Kandidatenverfahren setzt also voraus, dass die aufnehmende Schule die aus Systemsicht „richtigen“ Adressangaben für die Suche verwendet. Meldet sich z.B. ein Schüler oder eine Schülerin nach einem Umzug an einer neuen Schule mit der neuen Adresse an, kann das Kandidatenverfahren nicht greifen. Insbesondere die Berufs- und Oberstufenschulen beklagen, dass die Zahl

dieser Fälle und der damit verbundene Rechercheaufwand zum Schuljahreswechsel erhebliche Probleme machen.

Unter anderen hat mich eine Berufsschule mit dem konkreten Vorschlag angeschrieben, zu prüfen, ob an der Stelle des Straßennamens ein anderes Suchkriterium wie der Geburtsort verwendet werden könne. Bei einem Gespräch in der Schule haben meine Mitarbeiter den gesamten Sachzusammenhang noch einmal hinterfragt. Es wurde dabei die Idee entwickelt, den Zugriff auf die Schülerdaten auch bei einer unvollständigeren Suche zu gewähren, dabei aber die zugänglichen Daten gezielt einzuschränken, um eine Aufenthaltsbestimmung unmöglich bzw. die aktuell besuchte Schule nicht kenntlich zu machen. Auch dieser Datensatz kann durch die aufnehmende Schule für die Schuljahresplanung verwendet werden, und wird im Weiteren mit der Freigabe durch die abgebende Schule vervollständigt.

Nach diesem Vor-Ort-Besuch habe ich den dort entwickelten Vorschlag aufgegriffen und mit den Projektzuständigen im Hessischen Kultusministerium über die grundsätzlichen Möglichkeiten und Rahmenbedingungen für eine arbeitserleichternde Änderung gesprochen. Fachleute und Verantwortliche werden prüfen, inwieweit mit der auch aus anderen Gründen anstehenden Neuprogrammierung dieses Moduls der LUSD eine datenschutzkonforme Umsetzung der Gesprächsergebnisse möglich ist. Das Kultusministerium will die Überlegungen in die Spezifikation für eine Ausschreibung zur Neuprogrammierung des Kandidatenverfahrens aufnehmen.

Wünschenswert ist, dass die Änderung des Verfahrens möglichst bald in einer der nächsten LUSD-Versionen zu einer Erleichterung des Verwaltungsalltags der Schulen beiträgt. Der ganze Vorgang ist ein gelungenes Beispiel für eine konstruktive Lösungssuche aller Beteiligten, bei der die datenschutzrechtlichen Anforderungen sichergestellt bleiben.

3.3.6 Gesundheitswesen

3.3.6.1
Aufbau klinischer Krebsregister in Hessen

2013 hat der Deutsche Bundestag das Krebsfrüherkennungs- und -registergesetz verabschiedet. Entsprechend den Empfehlungen des Nationalen Krebsplans sieht das Bundesgesetz vor, dass die Länder klinische Krebsregister einrichten. Die notwendigen (datenschutz-)rechtlichen Regelungen für die konkrete Einrichtung und den Betrieb der klinischen Krebsregister bleiben landesrechtlicher Regelung vorbehalten und wurden von der Landesregierung mit meiner Dienststelle abgestimmt.

3.3.6.1.1
Ziel und Regelungsumfang des Bundesgesetzes

In Übereinstimmung mit dem Nationalen Krebsplan, der insbesondere auch den flächendeckenden Aufbau von klinischen Krebsregistern unter einheitlichen Rahmenbedingungen empfohlen hat (http://www.bmg.bund.de/praevention/nationaler-krebsplan/der-nationale-krebsplan-stellt-sich-vor.html), sieht das Krebsfrüherkennungs- und -registergesetz (KFRG) Regelungen zur Weiterentwicklung der Krebsfrüherkennung und zum flächendeckenden Aufbau klinischer Krebsregister vor. Hierfür wurden das Sozialgesetzbuch (SGB) V, das Krankenhausfinanzierungsgesetz (KHG) und das Krankenhausentgeltgesetz (KHEntgG) geändert. In § 65 c Abs. 1 SGB V ist normiert, dass die Länder zur Verbesserung der Qualität der onkologischen Versorgung klinische Krebsregister einrichten und die Aufgaben der klinischen Krebsregister sind detailliert festgelegt.

§ 65 c Abs. 1 SGB V

(1) Zur Verbesserung der Qualität der onkologischen Versorgung richten die Länder klinische Krebsregister ein. Die klinischen Krebsregister haben insbesondere folgende Aufgaben:

1. die personenbezogene Erfassung der Daten aller in einem regional festgelegten Einzugsgebiet stationär und ambulant versorgten Patientinnen und Patienten über das Auftreten, die Behandlung und den Verlauf von bösartigen Neubildungen einschließlich ihrer Frühstadien sowie von gutartigen Tumoren des zentralen Nervensystems nach Kapitel II der Internationalen statistischen Klassifikation der Krankheiten und verwandter Gesundheitsprobleme (ICD) mit Ausnahme der Daten von Erkrankungsfällen, die an das Deutsche Kinderkrebsregister zu melden sind,

2. die Auswertung der erfassten klinischen Daten und die Rückmeldung der Auswertungsergebnisse an die einzelnen Leistungserbringer,

3. den Datenaustausch mit anderen regionalen klinischen Krebsregistern bei solchen Patientinnen und Patienten, bei denen Hauptwohnsitz und Behandlungsort in verschiedenen Einzugsgebieten liegen, sowie mit Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene,

4. die Förderung der interdisziplinären, direkt patientenbezogenen Zusammenarbeit bei der Krebsbehandlung,

5. die Beteiligung an der einrichtungs- und sektorenübergreifenden Qualitätssicherung des Gemeinsamen Bundesausschusses nach § 137 Absatz 1 Nummer 1 in Verbindung mit § 135a Absatz 2 Nummer 1,

6. die Zusammenarbeit mit Zentren in der Onkologie,

7. die Erfassung von Daten für die epidemiologischen Krebsregister,

8. die Bereitstellung notwendiger Daten zur Herstellung von Versorgungstransparenz und zu Zwecken der Versorgungsforschung.

Die klinische Krebsregistrierung erfolgt auf der Grundlage des bundesweit einheitlichen Datensatzes der Arbeitsgemeinschaft Deutscher Tumorzentren und der Gesellschaft der epidemiologischen Krebsregister in Deutschland zur Basisdokumentation für Tumorkranke und ihn ergänzender Module flächendeckend sowie möglichst vollzählig. Die Daten sind jährlich landesbezogen auszuwerten. Eine flächendeckende klinische Krebsregistrierung kann auch länderübergreifend erfolgen. Die für die Einrichtung und den Betrieb der klinischen Krebsregister nach Satz 2 notwendigen Bestimmungen einschließlich datenschutzrechtlicher Regelungen bleiben dem Landesrecht vorbehalten.

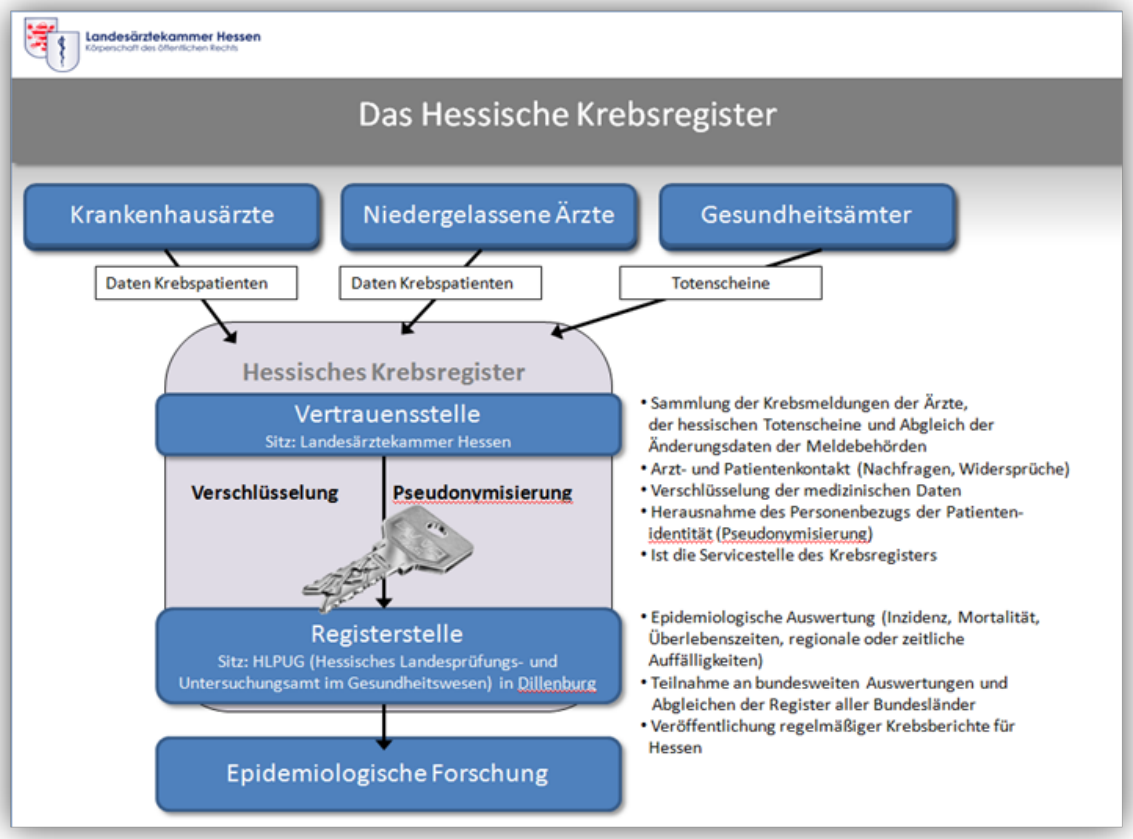
Gem. § 65c Abs. 1 SGB V bleiben die für die Einrichtung und den Betrieb der klinischen Krebsregister notwendigen Bestimmungen einschließlich datenschutzrechtlicher Regelungen dem Landesrecht vorbehalten. Vom Landesgesetzgeber ist daher insbesondere zu regeln:

– die Struktur der Krebsregistrierung, insbesondere die Art und Weise der Verzahnung von klinischen und epidemiologischen Krebsregistern,
– die Betreiber der klinischen Krebsregister,
– ob für die meldenden Leistungserbringer ein Melderecht oder eine Meldepflicht besteht und
– welche Rechte die Patienten haben (Notwendigkeit der Einwilligung des Patienten oder Widerspruchsrecht).

3.3.6.1.2
Ausgestaltung der klinischen Krebsregister in Hessen

Derzeit existiert in Hessen lediglich das epidemiologische Hessische Krebsregister. Dieses Register hat die Aufgabe, bevölkerungsbezogene Auswertungen von Krebserkrankungen zu ermögli-

chen. Es besteht aus zwei organisatorisch und räumlich getrennten Einheiten, der Vertrauensstelle und der Registerstelle (Treuhandstelle).



Die Vertrauensstelle ist bei der Landesärztekammer in Frankfurt angesiedelt. Ärztinnen und Ärzte bzw. Zahnärztinnen und Zahnärzte melden für jeden Krebskranken einerseits Angaben zur Person (Identitätsdaten, wie Name, Geschlecht, Anschrift), andererseits kurze Angaben zur Erkrankung (Diagnose, Therapie) an diese Stelle. Nach Entgegennahme der Meldungen nimmt die Vertrauensstelle Plausibilitätsprüfungen und Verschlüsselungen der medizinischen Daten vor. Dann werden die Identitätsdaten der Patienten vor der Weitergabe an die Registerstelle, die die epidemiologischen Auswertungen vornimmt, so verschlüsselt, dass die Registerstelle die Personen nicht identifizieren kann, deren Krankheitsdaten sie erhalten hat. Der Personenbezug kann nur mit Hilfe eines beim Hessischen Datenschutzbeauftragten hinterlegten Programms rückgängig gemacht werden. Nach Übermittlung an die Registerstelle werden in der Vertrauensstelle die Meldeunterlagen vernichtet und die Klartextdaten gelöscht (http://laekh.de/krebsregister/hessisches-krebsregister).

Die Aufgaben und die für die Erfüllung der Aufgaben benötigten Daten von epidemiologischen und von klinischen Krebsregistern überschneiden sich teilweise, sodass künftig eine Koordination bzw. Zusammenführung der verschiedenen Aufgaben der beiden Register denkbar ist. Aus daten-

schutzrechtlicher Sicht ist es in jedem Fall für die Ausgestaltung des klinischen Krebsregisters von zentraler Bedeutung, dass nur für diejenigen Aufgaben, die tatsächlich eine Verarbeitung personenbezogener Daten erfordern, auch personenbezogene Daten zur Verfügung stehen.

Dies könnte z.B. die Weitergabe von Patientendaten an Leistungserbringer sein, wenn und soweit dies die interdisziplinäre, direkt patientenbezogene Zusammenarbeit bei der Krebsbehandlung fördert. Alle anderen Aufgaben müssen mit pseudonymisierten oder anonymisierten Daten durchgeführt werden, z.B. die in § 65c Abs. 1 Nr. 5 SGB V normierte Beteiligung an der einrichtungs- und sektorenübergreifenden Qualitätssicherung des Gemeinsamen Bundesausschusses nach § 137 Abs. 1 Nr. 1 i.V.m. § 135a Abs. 2 Nr. 1 SGB V.

§ 137 Abs. 1 Satz 1 SGB V
(1) Der Gemeinsame Bundesausschuss bestimmt für die vertragsärztliche Versorgung und für zugelassene Krankenhäuser grundsätzlich einheitlich für alle Patienten durch Richtlinien nach § 92 Abs. 1 Satz 2 Nr. 13 insbesondere
1. die verpflichtenden Maßnahmen der Qualitätssicherung nach § 135a Abs. 2, § 115b Abs. 1 Satz 3 und § 116b Absatz 3 Satz 3 unter Beachtung der Ergebnisse nach § 137a Abs. 2 Nr. 1 und 2 sowie die grundsätzlichen Anforderungen an ein einrichtungsinternes Qualitätsmanagement.

§ 135a Abs. 1 und 2 Nr. 1 SGB V
(1) Die Leistungserbringer sind zur Sicherung und Weiterentwicklung der Qualität der von ihnen erbrachten Leistungen verpflichtet. Die Leistungen müssen dem jeweiligen Stand der wissenschaftlichen Erkenntnisse entsprechen und in der fachlich gebotenen Qualität erbracht werden.

(2) Vertragsärzte, medizinische Versorgungszentren, zugelassene Krankenhäuser, Erbringer von Vorsorgeleistungen oder Rehabilitationsmaßnahmen und Einrichtungen, mit denen ein Versorgungsvertrag nach § 111a besteht, sind nach Maßgabe der §§ 137 und 137d verpflichtet,
1. sich an einrichtungsübergreifenden Maßnahmen der Qualitätssicherung zu beteiligen, die insbesondere zum Ziel haben, die Ergebnisqualität zu verbessern.

Im Detail gibt es noch offene Fragen, welche Stelle welche Aufgaben auf welche Weise erfüllen soll und wie die Zusammenarbeit der klinischen Krebsregister untereinander bundesweit und mit den epidemiologischen Krebsregistern ausgestaltet werden kann.

Das Hessische Sozialministerium hat einen wissenschaftlichen Krebsbeirat eingerichtet, der die Fragen der künftigen Ausgestaltung des klinischen Krebsregisters diskutiert, und meine Dienststel-

le zu den Sitzungen eingeladen. Ich habe die Teilnahme zugesagt, um zur datenschutzkonformen Umsetzung der Ziele des Bundesgesetzes beizutragen. Ein Gesetzentwurf wird voraussichtlich im ersten Halbjahr 2014 erarbeitet werden.

3.3.6.2
Notwendigkeit der Eingrenzung der Datenübermittlungen vom Medizinischen Dienst der Krankenversicherung an die Krankenkasse

Nicht alle Informationen, die in einem Gutachten des Medizinischen Dienstes der Krankenversicherung enthalten sind, dürfen an die Krankenkasse weitergeleitet werden.

3.3.6.2.1
Anlass

Mir lag eine Eingabe eines Petenten zum Umfang und Inhalt der in einem Gutachten des Medizinischen Dienstes der Krankenversicherung (MDK) enthaltenen Informationen vor. Im vorliegenden Fall hatte eine gesetzliche Krankenkasse den MDK beauftragt, ein Gutachten zur voraussichtlichen Dauer der Arbeitsunfähigkeit zu erstellen. Nach erfolgter körperlicher Untersuchung erstellte der MDK ein umfängliches Gutachten und schickte dieses an die beauftragende Krankenkasse. Neben den Diagnosen, dem Verlauf der Untersuchung, den Befunden und der Aussage zur Dauer der Arbeitsunfähigkeit enthielt das Gutachten auch Angaben zur Anamnese, Äußerungen des Patienten gegenüber dem Gutachter und Beobachtungen im Zusammenhang mit der Untersuchung. Nach Meinung des Petenten sei ein Teil der Informationen für die Krankenkasse nicht relevant.

Ich habe den Fall zum Anlass genommen, mich nochmals mit den Übermittlungsbefugnissen des MDK an die Krankenkassen zu befassen, da diese Frage auch bundesweit aktuell diskutiert wird.

3.3.6.2.2
Datenschutzrechtliche Bewertung

Zu den Aufgaben des MDK gehört es, gutachterliche Stellungnahmen für die gesetzliche Krankenkasse zu fertigen (§ 275 SGB V).

Zu berücksichtigende datenschutzrechtliche Bestimmungen sind dabei die Regelungen zum Sozialgeheimnis (§ 35 SGB I) und zum Schutz von Sozialdaten (§§ 67 ff. SGB X) sowie die Vorschrift zur Verletzung von Privatgeheimnissen (§ 203 StGB).

Eine Weitergabe von Daten darf nur dann erfolgen, wenn der Versicherte eingewilligt hat oder es eine gesetzliche Grundlage für Weitergabe von Patientendaten gibt.

§ 277 Abs. 1 S. 1 SGB V

Der Medizinische Dienst hat dem an der vertragsärztlichen Versorgung teilnehmenden Arzt, sonstigen Leistungserbringern, über deren Leistungen er eine gutachterliche Stellungnahme abgegeben hat, und der Krankenkasse das Ergebnis der Begutachtung und der Krankenkasse die erforderlichen Angaben über den Befund mitzuteilen.

§ 277 SGB V regelt die Mitteilungspflichten des MDK gegenüber der gesetzlichen Krankenkasse. Im Rahmen dieser Vorschrift ist es zulässig, medizinische Daten an die Krankenkasse weiterzugeben. Gleichzeitig hat der Gesetzgeber aber damit auch den Übermittlungsumfang eingegrenzt. So ist die Übermittlung von Daten auf das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund zu beschränken (§ 277 Abs. 1 S. 1 SGB V). Für eine darüber hinausgehende Übermittlung gibt es keine rechtliche Grundlage. Auch eine Erweiterung des Übermittlungsumfanges mit einer Einwilligungserklärung des Betroffenen scheidet aus, da diese die gesetzlich klar und abschließend festgelegte Einschränkung des § 277 Abs. 1 S. 1 SGB V umgehen würde.

Im Rahmen einer Begutachtung werden vom MDK umfängliche medizinische Daten erhoben, um auf die Fragestellung der Krankenkasse antworten zu können. Bei der Antwort an die Krankenkasse ist dann jedoch abzuschichten, welche Daten davon für die Aufgaben der Krankenkasse erforderlich sind und damit übermittelt werden können. Die aus dem Gutachten übermittelten Informationen müssen geeignet sein, die Krankenkasse in die Lage zu versetzen, eine Leistungsentscheidung zu treffen. Eine reine Übermittlung des Ergebnisses der Begutachtung wird aber in vielen Fällen nicht ausreichen. So kann es erforderlich sein, dass weitere Kontextfaktoren mit angegeben werden müssen, um zu begründen, wieso die aufgeführten Befunde/Diagnosen letztlich zu einer Arbeitsunfähigkeit führen. Es darf jedoch nicht sein, dass in jedem Fall stets das komplette Gutachten übermittelt wird. Der Gutachter des MDK muss im Einzelfall entscheiden, welche Informationen aus dem Gesamtgutachten ergänzend zum Befund als „erforderliche Angaben über den Befund“ aufzunehmen sind.

Um einen Eindruck vom Umfang und Inhalt der an die Krankenkasse übermittelten Gutachten zu gewinnen, habe ich Gespräche mit dem MDK Hessen geführt. Bei meiner stichprobenhaften Prü-

fung der Gutachten konnte ich festzustellen, dass in vielen Fällen die kompletten Gutachten an die Krankenkasse übermittelt wurden. Eine Abschichtung oder Ausblendung von Gutachtenbestandteilen war nicht immer erkennbar, so z.B. auch nicht im konkreten Beschwerdefall.

Die Entscheidung, ob neben den Befunden auch in Einzelfällen Angaben aus der Anamnese in die Mitteilungen an die Krankenkasse mit aufgenommen werden können, fällt in der Praxis nicht leicht. Teilweise ist die Angabe dieser Erhebungen aber wichtig, um die Befunde hinreichend verständlich zu machen. In Einzelfällen war mir dies auch nachvollziehbar.

Nach meinen Gesprächen mit dem MDK Hessen bestand Einigkeit, dass nicht alle Informationen, die bei der Gutachtenerstellung anfallen, von der Krankenkasse benötigt werden. Der MDK Hessen hat zugesagt, zukünftig verstärkt darauf achten, dass nur die Teile des Gutachtens an die Krankenkasse übermittelt werden, die notwendige den Befund untermauernde medizinische Angaben mit Bedeutung für die Leistungsgewährung enthalten.

3.3.6.3
Voraussetzungen einer zulässigen Verwendung von Selbstauskunftsbogen durch die Krankenkassen

Gesetzliche Krankenkassen können in Arbeitunfähigkeitsfällen selbst Daten bei den Versicherten erheben. Dabei ist jedoch die Abgrenzung zum Medizinischen Dienst der Krankenversicherung zu beachten.

3.3.6.3.1
Der Anlass

In den letzten Monaten wurde in den Medien wiederholt das Verfahren zahlreicher Krankenkassen kritisiert, Versicherte umfassend zu ihrer Erkrankung und ihrer persönlichen Situation zu befragen, sobald diese Krankengeld beziehen. Ich habe mich daher mit den datenschutzrechtlichen Voraussetzungen für den Einsatz solcher Fragebogen in Hessen befasst.

3.3.6.3.2
Datenschutzrechtliche Bewertung

Unter welchen Voraussetzungen gesetzliche Krankenkassen Daten erheben dürfen, wurde vom Gesetzgeber in den Sozialgesetzbüchern abschließend geregelt. Nach § 284 Abs. 1 Nr. 4 SGB V sind Krankenkassen berechtigt, Sozialdaten für Zwecke der Krankenversicherung zu erheben und zu speichern, sofern dies für die Prüfung der Leistungspflicht und die Erbringung von Leistungen an Versicherte erforderlich ist. Hierzu können sie auch Kontakt mit ihren Versicherten aufnehmen, um bestimmte Informationen zu erfragen.

Die datenschutzrechtliche Zulässigkeit beurteilt sich dabei nach der Erforderlichkeit für die jeweilige konkrete Aufgabe. Durch das gesetzlich geregelte Verhältnis der gesetzlichen Krankenkassen zum medizinischen Dienst der Krankenversicherung (MDK) sind den Krankenkassen jedoch Grenzen bei Umfang und Inhalt der Datenerhebung in Arbeitsunfähigkeitsfällen gesetzt, da die medizinische Fachkompetenz im Zuständigkeitsbereich des MDK liegt.

So legt § 275 SGB V fest, in welchen Fällen der MDK einzuschalten ist. Danach ist immer, wenn eine Arbeitsunfähigkeit nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf es erforderlich macht, die Krankenkasse verpflichtet, eine gutachterliche Stellungnahme des MDK einzuholen (§ 275 Abs. 1 SGB V). Die Prüfung, ob ein Arbeitunfähigkeitsfall den vorgenannten Kriterien entspricht, obliegt der Krankenkasse.

Hat die Krankenkasse Anhaltspunkte, dass es sich um einen Fall im Sinne des § 275 SGB V handeln könnte, ist sie im nächsten Schritt auch befugt, ggf. Vorermittlungen auf der Grundlage weiterer Datenerhebungen zum Beispiel auch durch Selbstauskunftsbogen einzuleiten, um zu klären, ob dies tatsächlich der Fall ist.

Zu einer pauschalen Datenerhebung mit Selbstauskunftsbogen bei allen Arbeitsunfähigkeitsfällen darf dies jedoch nicht führen, denn ein solches Vorgehen verstieße gegen den Grundsatz der Erforderlichkeit, da nicht bei jeder Arbeitsunfähigkeit überhaupt eine Vorlage beim MDK in Betracht kommt. Ebenfalls muss der verwendete Fragebogen im Inhalt und Umfang dem Grundsatz der Verhältnismäßigkeit entsprechen. So sind Fragen, die für die Leistungsprüfung nicht benötigt werden, auch nicht zulässig.

Die aus den Selbstauskunftsbogen gewonnenen Informationen sind dazu bestimmt, den Mitarbeitern der Krankenkasse zu helfen, eine Entscheidung zu treffen, ob ein Fall dem MDK vorgelegt werden muss (§ 284 Abs. 1 Nr. 4 SGB V), zusätzliche Leistungen erforderlich sind, die Zuständig-

keit eines anderen Leistungsträgers vorliegt oder zur Zeit keine weiteren zusätzlichen Maßnahmen angezeigt sind.

Sollte nach diesen Vorerhebungen eine medizinische Klärung erforderlich sein, erteilt die Krankenkasse im nächsten Schritt einen Auftrag zur gutachterlichen Stellungnahme an den MDK.

Auch hier hat die Krankenkasse die Möglichkeit, medizinische Daten zu ermitteln, die für den MDK notwendig sind (§ 284 Abs. 1 Nr. 7 SGB V). Aufgrund des Erforderlichkeitsgrundsatzes dürfen die Mitarbeiter der Krankenkasse diese für den MDK erhobenen Daten jedoch nicht zur Kenntnis nehmen. Die angeforderten Unterlagen sind direkt vom Arzt an den MDK zu übersenden oder können z.B. im verschlossenen Umschlag für den MDK bei der Krankenkasse hinterlegt werden. Reichen dem MDK die vorgelegten Unterlagen letztendlich nicht aus, hat der MDK auch die Möglichkeit, die benötigten Unterlagen eigenständig anzufordern (§ 276 Abs. 2 SGB V).

Zusammenfassend ist ein Einsatz von Selbstauskunftsbogen im Krankengeldfallmanagement möglich, wenn der Einsatz nur gezielt erfolgt, ein konkreter Anlass besteht und die abgefragten Informationen für die Prüfung der Leistungsgewährung erforderlich sind. Die im jeweiligen Fall nicht erforderlichen Fragen sind aus dem Fragebogen zu löschen oder zu streichen. Außerdem ist der Versicherte auf die Rechtsgrundlage für die Erhebungen und die Folgen bei Verweigerung der Auskunft bzw. ansonsten die Freiwilligkeit seiner Angaben hinzuweisen (§ 67a Abs. 3 SGB X).

Aufgrund der öffentlichen Diskussionen habe ich die gesetzlichen Krankenkassen innerhalb meines Zuständigkeitsgebietes angeschrieben und nach Umfang und Zweck des Einsatzes von Selbstauskunftsbogen im Zusammenhang mit der Krankengeldzahlung gefragt. Soweit überhaupt Selbstauskunftsbogen verwendet werden, habe ich darin keine Anhaltspunkte für eine Überschreitung des rechtlichen Rahmens gewonnen.

Im Berichtszeitraum erreichten mich auch keine Beschwerden, die Fragebogen von Krankenkassen in meinem Zuständigkeitsbereich betreffen.

3.3.6.4
Ungesicherte Krankenakten im Universitätsklinikum

Auch für den Fall, dass in Archiven mit Krankenakten Bauarbeiten mit Fremdfirmen durchgeführt werden, ist sicher zu stellen, dass die Akten gegen fremden Zugriff geschützt sind. Entsprechendes lässt sich in der Regel mit einfachen organisatorischen und baulichen Maßnahmen zeitnah umsetzen. Auch Aspekte der Datensicherheit spielen hierbei eine Rolle.

3.3.6.4.1
Der Anlass

Der Ausgangspunkt dieses Beitrages war eine Eingabe betreffend die ungesicherte Verwahrung einer Krankenakte auf einer Station im Klinikum der Johann Wolfgang Goethe-Universität Frankfurt am Main. Der Datenschutzbeauftragte der Klinik hat diese Eingabe zum Anlass genommen, eine ausführliche Datenschutzbegehung auf der Station durchzuführen. Hierbei stellte sich heraus, dass während fortdauernder Bauarbeiten im Keller zwei Archive mit Krankenakten nicht hinreichend gegen fremden Zugriff geschützt waren. Insbesondere fehlte es an einer verschließbaren, räumlichen Abtrennung.

3.3.6.4.2
Datenschutzrechtliche Bewertung

Um sich ein besseres Bild von der Lage zu machen, wurde von dieser Seite eine Ortsbegehung durchgeführt.

Im Zentralarchiv wurden die Patientenunterlagen in Stehordnern, unverschlossenen Aktenschränken und in Umzugskisten gelagert. Über diesen Raum erreichte man auch Zugang zu technischen Anlagen und zu einem Lagerraum.

Ein weiterer Raum wurde als Krankenblattarchiv der Infektologie genutzt. Dort war zugleich ein Zugang zu Technikräumen, Kühlanlagen für die Tropenmedizin und zur Aufbewahrung von Forschungsunterlagen gegeben. Die Patientenakten lagerten auch hier in unverschlossenen Aktenschränken, Umzugskisten oder waren lose auf den Schränken abgelegt.

Bedingt durch die Mehrfachnutzung der Räume war von einem großen Personenkreis auszugehen, der Zugang zu den Räumlichkeiten und damit auch den Patientenakten hatte. Aus datenschutzrechtlichen Gründen (§ 12 HKHG i.V.m. § 10 HDSG) und aus Gründen der ärztlichen Schweigepflicht (§ 203 StGB) ist dies nicht zulässig. In der vorgefundenen Ausgestaltung war die Nutzung der Räume als Archiv nicht mit einem datenschutzkonformen Umgang mit Patientenunterlagen zu vereinbaren. Dies wurde dem Vorstand und dem Datenschutzbeauftragten des Klinikums mitgeteilt. Zugleich wurde darauf gedrungen, dass die aufgezeigten Mängel umgehend beseitigt werden.

3.3.6.4.3
Weitere Entwicklung

Das Klinikum hat zeitnah auf meine Vorgaben reagiert. Um die aufgezeigten Mängel zu beseitigen, wurde in den beiden Archiven jeweils ein fest verankerter Metallgitterzaun mit verschließbaren Eingängen eingezogen.

Im Zentralarchiv wurden zusätzlich Bleche als Sichtschutz angebracht, da hier einige Regale mit Akten direkt am Zaun aufgestellt sind. Die Ausgabe der Akten wird durch einen Mitarbeiter überwacht, der seinen Arbeitsplatz im Archiv hat.

Die Aktenausgabe im Krankenblattarchiv der Infektologie erfolgt künftig mittels eines Schlüssels, der auf der Station aufbewahrt wird und – gegen Unterschrift in einer Ausgabeliste – an berechtigte Personen ausgegeben wird. Da die Unterlagen ausschließlich in Aktenschränken aufbewahrt werden, ist ein Sichtschutz nicht erforderlich.

3.3.6.4.4
Nachbegehungen

Im Anschluss an die Umsetzung der Maßnahmen fanden insgesamt zwei Nachbegehungen statt. Ich konnte mir ein Bild davon machen, dass die als Archiv genutzten Bereiche nunmehr von den übrigen Bereichen abgetrennt sind.

Verbesserungsvorschläge wurden lediglich im Hinblick auf die Datensicherheit gemacht. So wird das Zentralarchiv auf seiner gesamten Deckenfläche von Versorgungsleitungen durchzogen (Wasser, Abwasser, Abluft, Heizung, Strom, IT). Da die untersten Regalböden nicht direkt auf Bodenhöhe sind, ist hier bei einem Wasserschaden keine direkte Gefahr für die Akten gegeben. Im oberen Bereich sind die Regale jedoch offen, so dass zumindest in den Bereichen, in denen Rohre mit gefahrgeneigten Funktionen liegen, die Regale so abgedeckt werden sollten, dass Flüssigkeiten nicht oder zumindest nicht direkt in die Ablagebereiche gelangen.

Des Weiteren wurde festgestellt, dass sich einzelne, gekippte Kellerfenster im Archiv nicht mehr ohne weiteres schließen lassen.

Unter dem Aspekt der Datensicherheit wurde letztlich auch darum gebeten, in eigener Zuständigkeit zu prüfen, ob der Brandschutz in beiden Archiven entsprechend gewährleistet ist.

Auch die Vorgaben zur Datensicherheit wurden in kürzester Zeit durch das Klinikum und dessen Datenschutzbeauftragten umgesetzt. Die Regale wurden nach oben hin mit Regalböden soweit wie möglich gegen Wassereinbruch gesichert und die Kippfenster wurden wieder gangbar gemacht.

Aufgrund der Begehung des Brandschutzbeauftragten hat der gesamte Archivbereich nachträglich eine flächendeckende Brandfrüherkennungsanlage (Rauchmelder) erhalten.

3.3.7 Sozialwesen

3.3.7.1
Kooperation im Sozialwesen:
Zur Bedeutung des Sozialdatenschutzes

Die Zusammenarbeit der öffentlichen Sozialverwaltung mit nicht öffentlichen Stellen, insbesondere freien Trägern im Sozialbereich, ist für das Sozialwesen prägend. Das für diese nicht öffentlichen Stellen an sich primär geltende Bundesdatenschutzgesetz wird mit Blick auf diese Zusammenarbeit durch das spezielle Datenschutzrecht des Sozialgesetzbuchs (Sozialdatenschutz) erheblich verdrängt.

3.3.7.1.1
Der Anlass

Regelmäßig erhalte ich Anfragen, sei es von Behörden, freien Trägern im Sozialbereich, aber auch von Bürgerinnen und Bürgern, die die datenschutzrechtlichen Rahmenbedingungen bei der Zusammenarbeit von öffentlicher Sozialverwaltung und nicht öffentlichen Stellen betreffen. Auf einige Datenschutzaspekte, die in meiner Beratungspraxis im Sozialwesen regelmäßig eine besondere Bedeutung spielen, möchte ich nachfolgend eingehen.

3.3.7.1.2
Datenschutzrechtliche Rahmenbedingungen

Für die öffentliche Sozialverwaltung gilt, soweit personenbezogene Daten betroffen sind, in erster Linie das speziell im SGB geregelte Sozialdatenschutzrecht (insbesondere §§ 35 SGB I, 67 ff.

SGB X). Allerdings wird im Sozialbereich nicht nur – wie sonst im Datenschutzrecht – an personenbezogene Daten angeknüpft, sondern auch an Betriebs- und Geschäftsgeheimnisse: Diese stehen Sozialdaten gleich (§ 35 Abs. 4 SGB I). Betriebs- und Geschäftsgeheimnisse sind alle betriebs- und geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben (näher hierzu bspw. Steinbach in Hauck/ Noftz, SGB I, § 35 Rdnr. 57 ff.).

Für nicht öffentliche Stellen der Sozialbranche gilt – was auch für andere nicht öffentliche Stellen außerhalb des Sozialwesens in erster Linie maßgebend ist – das BDSG. Für die Sozialpraxis am bedeutsamsten sind § 4 a BDSG (Einwilligung des Betroffenen) sowie § 28 BDSG (Datenerhebung und –verarbeitung für eigene Geschäftszwecke).

Kooperiert die öffentliche Sozialverwaltung mit nicht öffentlichen Stellen, wird das allgemeine Datenschutzrecht durch Bestimmungen des Sozialgesetzbuches regelmäßig verdrängt. Praktisch bedeutsam sind deshalb die Normen des Sozialdatenschutzes, die besagte Kooperation in ihren unterschiedlichen Formen betreffen.

Lässt bspw. eine Sozialbehörde Daten durch eine nicht-öffentliche Stelle im Auftrag verarbeiten, gilt nicht § 4 HDSG, sondern § 80 SGB X. Das hat unter anderem zur Konsequenz, dass sich der Auftragnehmer nicht – wie sonst geboten – der Kontrolle des Hessischen Datenschutzbeauftragten unterwerfen darf. Zuständig für die Kontrolle des nicht öffentlichen Auftragnehmers ist die Datenschutzaufsichtsbehörde, in deren Bundesland dieser seinen Unternehmenssitz hat (vgl. § 4 Abs. 3 HDSG einerseits, § 80 Abs. 6 S. 4 SGB X andererseits).

Liegt eine Kooperationsform außerhalb der Auftragsdatenverarbeitung vor und übermittelt die Sozialbehörde Sozialdaten an eine nicht öffentliche Stelle, so ist diese verpflichtet, das datenschutzrechtliche Sozialgeheimnis zu beachten. Insofern wird der an sich nur für die öffentliche Sozialverwaltung geltende Sozialdatenschutz auf die nicht öffentlichen Stellen ausgedehnt. Geregelt ist diese Ausdehnung in § 78 SGB X. Bei dieser Norm – so die amtliche Überschrift – geht es um die Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden.

§ 78 Abs. 1 und 2 SGB X

(1) Personen oder Stellen, ... denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind...

(2) Werden Daten an eine nicht-öffentliche Stelle übermittelt, so sind die dort beschäftigten Personen, welche diese Daten verarbeiten oder nutzen, von dieser Stelle vor, spätestens bei der Übermittlung auf die Einhaltung der Pflichten nach Absatz 1 hinzuweisen.

Neben dieser die Bedeutung des Sozialdatenschutzes auf den nicht öffentlichen Bereich erstreckenden Norm gibt es speziell im Kinder- und Jugendhilferecht (SGB VIII) eine Vorschrift, die die freien Träger auf die Orientierung am gesamten kinder- und jugendhilferechtlichen Sozialdatenschutz verpflichtet. Dies gilt für den Fall, dass Träger der öffentlichen Jugendhilfe Träger der freien Jugendhilfe in Anspruch nehmen (§ 61 Abs. 3 SGB VIII). Durch die Inanspruchnahme freier Träger soll das sozialdatenschutzrechtliche Niveau keine Einbuße erleiden.

§ 61 Abs. 3 SGB VIII

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

Wer als Träger der freien Jugendhilfe anerkannt ist, ist gesetzlich näher geregelt. Hierunter fallen insbesondere die Kirchen und Religionsgemeinschaften des öffentlichen Rechts sowie die auf Bundesebene zusammengeschlossenen Verbände der freien Wohlfahrtspflege (§ 75 SGB VIII).

Auf diese soeben skizzierten datenschutzrechtlichen Aspekte mache ich insbesondere anfragende Stellen regelmäßig aufmerksam.

3.3.7.2
Fonds „Heimerziehung in der Bundesrepublik Deutschland in den Jahren 1949 bis 1975“

Bei der Abwicklung des Fonds „Heimerziehung in der Bundesrepublik Deutschland in den Jahren 1949 bis 1975“ erleichtern datenschutzrechtliche Rahmenbedingungen die Arbeit der hessischen Anlauf- und Beratungsstellen. Inhaltlich geht es um die Entschädigung von ehemaligen Heimkindern in Hessen.

3.3.7.2.1
Der Anlass

Das Hessische Sozialministerium (HSM) hat sich an mich gewandt, um datenschutzrechtliche Fragestellungen zu erörtern, die die Umsetzung der Empfehlungen des Runden Tisches Heimkinder im Zeitraum 1949 bis 1975 betreffen. Konkret geht es um die Aufgabenwahrnehmung der für diese

Thematik zuständigen hessischen Anlauf- und Beratungsstellen, die bei den sechs hessischen Ämtern für Versorgung und Soziales errichtet wurden. Damit ehemalige Heimkinder auf ihren Antrag hin Leistungen aus dem Fonds erhalten können, ist es für die Anlauf- und Beratungsstellen mitunter nötig, Informationen seitens der Jugendämter zu erlangen. Eine große mittelhessische Kommune war jedoch zunächst nicht damit einverstanden, dass ihr Jugendamt Unterlagen an diese Stellen versendet. Vor diesem Hintergrund hat das Sozialministerium um eine Stellungnahme zu folgenden Fragestellungen gebeten:

– Dürfen Akten der Jugendämter (mit geschwärzten personenbezogenen Daten Dritter) an die hessischen Anlauf- und Beratungsstellen übersendet werden?

– Reicht die schriftliche Versicherung der Anlauf- und Beratungsstelle aus, dass die schriftliche Einwilligung des ehemaligen Heimkindes für die Übersendung seiner Jugendamtsakte vorliegt?

3.3.7.2.2
Datenschutzrechtliche Bewertung

Datenschutzrechtlich ist es zulässig, dass Aktenausschnitte im sachlich erforderlichen Umfang vom Jugendamt auf der Grundlage einer Einwilligung der den Antrag stellenden Person übermittelt werden (§§ 67b Abs. 1 Satz 1 SGB X, § 61 Abs. 1 Satz 1 SGB VIII). Deshalb dürfen Akten mit geschwärzten Daten Dritter an die Hessischen Anlauf- und Beratungsstellen übersendet werden.

Diese Stellen sind wiederum strikt an das Datenschutzrecht gebunden, haben also insbesondere die Zweckbindung der Datenübermittlung zu beachten. Diese Verpflichtung, die Zweckbindung einzuhalten, ergibt sich im vorliegenden Kontext aus §§ 78 Abs. 1 Satz 1 SGB X, 61 Abs. 1 Satz 1 SGB VIII, weil den Anlauf- und Beratungsstellen vom Jugendamt Sozialdaten übermittelt werden:

§ 78 Abs. 1 SGB X

Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind.

Zwar gehören die Versorgungsämter zur Sozialverwaltung (§ 68 Nr. 7 SGB I) und sind insoweit Stellen im Sinne von § 35 SGB I. Die dort errichteten Anlauf- und Beratungsstellen sind jedoch keine Stellen, die Aufgaben nach dem Sozialgesetzbuch wahrnehmen, demzufolge auch keine

Stellen i. S. v. § 35 SGB I und unterliegen deshalb dem in § 78 SGB X normierten Zweckbindungsgebot.

Hinsichtlich der Übermittlung von Sozialdaten seitens des Jugendamtes ist zu beachten, dass die Betroffenen hinreichend vor ihrer Einwilligung informiert werden und die Schriftform notwendig ist (§ 67b Abs. 2 SGB X).

Die Einwilligung muss dem Jugendamt aber nicht im Original vorgelegt werden, ausreichend ist vielmehr eine entsprechende schriftliche Versicherung der Anlauf- und Beratungsstelle gegenüber dem Jugendamt (§ 67d Abs. 2 S. 2 SGB X).

§ 67d Abs. 2 SGB X

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung für die Richtigkeit der Angaben in seinem Ersuchen.

Im Anschluss an meine entsprechende Stellungnahme gegenüber dem HSM fand ein Gespräch mit dem HSM und Vertretern der Kommune statt, die Anlass der Stellungnahme war. Das Resultat war, dass zukünftig datenschutzrechtlich wie oben beschrieben verfahren werden solle.

3.3.7.2.3
Weitere Entwicklung

In der Folgezeit hat das HSM meine Stellungnahme an die hessischen kommunalen Spitzenverbände versandt. Außerdem hat es angefragt, ob die Stellungnahme auch der Länder-Arbeitsgruppe, die sich mit der Umsetzung der Empfehlungen des Runden Tisches Heimkinder im Zeitraum 1949 bis 1975 befasst, zur Verfügung gestellt werden kann. Unbeschadet meines Hinweises, dass meine Stellungnahme für andere Bundesländer ohne jede rechtliche Bindung ist, bin ich damit gerne einverstanden gewesen.

Mitte 2012 ist eine umfangreiche Drucksache betreffend die Umsetzung der Leistungen des bundesweiten Fonds „Heimerziehung in der Bundesrepublik Deutschland in den Jahren 1949 bis 1975“ erschienen (BTDrucks. 17/9682 vom 18. Mai 2012).

Zusätzlich hat das HSM eine Handreichung für die hessischen Anlauf- und Beratungsstellen sowie einen Leitfaden für ehemalige Heimkinder in Hessen, beide betreffend besagte Heimerziehung, herausgegeben.

Anfang des Jahres 2013 habe ich mich beim HSM erkundigt, ob die Kooperation der Anlauf- und Beratungsstellen mit den Jugendämtern mittlerweile problemlos verlaufe, was das HSM bejahend beantwortet hat.

Mitte 2013 ist der Bericht der Bundesregierung zum Stand der Umsetzung der Empfehlungen des Runden Tisches „Heimerziehung“ sowie der Empfehlungen zur Prävention und Zukunftsgestaltung erschienen (BTDrucks. 17/13671 vom 22. Mai 2013).

Eingaben von Bürgerinnen und Bürgern zum Thema „Heimerziehung“ sind bei mir nicht eingegangen.

3.3.7.3
Dauerbrenner bei Hartz IV: Übermittlung von Sozialdaten an Vermieter

Fast schon zum Tagesgeschäft gehören Anfragen von Betroffenen, wonach das Jobcenter zur Feststellung der Kosten der Unterkunft und Heizung parallel die Vorlage des Mietvertrages und von Unterlagen zu Heiz- und Nebenkosten, als auch gleichzeitig eine vom Vermieter ausgefüllte Mietbescheinigung (meist auf einem nicht neutralen Formular der Behörde) verlange. Regelmäßig antworte ich darauf, dass ich dieses parallele Verlangen für rechtswidrig halte und es keine rechtliche Grundlage dafür gibt, die Antragstellern auferlegt, so den Sozialleistungsbezug gegenüber deren Vermietern offenbaren zu müssen.

Für die Berechnung der Hilfebedürftigkeit im Bereich des SGB II benötigen die Leistungsträger, also die Jobcenter, auch Angaben zu den Wohnverhältnissen. Dies ergibt sich aus § 22 Abs. 1 Satz 1 SGB II.

§ 22 Abs. 1 Satz 1 SGB II

Bedarfe für Unterkunft und Heizung werden in Höhe der tatsächlichen Aufwendungen anerkannt, soweit diese angemessen sind.

Betroffenen obliegen in diesem Zusammenhang Mitwirkungspflichten, die jedoch nicht grenzenlos sind.

Wenn Betroffene in einem Mietverhältnis stehen, sind für die Prüfung der Kosten der Unterkunft Angaben zum Namen und zur Anschrift des Vermieters nicht zwingend. Eine Verpflichtung, dem Leistungsträger den gesamten Mietvertrag zu offenbaren, besteht grundsätzlich nicht. Um die aktuelle Miete bzw. die Nebenkosten nachzuweisen, genügt es, wenn z.B. das letzte Mieterhöhungsschreiben bzw. die Betriebskostenabrechnung vorgelegt wird.

Sollte die Vorlage des Vertrages dennoch ausdrücklich verlangt werden, so ist aus datenschutzrechtlicher Sicht darauf zu achten, nicht erforderliche Angaben zu schwärzen, um nicht Daten des Vermieters oder etwaiger Mitmieter preiszugeben.

Häufig fordern Jobcenter in Fällen beabsichtigter Neuanmietung von Wohnraum Mietbescheinigungen an. Sie gleichen nach Abschluss eines Mietvertrages die dortigen Angaben mit denen aus der Mietbescheinigung ab.

Grundsätzlich ist es nicht erforderlich, eine zusätzliche Bestätigung durch den Vermieter einzuholen. Das verwendete Formular dient offenbar als reine Arbeitshilfe für die Sachbearbeitung. Wenn die zur Beurteilung der Angemessenheit des Mietvertrages notwendigen Daten aus einem frei formulierten Schreiben des Vermieters zu entnehmen sind, ist eine zusätzliche Bescheinigung des Vermieters nicht erforderlich. Der Nachweis von Mietzahlungen kann schließlich mit Vorlage von Kontoauszügen durch den Betroffenen erfolgen.

Diese Rechtsauffassung teile ich seit Jahren regelmäßig den anfragenden Betroffenen mit. Parallel hierzu suche ich auch den direkten Kontakt zu den Jobcentern, um diese auf deren nicht datenschutzkonformes Verhalten hinzuweisen.

In meiner Rechtsauffassung sehe ich mich durch ein Urteil des Bundessozialgerichts vom 25. Januar 2012, Az. B 14 AS 65/11 bestätigt. Der Leitsatz dieses Urteils lautet: „Der Bezug von Arbeitslosengeld II ist ein Sozialdatum, dessen Offenbarung durch das Jobcenter nur zulässig ist, wenn der Leistungsbezieher eingewilligt hat oder eine gesetzliche Offenbarungsbefugnis vorliegt.“ An beiden Voraussetzungen mangelt es in den hier regelmäßig vorgetragenen Fallkonstellationen.

Abschließend ist darauf hinzuweisen, dass eine Offenbarungsbefugnis nicht aus den allgemeinen Vorschriften zur Übermittlung hergeleitet werden kann.

3.3.7.4
Eigeninitiierte Sozialdatenübermittlung eines Jobcenters an die Polizei

Durch verschiedene Jobcenter ebenso wie durch die Polizeiakademie Hessen wurde die Frage an mich herangetragen, unter welchen gesetzlichen Bestimmungen ein Jobcenter von sich aus Daten an die Polizei übermitteln könnte, wenn der Verdacht auf Sozialleistungsmissbrauch durch eine Straftat wegen Urkundenfälschung besteht. In enger Kooperation mit dem Fachbereich Kriminalitätsbekämpfung der Polizeiakademie Hessen habe ich die Voraussetzungen herausgearbeitet, unter denen eine SGB-Stelle (Jobcenter, Sozialamt o. a.) diesbezüglich initiativ werden kann. Dies wird nun landesweit durch die Polizeiakademie Hessen mitgeschult.

Bereits in meinem 33. Tätigkeitsbericht (Ziff. 5.9.2), habe ich unter dem Titel „Zusammenarbeit Sozialamt und Polizei“ die Zulässigkeit der Übermittlung von Sozialdaten an die Polizei behandelt.

Aktueller Anlass für eine nochmalige Befassung mit dem Thema sind zum einen Anfragen von Jobcentern im Berichtszeitraum zur Zulässigkeit der Sozialdatenübermittlung von diesen an die Polizei aus eigener Initiative. Zum anderen und vor allem aber die Polizeiakademie Hessen, die sich durch den dortigen Fachbereich Kriminalitätsbekämpfung mit der Frage an mich gewandt hat, wann Beschäftigte von Jobcentern oder Sozialämtern der Polizei rechtmäßig eigeninitiativ Daten zur Überprüfung zur Verfügung stellen können.

Hintergrund beider Anfragen war, dass vermehrt bei Vorsprachen in Stellen für Sozialleistungen – wie Jobcenter oder Sozialamt – bei der Prüfung vorgelegter Ausweisdokumente durch die dortigen Beschäftigten der begründete Verdacht entstehe, dass vorgelegte Dokumente gefälscht sein könnten. Diese Dokumente würden nahezu ausschließlich von ausländischen Personen bei der Beantragung von Sozialleistungen vorgelegt, sodass dann regelmäßig der Verdacht bestehe, es solle Sozialleistungsmissbrauch durch falsche oder gefälschte Urkunden, also eine Straftat, begangen werden.

Die Polizeiakademie Hessen, Fachbereich Kriminalitätsbekämpfung, bietet generell vor Ort in Sozialbehörden Schulungen an, durch die dortige Beschäftigte in die Lage versetzt werden, durch unterschiedliche Prüfungsmethoden bereits nahezu sicher selbst erkennen zu können, ob ein vorgelegtes Personalausweis- oder Passdokument echt oder gefälscht ist.

Die Polizeiakademie Hessen wollte ihr Angebot nun auf breitere Füße stellen und durch die enge Kooperation mit meinem Haus Sozialbehörden dahingehend Ängste nehmen, dass deren Einschaltung der Polizei rechtswidrig – weil ohne sozialdatenschutzrechtliche Übermittlungsgrundlage – sein könnte.

Zur Bedeutung des Sozialdatenschutzes bei der Übermittlung von Sozialdaten habe ich mich bereits in meinem 41. Tätigkeitsbericht (Ziff. 3.3.5.2: Datenübermittlung des Jobcenters an die Ausländerbehörde bei SGB II-Anträgen durch europäische Unionsbürgerinnen und -bürger) umfassend geäußert.

Eine Übermittlung von Sozialdaten ist auch in der hiesigen Fallkonstellation gemäß § 67 d Abs. 1 SGB X nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt. Die Verantwortung für die Zulässigkeit der Übermittlung trägt gem. § 67d Abs. 2 Satz 1 SGB X die übermittelnde Stelle. Vorliegend steht als Rechtsgrundlage für die selbstinitiierte Datenübermittlung § 69 Abs. 1 Nr. 1, 2. Alt. SGB X zur Verfügung.

§ 69 Abs. 1 SGB X

Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist

1. für die Erfüllung der Zwecke, für die sie erhoben worden sind oder für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach diesem Gesetzbuch oder einer solchen Aufgabe des Dritten, an den die Daten übermittelt werden, wenn er eine in § 35 des Ersten Buches genannte Stelle ist,

2. für die Durchführung eines mit der Erfüllung einer Aufgabe nach Nummer 1 zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens oder

3. für die Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen im Zusammenhang mit einem Verfahren über die Erbringung von Sozialleistungen; die Übermittlung bedarf der vorherigen Genehmigung durch die zuständige oberste Bundes- oder Landesbehörde.

§ 69 Abs. 1 Nr. 1 SGB X gestattet die Übermittlung von Sozialdaten, um eine ordnungsgemäße und reibungslose Zusammenarbeit der in § 35 Abs. 1 SGB I genannten Stellen zu ermöglichen, und beinhaltet drei Fallvarianten. Nach Abs. 1 Nr. 1 ist in dessen zweiter Fallvariante die Übermittlung von Sozialdaten zulässig für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem SGB, d.h. für die Erfüllung einer sog. Eigenaufgabe.

Als gesetzliche Aufgabe ist auch hier – vgl. vorgenannter Beitrag aus meinem 41. Tätigkeitsbericht (Ziff. 3.3.5.2) – jede Aufgabe anzusehen, die sich aus dem SGB insgesamt ergibt. Wenn ein Jobcenter bei der Prüfung vorgelegter Personalausweis- oder Passdokumente im Rahmen einer An-

tragstellung auf Sozialleistungen selbstbegründet zu dem Ergebnis kommt, dass im konkreten Einzelfall ein Verdacht auf Sozialleistungsmissbrauch durch die Vorlage gefälschter Urkunden besteht, dann kann eine Datenübermittlung an die Polizei auf die Grundlage von § 69 Abs. 1 Nr. 1, 2. Alt. SGB X gestützt werden. Eine Urkundenfälschung ist kein Kavaliersdelikt, sondern eine Straftat, die vorliegend noch zusätzlich zu Lasten der Solidargemeinschaft erhebliche finanzielle Konsequenzen und Ausweitungen haben kann.

Diese Rechtslage habe ich dem Fachbereich Kriminalitätsbekämpfung der Polizeiakademie Hessen in einer ausführlichen Stellungnahme dargelegt.

In der Folge und zum Abschluss unserer Kooperation bezüglich dieser Fragestellung habe ich an einer der ganztägigen Schulungen der Polizeiakademie Hessen von Beschäftigten einer Sozialverwaltung teilgenommen und hier die sozialdatenschutzrechtlichen Aspekte selbst nochmals mit eingebracht und verdeutlicht. Diese Schulungen werden nun mit dem Einfluss der sozialdatenschutzrechtlichen Aspekte landesweit von der Polizeiakademie Hessen angeboten und durchgeführt.

3.3.7.5
Vorlage eines ärztlichen Attestes bei der Erteilung einer Erlaubnis zur Vollzeitpflege in der Kinder- und Jugendhilfe

Bei der Erteilung einer Erlaubnis zur Vollzeitpflege für Bewerberinnen und Bewerber in der Kinder- und Jugendhilfe spielen mehrere Kriterien eine Rolle. Die Frage, ob im Rahmen der Prüfung der Erlaubniskriterien von Bewerberinnen und Bewerbern auch ein ärztliches Attest zur Vorlage beim Entscheidungsträger verlangt werden kann, ist aus datenschutzrechtlicher Sicht zu bejahen.

3.3.7.5.1
Der Anlass

Durch eine Anfrage des Landesbeauftragten für den Datenschutz Schleswig-Holstein innerhalb der Datenschutz-Aufsichtsbehörden zur bisherigen Befassung mit einem Thema aus dem Rechtsbereich der Kinder- und Jugendhilfe wurde ich auf eine mögliche Problematik aufmerksam gemacht, und zwar bei der Erteilung einer Erlaubnis zur Vollzeitpflege.

Die Rechtsgrundlage für die Erlaubnis zur Vollzeitpflege findet sich in § 44 SGB VIII.

§ 44 SGB VIII

(1) Wer ein Kind oder einen Jugendlichen über Tag und Nacht in seinem Haushalt aufnehmen will (Pflegeperson), bedarf der Erlaubnis. Einer Erlaubnis bedarf nicht, wer ein Kind oder einen Jugendlichen

1. im Rahmen von Hilfe zur Erziehung oder von Eingliederungshilfe für seelisch behinderte Kinder und Jugendliche aufgrund einer Vermittlung durch das Jugendamt,
2. als Vormund oder Pfleger im Rahmen seines Wirkungskreises,
3. als Verwandter oder Verschwägerter bis zum dritten Grad,
4. bis zur Dauer von acht Wochen,
5. im Rahmen eines Schüler- oder Jugendaustausches,
6. in Adoptionspflege (§ 1744 des Bürgerlichen Gesetzbuchs)

über Tag und Nacht aufnimmt.

(2) Die Erlaubnis ist zu versagen, wenn das Wohl des Kindes oder des Jugendlichen in der Pflegestelle nicht gewährleistet ist. § 72a Absatz 1 und 5 gilt entsprechend.

(3) Das Jugendamt soll den Erfordernissen des Einzelfalls entsprechend an Ort und Stelle überprüfen, ob die Voraussetzungen für die Erteilung der Erlaubnis weiter bestehen. Ist das Wohl des Kindes oder des Jugendlichen in der Pflegestelle gefährdet und ist die Pflegeperson nicht bereit oder in der Lage, die Gefährdung abzuwenden, so ist die Erlaubnis zurückzunehmen oder zu widerrufen.

(4) Wer ein Kind oder einen Jugendlichen in erlaubnispflichtige Familienpflege aufgenommen hat, hat das Jugendamt über wichtige Ereignisse zu unterrichten, die das Wohl des Kindes oder des Jugendlichen betreffen.

Strittig und datenschutzrechtlich zu beurteilen in der vorliegenden Anfrage war die Frage, ob von Bewerberinnen und Bewerbern um eine Erlaubnis zur Vollzeitpflege ein ärztliches Attest eingefordert werden kann (Vorlagepflicht).

3.3.7.5.2
Befragung einiger Jugendämter zur Prüfung der Zulässigkeit der Forderung

Da ich mit dieser Frage bisher noch nicht befasst war und um mir ein Bild über die im Kontext der Frage stehende Gesamtsituation machen zu können, habe ich zunächst eine Umfrage bei einigen hessischen Jugendämtern gestartet. Ich habe diese befragt, nach welchen Kriterien und welchem organisatorischen Ablauf diese ihre Entscheidung über die Erteilung einer Erlaubnis zur Vollzeitpflege in der Kinder- und Jugendhilfe treffen. Dabei sollten sich die Ämter dazu äußern, ob sie es für erforderlich halten, von den Bewerberinnen und Bewerbern ein ärztliches Attest zu verlangen, durch das die Geeignetheit oder Nichtgeeignetheit für die Durchführung einer Vollzeitpflege von Kindern bestätigt werden soll.

3.3.7.5.3
Rückmeldungen der Jugendämter

Nach der Befragung von vier Jugendämtern (je zwei in zwei kreisfreien hessischen Städten bzw. hessischen Landkreisen) zu deren Umsetzung des § 44 SGB VIII ergibt sich das Bild, dass i.d.R. für die Vollzeitpflege eine Bescheinigung eines (Haus-)Arztes verlangt wird, wonach gegen die Durchführung der Vollzeitpflege keine ärztlichen Bedenken bestehen.

Ein Jugendamtsbezirk fordert darüber hinaus, dass sich alle Pflegeelternbewerber und alle im selben Haushalt lebenden Personen ab dem 16. Lebensjahr beim dortigen Amt für Gesundheit einer Untersuchung unterziehen.

3.3.7.5.4
Ergebnisse im Detail

Jugendamt A
fordert, dass alle Pflegeelternbewerber sich beim dortigen Amt für Gesundheit einer Untersuchung unterziehen. Es wird ein Auftrag an das Amt für Gesundheit formuliert, wonach dieses eine Anamnese-, eine körperliche, eine Blutuntersuchung und ggf. weitere fachärztliche Untersuchungen sowie ein Drogenscreening und CDT *[Anmerkung: CDT ist die Abkürzung für eine Variante des Glycoproteins Transferrin und dient zum Nachweis des Alkoholmissbrauchs]* durchzuführen hat. Neben den Pflegeeltern müssen sich auch alle weiteren Familienmitglieder ab dem 16. Lebensjahr dieser Untersuchung unterziehen. Das Amt für Gesundheit teilt im Ergebnis jedoch keinerlei Dia-

gnosen mit, es erfolgt lediglich die Erklärung, ob die untersuchten Personen geeignet sind oder nicht. Diese Untersuchung wird alle fünf Jahre durchgeführt, ansonsten nur bei Verdachtsfällen.

Jugendamt B
fordert von den Antragsstellern ein Attest von deren Hausarzt, aus dem hervorgeht, dass aus ärztlicher Sicht gegen eine Tätigkeit als Vollzeitpflegeeltern keine Bedenken bestehen. Das Jugendamt nimmt selbst keinen Kontakt mit dem Hausarzt auf, das Verfahren bleibt in der Hand der Antragsteller. Bei unklarem Ergebnis der Erklärung des Hausarztes fordert das Jugendamt eine Erklärung nach amtsärztlicher Untersuchung, dass gegen eine Tätigkeit als Vollzeitpflegeltern keine Bedenken bestehen. Sollte ein Verdacht auf Alkohol- und Suchtmittelmissbrauch aufkommen, werden von den Pflegeeltern entsprechende Screenings verlangt. Falls psychische Beeinträchtigungen der Antragsteller bestehen, lässt sich das Jugendamt überdies eine Befreiung von der ärztlichen Schweigepflicht erteilen, um die im Einzelfall bestehenden Beeinträchtigungen direkt mit den Ärzten zu erörtern.

Jugendamt C
fordert die Vorlage einer Erklärung des Hausarztes. In der Erklärung bestätigt dieser, dass die Person bei ihm eingehend ärztlich untersucht wurde und dass aus medizinischer Sicht keine Bedenken gegen die Aufnahme eines Pflegekindes bestehen. Bescheinigungen hinsichtlich im selben Haushalt lebender Kinder und Jugendlichen werden nicht verlangt. In der Folge finden keine routinemäßigen Untersuchungen statt. Eine regelmäßige Schweigepflichtentbindung wird nicht gefordert – es sei denn, es gibt im Einzelfall Hinweise auf schwerwiegende Beeinträchtigungen.

Jugendamt D
ließ sich bis zu meiner Anfrage eine Bescheinigung des Hausarztes vorlegen, in der dieser bzgl. verschiedener schriftlich fixierter Merkmale bescheinigte, dass keine gesundheitlichen Bedenken bestehen. Äußerte der Arzt gesundheitliche Bedenken, hatten die Antragsteller diesen im weiteren Verfahren von der Schweigepflicht zu entbinden. Als Antwort auf meine Nachfrage nach der dortigen Praxis teilte das Jugendamt mit, sich fortan – auch auf Anregung des dortigen behördlichen Datenschutzbeauftragten – von den jeweiligen Hausärzten keine Unbedenklichkeit hinsichtlich einzelner Merkmale bescheinigen zu lassen. Stattdessen soll die Auskunft des Hausarztes auf die Ergebnisse „geeignet“ oder „es bestehen Bedenken“ beschränkt werden. Falls aus ärztlicher Sicht Bedenken bestehen, solle dies zunächst ebenfalls vom Arzt nur pauschal mitgeteilt werden. Es läge dann beim Antragsteller, ob er bei diesen Bedenken des Arztes dem Jugendamt in Form einer Schweigepflichtentbindung die Möglichkeit einräumt, sich über die Art der Einschränkung und die Auswirkungen auf ein Pflegeverhältnis ein weiteres Bild zu verschaffen.

3.3.7.5.4
Rechtliche Bewertung / Ergebnis

Meines Erachtens gibt § 44 SGB VIII für die Vollzeitpflege den Jugendämtern die Befugnis, von den Antragstellern die Vorlage eines ärztlichen Attestes zu verlangen. Aus diesem hat hervorzugehen, dass gegen eine Pflege aus ärztlicher Sicht keine Bedenken bestehen. Im Rahmen der Eignungsprüfung ist die gesundheitliche Eignung der Antragsteller ein wesentlich zu berücksichtigender Gesichtspunkt.

Es ist jedoch der Grundsatz der Datenerforderlichkeit in der Kinder- und Jugendhilfe gem. § 62 Abs. 1 SGB VIII zu beachten.

§ 62 Abs. 1 SGB VIII

Sozialdaten dürfen nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist.

Der Umfang des ärztlichen Attestes ist daher zu begrenzen. Die generelle Mitteilung des Arztes an das Jugendamt, seit wann der Antragsteller bei ihm in Behandlung ist und welche konkreten schwerwiegenden Erkrankungen (psychisch, physisch, Sucht, Infektionen) vorliegen, sind in dieser Pauschalität nicht erforderlich. Für die Jugendämter reicht zunächst die Information „geeignet“ oder „es bestehen Bedenken“ aus, um weitere Verfahrensschritte im Antragsverfahren zu unternehmen. Sollten Bedenken bestehen, kann das Jugendamt mit dem Antragsteller in Kontakt treten und auf die generellen gesundheitlichen Bedenken hinweisen. Für eine weitere Überprüfung wäre dann – aber erst in diesem zweiten Schritt – eine freiwillige Schweigepflichtentbindung möglich (und auch erforderlich).

Meines Erachtens ist auch eine (aktuelle) Erklärung des Hausarztes ausreichend; einer Untersuchung durch das Gesundheitsamt bedarf es aus Erforderlichkeitsgrundsätzen nicht. Im Zweifel kennt der Hausarzt den Patienten bereits über einen längeren Zeitraum. Für eine Verpflichtung der Untersuchung beim Gesundheitsamt kann lediglich eine niedrigere Missbrauchs- oder gar Fälschungsanfälligkeit angeführt werden. Diesbezügliche etwaige Einzelfälle können aber nach meiner Auffassung keine generelle Untersuchungspflicht der Antragssteller beim Gesundheitsamt rechtfertigen. Etwaige Manipulationsanfälligkeiten können überdies i.d.R. auch schon im persönlichen Gespräch im fortdauernden Dialog zwischen Jugendamt und Bewerber durch die Ämter entdeckt werden. Überdies sollte das Verhältnis zwischen Pflegeeltern und Jugendämtern von gegenseitigem Vertrauen als Basis für jedwede Pflegeverhältnisse geprägt sein.

Hinsichtlich der Untersuchung von im selben Haushalt lebenden Personen über 16 Jahre im Zusammenhang mit der Erteilung einer Erlaubnis zur Vollzeitpflege nach § 44 SGB VIII reicht ebenfalls eine generelle Bescheinigung des Arztes, ob Bedenken bestehen oder nicht, aus. Auch hier können Bedenken alleine dadurch ermittelt werden – für einen intensiveren grundrechtlichen Eingriff durch eine Untersuchung durch das (staatliche) Gesundheitsamt fehlt es an der Erforderlich-, jedenfalls an der Verhältnismäßigkeit.

Während der Dauer des Pflegeverhältnisses halte ich vor dem Hintergrund, dass die Pflegeperson verpflichtet ist, das Jugendamt auch über schwere Krankheiten zu unterrichten, und ohnehin ein ständiger Dialog zwischen Amt und Jugendämtern besteht – eine anlasslose Untersuchungspflicht in einem bestimmten (engen) zeitlichen Rahmen für nicht angemessen.

Routinemäßige Überprüfungen der Pflegestellen ohne konkrete Hinweise sind vor dem Hintergrund des gegenseitigen Vertrauens zwischen Amt und Pflegeeltern nicht zulässig – bei entsprechenden Anhaltspunkten, die sich im fortwährenden Dialog der Beteiligten ergeben, ist dies dann freilich anders zu beurteilen.

Diese Sichtweise habe ich dem ursprünglich anfragenden Landesbeauftragten für den Datenschutz Schleswig-Holstein in einer umfangreichen Stellungnahme, ebenso wie nachrichtlich den übrigen Datenschutz-Aufsichtsbehörden der anderen Bundesländer sowie dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mitgeteilt. Auch die vier von mir befragten Jugendämter habe ich nachrichtlich entsprechend in Kenntnis gesetzt.

Den hier geschilderten Standpunkt werde ich auch anderen Jugendämtern gegenüber vertreten.

3.3.7.6
Videoaufnahmen von Kindern im Kindergarten oder in einer Kindertagesstätte

Immer wieder erreichen mich Anfragen zur Möglichkeit der Fertigung von Videoaufnahmen oder -mitschnitten von Kindern in einem Kindergarten oder in Kindertagesstätten. Die anfragenden Stellen weise ich regelmäßig darauf hin, dass dies – trotz meist bester Absichten – nicht ohne Weiteres, sondern nur mit einer vorherigen, informierten Einwilligung der Erziehungsberechtigten möglich ist.

Zuletzt wandte sich eine Gemeinde an mich, die in ihrem Gemeinde-Kindergarten den Einsatz eines iPad – auch zur Aufnahme von Fotos und Videos der Kinder – als Arbeitsmittel für die dortigen Erzieherinnen in Erwägung zog. Mit den aufgenommenen Videos sollten z.B. den Eltern dann

bestimmte Verhaltens- und Spielsituationen aufgezeigt werden. Auch die Integration der Videos in die sogenannten Entwicklungsgespräche zwischen den Erzieherinnen und den Eltern war beabsichtigt.

Ich habe der Gemeinde mitgeteilt, dass Rechtspositionen wie das „Recht am eigenen Bild“ oder das „Recht am gesprochenen Wort“, abgeleitet aus dem Persönlichkeitsrechtsschutz bei Erhebungen und Verwendungen seine Person betreffender Daten und Informationen, den Anspruch des Einzelnen auf informationelle Selbstbestimmung spiegeln.

Das „Recht am eigenen Bild“ schützt vor jeder Art der unbefugten Anfertigung, Verbreitung oder Veröffentlichung einer bildlichen Darstellung einer Person durch stoffliche Fixierung und z.B. auch vor der mittels technischer Geräte bewirkten Direktübertragung des Erscheinungsbildes. Mit anderen Worten: Auch hinsichtlich der Herstellung und Verbreitung ihrer Bilder steht Betroffenen ein Selbstbestimmungsrecht zu, nach dem regelmäßig nur sie selbst darüber zu befinden haben, ob und wie sie sich in der Öffentlichkeit oder gegenüber Dritten darstellen wollen und wer Daten – hier in Form eines Bildes oder einer Aufnahme – über sie speichert, nutzt und übermittelt.

Bereits in meinem 36. Tätigkeitsbericht (Ziff. 5.6.4, Datenschutzfragen bei der Erstellung und Behandlung von Schülerfotos) habe ich festgestellt, dass eine Schule kein Recht am Bild der Schülerinnen und Schüler besitzt und diese auch nicht die Pflicht haben, ein Foto zu dulden. Dies ist auf die hier vorliegende Anfrage entsprechend übertragbar.

Seine Grundlagen hat das Recht am eigenen Bild im Persönlichkeitsrecht der Art. 1 Abs. 1 und 2 Abs. 1 GG, in den §§ 22, 23 des Kunsturhebergesetzes (KUG) i.V.m. § 33 KUG und in § 201a StGB.

§ 22 KUG

Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, daß er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

§ 23 KUG

(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

§ 33 KUG

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen den §§ 22, 23 ein Bildnis verbreitet oder öffentlich zur Schau stellt.

(2) Die Tat wird nur auf Antrag verfolgt.

§ 201a StGB

(1) Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer eine durch eine Tat nach Absatz 1 hergestellte Bildaufnahme gebraucht oder einem Dritten zugänglich macht.

(3) Wer eine befugt hergestellte Bildaufnahme von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, wissentlich unbefugt einem Dritten zugänglich macht und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(4) Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

Das Recht am eigenen Bild ist also hinsichtlich der unbefugten Verarbeitung bzw. Veröffentlichung des Bildes einer Person strafrechtlich durch § 33 KUG geschützt, der ein in § 22 KUG enthaltenes Verbot sanktioniert. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder zur Schau gestellt werden (vgl. § 22 Abs. 1 KUG), wobei unter Bildnis – unabhängig vom eingesetzten Verfahren – jede Wiedergabe des äußeren Erscheinungsbildes einer identifizierbaren Person zu verstehen ist.

Wenn vorliegend die Eltern ihre erforderliche (vorherige) Einwilligung schriftlich verweigern, dann hat sich die Gemeinde und deren Kindergarten oder Kindertagesstätte daran zwingend zu halten. Tut sie das nicht, handelt sie widerrechtlich.

Grundsätzlich sehe ich bereits die Gestaltung eines hinreichend präzisen Einwilligungstextes in solchen Fällen als schwierig an. Eine (evtl. nur einmal beim Eintritt in den Kindergarten oder die Kindertagesstätte abgegebene) „Pauschal-Einverständniserklärung“ für die Aufnahme von Fotos und/oder Filmen des Kindes für die Dauer dessen Zugehörigkeit zum Kindergarten oder zu der Kindertagesstätte halte ich für zu unbestimmt und global – eine „informierte“ Einwilligung, die das Datenschutzrecht als Rechtsgrundlage fordert, ist den Eltern so nicht möglich.

Diese Rechtslage habe ich der Gemeinde mitgeteilt. Da hierauf keine weitere Reaktion von dieser mehr erfolgt ist, gehe ich davon aus, dass man vom Einsatz eines iPad als Arbeitsmittel für Erzieherinnen zum Zweck der Aufnahme von Fotos und/oder Videos wieder abgerückt ist und diesen verworfen hat.

3.3.8 Personalwesen

3.3.8.1
Begleitung des Projekts „Optimierung der Personalverwaltung“

Zur Erreichung des Ziels „Umstellung auf moderne elektronische Geschäftsprozesse in der Personalverwaltung unter Berücksichtigung der Einführung von Dienstleistungszentren“ hat die Landesverwaltung bereits im Jahr 2011 das Gesamtprojekt „Optimierung der Personalverwaltung“ gestartet.

Bereits in meinem 40. Tätigkeitsbericht hatte ich unter Ziff. 3.10.4 berichtet, dass die Landesverwaltung an verschiedenen Projekten zur Optimierung der Personaldatenverarbeitung arbeitet.

Das Teilprojekt “Zentralisierung der Reisekostenabrechnung” ist inzwischen soweit abgeschlossen, dass bis auf das Kultusministerium, das Ministerium des Innern und für Sport und das Ministerium für Umwelt, Energie, Landwirtschaft und Verbraucherschutz alle Ressorts produktiv gesetzt wurden.
Die Reisekosten werden zukünftig zentral bei der HBS berechnet. Die erforderlichen Daten werden von den Bediensteten selbst erfasst und elektronisch – mittels Employee Self Service (ESS) – in einem webbasierten Anwendungsprogramm zur Abrechnung an die HBS übermittelt.

Das Teilprojekt “Optimierung der landesinternen Fortbildung” hat inzwischen die Informationsplattform für Tagungsstätten bereitgestellt, auf der Informationen über die für die Fortbildungsmaßnahmen zur Verfügung stehenden Tagungsstätten abgerufen werden können. Zurzeit wird die Beschaffung von notwendigen Lizenzen sowie deren Finanzierung durch das Ministerium der Finanzen geprüft. Erst nach Klärung dieser Fragen wird entschieden, in welchem Umfang dieses Teilprojekt fortgeführt werden kann.

Im Teilprojekt “Elektronische Personalakte” wurde das Lastenheft, in dem die fachliche und technische Anforderung an eine elektronische Personalakte beschrieben wird, sowie das Scan-Konzept, in dem das initiale Scannen des Papieraktenbestandes sowie die Dokumentendigitalisierung im laufenden Tagesgeschäft beschrieben wird, erstellt. Dieses Teilprojekt befindet sich zurzeit noch in der Abstimmung und im Entscheidungsprozess.

Auch das Teilprojekt “Elektronische Bewerberplattform/eRecruting”, in dem geprüft werden soll, ob eine zentrale Plattform für Stellenausschreibungen und Ausbildungsmöglichkeiten im Internet- und Mitarbeiterportal des Landes eingeführt werden kann, die hinsichtlich des Zugangs, des Designs, der Navigation, der Information und Interaktivität modernen Ansprüchen genügt, befindet sich zurzeit noch in der Abstimmung und im Entscheidungsprozess.

In allen Projekten war ich bei der Erarbeitung der Konzepte eingebunden und konnte auf datenschutzrechtlich bedeutsame Sachverhalte hinweisen, was in allen Fällen dazu führte, dass organisatorische und inhaltliche Lösungen gefunden wurden, die datenschutzkonform sind.

Ich werde alle Projekte weiterhin eng begleiten und zur gegebenen Zeit den Einsatz der Programme und die tatsächliche programmtechnische Umsetzung der Konzepte vor Ort überprüfen.

Die Zusammenarbeit mit den Projektentwicklern war jederzeit konstruktiv und im Sinne des Datenschutzes erfolgreich.

3.3.9 Kommunale Selbstverwaltungskörperschaften

3.3.9.1
Gesetzentwurf der Fraktionen von CDU und FDP zur Änderung des Brand- und Katastrophenschutzgesetzes – Einführung einer „Bevölkerungswarndatei“

Die Aufnahme einer Vorschrift in das Brand- und Katastrophenschutzgesetz zur Erhebung von Mobilfunknummern der Bevölkerung, um diese im Brand- und Katastrophenfall frühzeitig warnen zu können, ist datenschutzrechtlich dann nicht zu beanstanden, wenn klar und eindeutig geregelt ist, wie und wo diese Daten verarbeitet werden.

Im April des Jahres haben die Fraktionen der CDU und FDP den Gesetzentwurf für ein Drittes Gesetz zur Änderung des Hessischen Brand- und Katastrophenschutzgesetzes (HBKG) (LTDrucks. 18/7251) vorgelegt. Der Innenausschuss des Hessischen Landtags hat mir Gelegenheit gegeben, mich zu dem Gesetzentwurf zu äußern.

Von datenschutzrechtlicher Bedeutung ist die beabsichtigte Einfügung der Vorschrift des § 34a, mit der eine Warnung der Bevölkerung auch durch Nachricht auf Mobilfunkendgeräte ermöglicht werden soll.

§ 34a HBKG

Die nach § 3 Abs. 1 Nr. 5 oder § 4 Abs. 1 Nr. 6 zuständigen Behörden sind zur Erfüllung ihrer Aufgaben im Brandschutz, in der Allgemeinen Hilfe und im Katastrophenschutz befugt, Warnungen der Personen, die sich zu diesem Zwecke haben registrieren lassen, Mitteilungen an Mobilfunkendgeräte zu übermitteln. Diese Warnmitteilungen können auch Verhaltensempfehlungen enthalten.

Die Ausschöpfung der technischen Möglichkeiten, die die modernen Mobilfunkendgeräte bieten, um Bürger im Falle von Katastrophen, Unglücksfällen und anderen schädigenden Ereignissen warnen zu können, ist begrüßenswert.

Da die dazu erforderlichen Kontaktdaten der Mobilfunkrufnummer und der E-Mail-Adresse erst erhoben und gespeichert werden, nachdem der Bürger sich mittels einer Kurzmitteilung (SMS) auf

eigene Veranlassung hin freiwillig registriert hat, bestehen gegen eine Erhebung und Speicherung dieser Daten grundsätzlich keine datenschutzrechtlichen Bedenken.

Nach § 7 Abs. 1 Nr. 3 HDSG ist eine Verarbeitung personenbezogener Daten zulässig, wenn der Betroffene ohne jeden Zweifel eingewilligt hat. Nach § 7 Abs. 2 S. 1 HDSG bedarf diese Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sinn und Zweck dieser Regelung ist es, dass auch aus der nicht in schriftlicher Form erfolgten Einwilligung unzweifelhaft ersichtlich ist, dass diese andere Form keinerlei Einfluss auf die Entscheidungsfreiheit des Bürgers hat. Solange die Erhebung und Speicherung der personenbezogenen Daten erst auf einen Initiativakt des Bürgers hin – die Sendung einer Kurzmitteilung an eine bestimmte Adresse – erfolgt, sehe ich darin eine unzweifelhafte Einwilligung des Bürgers zur Erhebung und Speicherung der Daten zum Zwecke der Warnung vor Katastrophen und Unglücksfällen.

Allerdings fehlte aus meiner Sicht im Gesetzentwurf die Benennung der Stelle, die die vom Bürger angegebenen personenbezogenen Daten erhebt und speichert.

Nach § 55 Abs. 1 des Gesetzes, in den lediglich ein Verweis auf die jüngste Änderung des HDSG („geändert durch Gesetz vom 20. Mai 2011; GVBl. I S. 208“) eingefügt werden soll, gelten für die Bearbeitung personenbezogener Daten die Bestimmungen des HDSG „nach Maßgabe der folgenden Vorschriften“.

Diese nachfolgenden Vorschriften enthalten jedoch lediglich Regelungen hinsichtlich der Verarbeitung personenbezogener Daten von Feuerwehrangehörigen sowie Helferinnen und Helfern (Abs. 2), der Verarbeitung personenbezogener Daten zur Erfüllung von Entschädigungsansprüchen (Abs. 3), der Verarbeitung personenbezogener Daten Angehöriger besonderer Betriebe (Abs. 4) sowie der Verarbeitung personenbezogener Daten für die Erstellung einer landesweiten Statistik für den Brandschutz oder Katastrophenschutz (Abs. 5). Eine Regelung hinsichtlich der Stelle, die die vom Bürger für den Warndienst angegeben personenbezogenen Daten erheben und speichern soll, war hingegen nicht vorgesehen.

Aus dem vorgelegten Entwurf ließ sich nicht entnehmen, ob eine Speicherung durch eine öffentliche Stelle oder einen privaten Dienstleister, der in das System eingebunden ist, erfolgen soll. Auch wurde nicht hinreichend präzise bestimmt, ob diese Daten an einer zentralen Stelle für ganz Hessen oder dezentral in den jeweils am System teilnehmenden Kommunen gespeichert werden. Bezüglich dieser Frage habe ich deshalb eine weitere gesetzliche Klarstellung für erstrebenswert gehalten. Eine solche könnte beispielsweise auch durch eine Verordnung im Zusammenhang mit einer entsprechenden Verordnungsermächtigung erfolgen.

Diese Anregung ist mit einem fachlichen Beitrag von der Landesregierung aufgegriffen worden, die folgenden Änderungsvorschlag für § 69 des HBKG gemacht hat:

§ 69 wird wie folgt geändert:

a) Als neue Nr. 5 wird eingefügt:

5. die Bestimmung der Stelle, die befugt ist, personenbezogene Daten der Personen zu erheben und zu speichern, die sich zum Zwecke ihrer Warnung haben registrieren lassen (§ 34a),

Die für den Brand- und Katastrophenschutz zuständige Ministerin oder der zuständige Minister wären dadurch ermächtigt, durch Verordnung festzulegen, welche Stelle die „Warndatei“ führt. Dadurch würde für die Personen, die sich registrieren lassen wollen, Transparenz geschaffen, wo ihre Daten verarbeitet werden. Ich erwarte von dem zuständigen Minister bzw. der zuständigen Ministerin, dass von dieser Ermächtigung dann auch Gebrauch gemacht wird.

Dieser Vorschlag ist als Änderungsantrag der Fraktionen der CDU und der FDP im Plenum eingebracht und am 19. November 2013 vom Landtag nach zweiter Lesung angenommen worden.

3.3.9.2
Veröffentlichung von Einwenderdaten im Bebauungsplanverfahren unter anderem gegenüber der Presse

Einwendungen, die im Rahmen eines Bebauungsplanverfahrens vorgetragen werden, dürfen nicht personenbezogen beraten und an die Presse weitergegeben werden.

Ein Bürger hatte sich an meine Dienststelle und parallel an die Kommunalaufsicht gewandt und sich darüber beschwert, dass die von ihm vorgetragenen Einwendungen gegen einen Bebauungsplan unter Nennung seines Namens in der lokalen Presse nachzulesen waren. Der Beschwerdeführer war Mitglied im geschäftsführenden Vorstand einer in der Stadtverordnetenversammlung vertretenen Partei. Er erhob als Privatperson im Rahmen der Offenlegung des Bebauungsplanentwurfs schriftliche Einwendungen gegen den Entwurf. In der späteren öffentlichen Beratung über den Entwurf in der Stadtverordnetenversammlung wurde wörtlich aus seinen Einwendungen zitiert und der Name des Beschwerdeführers genannt. Zusätzlich fand sich sein Name und die von ihm vorgebrachten Einwendungen auch in der lokalen Presse.

Diese namentliche Nennung des Beschwerdeführers in öffentlicher Sitzung stellt einen Verstoß gegen datenschutzrechtliche Vorschriften dar. Das HDSG erlaubt grundsätzlich nur eine anonymisierte Erörterung von Einwendungen gegen einen Bebauungsplanentwurf in öffentlicher Sitzung kommunaler Gremien.

Da der Beschwerdeführer die Einwendungen gegen den Bebauungsplanentwurf als Privatperson erhoben hat, gilt der allgemeine datenschutzrechtliche Grundsatz, wonach eine Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine dem HDSG vorgehende Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, wenn das HDSG selbst dies zulässt oder der Betroffene ohne jeden Zweifel eingewilligt hat (§ 7 Abs. 1 HSDG).

Der Beschwerdeführer hat nicht in die Nennung seines Namens in öffentlicher Sitzung eingewilligt. Das Erheben von Einwendungen im Aufstellungsverfahren eines Bebauungsplans erhält keinen Erklärungswert dahin gehend, dass in die Nennung des Namens in öffentlicher Sitzung eingewilligt wird. Vielmehr beschränkt sich der Erklärungswert zunächst auf das Erheben bauplanungsrechtlicher Einwände. Damit verbunden ist lediglich eine Einwilligung in die für die Bearbeitung der Einwände notwendige Erhebung und Speicherung der personenbezogenen Daten bei der für den Planungsprozess zuständigen Behörde. Die Nennung des Namens in öffentlicher Sitzung geht in ihrer Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung jedoch über eine bloße Erhebung und Speicherung von Daten bei der Planungsbehörde deutlich hinaus. Sie stellt einen schwereren Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, da die Nennung des Namens des Einwendenden der allgemeinen Öffentlichkeit die Möglichkeit gibt, Informationen über den Einwendenden zu erfahren, die dieser evtl. nicht der allgemeinen Öffentlichkeit zugänglich machen wollte.

Mit der Bearbeitung bauplanungsrechtlicher Einwendungen geht gerade nicht notwendig eine erforderliche namentliche Erörterung der Einwände in öffentlicher Sitzung einher. Vielmehr können Einwendungen gegen einen Bebauungsplanentwurf grundsätzlich anonymisiert diskutiert werden. Denn die vorgebrachten Einwendungen im Aufstellungsverfahren eines Bebauungsplans sind zunächst grundstücksbezogen. Folglich vermag die Erhebung der Einwendung zwar die Einwilligung in die für den Planungsprozess erforderliche Erhebung und Speicherung von Daten implizieren, eine Einwilligung in die Nennung des Namens in öffentlicher Sitzung ist damit jedoch nicht verbunden.

Weder in der HGO noch im BauGB oder im HDSG findet sich eine Rechtsvorschrift, die die Nennung des Namens einer Person, die bauplanungsrechtliche Einwendungen erhebt, in öffentlicher Beratung vorsieht oder zwingend voraussetzt. Zwar fasst nach § 52 Abs. 1 S. 1 HGO die Gemeindevertretung ihre Beschlüsse in öffentlicher Sitzung und ist der Prozess der Bauleitplanung nach

den §§ 3 ff. BauGB ein kommunikativer Prozess der sich entwickelnden Diskussion und des öffentlichen Dialogs. Beide Vorschriften setzen jedoch eine Nennung des Namens von Personen, die Einwendungen gegen die Bauleitplanung erheben, nicht voraus. Denn der Zweck dieser Vorschriften, die öffentliche und transparente Befassung mit den Einwendungen, wird in gleicher Weise durch anonymisierte Diskussion der Einwände von Grundstücksinhabern erreicht.

Eine Nennung des Namens des Einwendenden in öffentlicher Sitzung würden § 52 Abs. 1 S. 1 HGO und §§ 3 ff. BauGB nur dann zwingend voraussetzen, wenn eine inhaltliche Beschäftigung mit den Einwendungen eine Individualisierung des Einwendenden notwendig machen würde. Dies wäre der Fall, wenn die Einwendungen nur verständlich diskutiert werden könnten, wenn zugleich die Person des Einwendenden bekannt wäre, also die Einwendungen personenbezogen wären. Dies kann jedoch lediglich dann angenommen werden, wenn die Einwendungen ausschließlich nach Nennung des Namens des Einwendenden inhaltlich nachvollziehbar wären. Dass eine individuelle Zuordnung der Einwendungen im betroffenen Prozess notwendig gewesen wäre, war jedoch im mir vorgetragenen Sachverhalt nicht erkennbar.

Ich habe die Kommune aufgefordert, diese Grundsätze künftig zu beachten. Die zuständige Kommunalaufsicht hat meine Rechtsauffassung geteilt.

3.3.9.3
Erteilung von Personenstandsurkunden

Die Übersendung von Geburtsurkunden über Personen, die unter den besonderen Schutz von § 63 Abs. 2 Personenstandsgesetz fallen, darf nicht ohne nähere Identitätsprüfung erfolgen.

Benötigt man etwa für eine beabsichtigte Eheschließung eine Geburtsurkunde, so kann man diese in der Regel über verschiedene Wege bei den Standesämtern beantragen:

1. Persönlich, indem man beim Standesamt vorspricht und sich durch Personalausweis oder Reisepass ausweist.
2. Schriftlich, indem man Familienname, Geburtsname, Vorname, Geburtsdatum und das beurkundende Standesamt angibt und seine Berechtigung durch Darlegung des Verwandtschaftsverhältnisses darlegt.
3. Telefonisch: hier werden in der Regel die Daten abgefragt, die sonst schriftlich anzugeben wären.
4. Online: Über die Formularserver der Kommunen können Personenstandsurkunden auch über das Internet bestellt werden. Auch hier muss der Antragsteller die bereits unter 2. genannten Daten in das Formular eintragen.

Die Berechtigung, eine Geburtsurkunde zu beantragten, haben:

1. der Betroffene selbst
2. sein Ehegatte oder Lebenspartner
3. Kinder, Enkel, Urenkel usw. der betroffenen Person
4. Eltern, Großeltern, Urgroßeltern usw. der betroffenen Person
5. Geschwister
6. derjenige, der ein berechtigtes Interesse an der Urkunde belegen kann
7. derjenige, der eine schriftliche Vollmacht der Personen unter 1. bis 6. vorlegt.

Durch eine Eingabe bin ich darauf aufmerksam gemacht worden, dass die Fälle der Urkundenausstellung im Falle der Antragsverfahren nach Nr. 2 bis 4 dann rechtlich problematisch sind, wenn die Urkunde aufgrund gesetzlicher Vorschrift zum Schutz von Betroffenen nur an Betroffene selbst ausgegeben werden darf.

§ 63 Abs. 2 Satz 1 PStG

Sind die Vornamen einer Person auf Grund des Transsexuellengesetzes vom 10. September 1980 (BGBl. I S. 1654) geändert oder ist festgestellt worden, dass diese Person als dem anderen Geschlecht zugehörig anzusehen ist, so darf abweichend von § 62 nur der betroffenen Person selbst eine Personenstandsurkunde aus dem Geburtseintrag erteilt werden.

Der hier betroffene Personenkreis hat gesteigertes Interesse daran, dass Unbefugte keine Kenntnis über ihre Vorgeschichte erlangen. D.h. hier müssen aus meiner Sicht besondere Anforderungen an die Prüfung der Berechtigung, eine Personenstandsurkunde aus dem Geburtseintrag zu erhalten, gestellt werden. Bei einer persönlichen Abholung auf dem Standesamt können die dortigen Bediensteten sich den Personalausweis oder Reisepass der Person, die den Antrag stellt, vorlegen lassen und prüfen, ob der bzw. die Betroffene selbst die Urkunde verlangt. Bei den drei anderen Antragswegen wird – jedenfalls bei dem von mir zu prüfenden Fall – lediglich eine Plausibilitätskontrolle durchgeführt. Ein echter Identitätsnachweis wird nicht verlangt. Deshalb kann nicht ausgeschlossen werden, dass eine Geburtsurkunde auch an eine nichtberechtigte Person übersandt wird.

Zunächst habe ich das Problem mit der betroffenen Kommune erörtert, die daraufhin vorgeschlagen hat, in den Fällen des § 63 Abs. 2 PStG bei der Meldebehörde des Antragstellers rückzufragen, ob die den Antrag stellende Person dort auch tatsächlich gemeldet ist. Dies ist aus meiner Sicht zwar eine Verbesserung gegenüber dem ursprünglichen Status. Allerdings wird durch die Rückfrage bei der Meldebehörde deren Aufmerksamkeit darauf gelenkt, dass es sich um einen

§ 63er-Fall handelt. Gerade in kleineren Orten könnte dies eher kontraproduktiv für das Interesse des Antragstellers bzw. der Antragstellerin sein.

Ich habe mich deshalb an das HMDIS gewandt und folgenden Vorschlag gemacht:
In den Fällen des § 63 Abs. 2 PStG sollen Personen, die den telefonischen, schriftlichen oder elektronischen Antragsweg wählen, immer aufgefordert werden, eine Kopie ihres Personalausweises einzureichen, wobei die maschinenlesbare Zone geschwärzt werden darf. Meines Erachtens ist dies ein Fall, in dem die Forderung nach einer Ausweiskopie erforderlich ist (vgl. meinen 41. Tätigkeitsbericht, Ziff. 2.1.2), um einerseits weiterhin ein bürgerfreundliches und unbürokratisches Antragsverfahren beizubehalten und andererseits die Betroffenrechte ausreichend zu wahren.

Mit dieser Vorgehensweise wäre eine Übersendung an eine unbefugte Person weitgehend ausgeschlossen. Das Ministerium sah ebenfalls Handlungsbedarf, wollte sich aber meiner Bitte, diesen Vorschlag als Erlass an die Standesämter weiterzuleiten, nicht anschließen, sondern hat eine entsprechende Empfehlung an diese gegeben. Ich gehe davon aus, dass diese Empfehlung von den Standesämtern befolgt wird, schon um datenschutzrechtliche Beanstandungen zu vermeiden.

3.3.9.4
Meldescheine in Beherbergungsstätten

Mit dem Hotelmeldeschein dürfen nur die im Hessischen Meldegesetz genannten personenbezogenen Daten erfragt werden. Das Einverständnis in Werbemaßnahmen muss mit einer gesonderten Unterschrift bestätigt werden.

Der Kunde eines großen Frankfurter Hotels beschwerte sich bei mir darüber, dass dort bei der Anmeldung Daten erfragt würden, die über das hinausgingen, was im Hessischen Meldegesetz (HMG) geregelt ist. Nach § 27 Abs. 2 HMG werden mit den Meldescheinen folgende Daten erhoben:

1. Tag der Ankunft und den der voraussichtlichen Abreise
2. Familienname
3. gebräuchlicher Vorname
4. Tag der Geburt
5. Anschrift
6. Staatsangehörigkeit

Die Erhebung weiterer Daten sieht das Meldegesetz nicht vor. Der mir vorgelegte Meldeschein enthielt zu den o.g. Datenfeldern noch ein Feld zur Angabe der Passnummer und ein Feld „E-Mail-Adresse“. Für den Gast stellte sich das Formular so dar, dass alle Felder Pflichtfelder sind, die ausgefüllt werden müssen. Die Erhebung der E-Mail-Adresse mag zweckmäßig sein, ist aber nur auf freiwilliger Basis rechtlich zulässig. Darauf hätte hingewiesen werden müssen. Die Dokumentation der Passnummer sollte ganz unterbleiben.

Im Kleingedruckten am Ende des Meldescheins fand sich noch folgender Hinweis:

> Durch Ihre Bereitstellung von Informationen („Gastinformationen“) an das Hotel autorisieren Sie xxx Hotels & xxx Worldwide Inc. und dessen angehörige und untergeordnete Firmen (die „xxx-Gruppe“), Gastinformationen für gesetzliche, xxx-Gruppengeschäftsbezogene Zwecke zu sammeln, zu verarbeiten und zu nutzen, Ihre Gastinformationen an verschiedenen Stellen zu speichern und an diese weltweit weiterzuleiten, entweder direkt oder durch dritte Händler, wie es der xxx-Gruppe angemessen erscheint, und zwar in oder außerhalb des Landes Ihres ständigen Wohnortes, den Vereinigten Staaten von Amerika oder anderswo. Weitere Informationen über unsere Datenerfassung und -nutzung finden Sie unter der Rubrik „Privacy Statement“ auf der Website xxxhotels.com.

Damit hatte das Hotel den gesetzlich vorgeschriebenen Meldeschein mit einer Einwilligung in Werbemaßnahmen gekoppelt. Ich habe das Hotel darauf hingewiesen, dass eine derartige Koppelung rechtlich unzulässig ist und dass eine Datenverarbeitung in der oben beschriebenen Weise nur zulässig ist, wenn der Hotelgast eine gesonderte Einwilligung unterschreibt.

Die Aufforderung zur Stellungnahme und ein Bericht über vorgenommene Änderungen ist zunächst trotz zweifacher Fristsetzung ausgeblieben, so dass ich mich veranlasst gesehen habe, ein Zwangsgeld anzudrohen. Daraufhin reagierte das Hotel und legte einen geänderten Meldeschein vor. Dieser Meldeschein entspricht den melde- und datenschutzrechtlichen Anforderungen. Es wird nun deutlich zwischen Pflichtangaben und freiwilligen Angaben unterschieden. Für die Nutzung der Daten zu Werbezwecken wird eine gesonderte Einwilligung eingeholt.

3.3.9.5
Erweiterte Melderegisterauskünfte an Rechtsanwälte

Eine erweiterte Melderegisterauskunft kann auch an Rechtsanwälte nur erteilt werden, wenn das berechtigte Interesse an der Auskunft eindeutig nachgewiesen wird. Ob und welche Unterlagen hierzu vorgelegt werden müssen, ist im Einzelfall zu prüfen.

Eine Rechtsanwaltskanzlei, die sich häufig mit der Durchsetzung von Forderungen befasst, beschwerte sich darüber, dass die Erteilung erweiterter Melderegisterauskünfte durch hessische Meldeämter überwiegend restriktiv gehandhabt werde. Eine Ursache hierfür sah die Kanzlei in dem Beitrag unter Ziff. 13.1 in meinem 29. Tätigkeitsbericht aus dem Jahr 2000. Dort hatte ich mich gegen floskelhafte Auskunftsbegehren ohne Fallbezug gewandt. An dieser Rechtsauffassung halte ich fest, erlaube mir aber folgende Präzisierung:

Die damals weit verbreitete Praxis, dass Anwaltskanzleien mit dem Hinweis auf die Stellung des Anwalts als Organ der Rechtspflege ein berechtigtes Interesse an einer erweiterten Melderegisterauskunft als automatisch gegeben ansahen, führte zu dem Beitrag im 29. Tätigkeitsbericht. Aus der Rechtsstellung als Anwalt erwächst nur ein Vertretungsrecht in konkreten Rechtsangelegenheiten. Das Hessische Meldegesetz verpflichtet die Meldeämter vor der Erteilung einer erweiterten Melderegisterauskunft nach § 34 Abs. 2 HMG zu prüfen, ob schutzwürdige Interessen der gemeldeten Personen einer Auskunft entgegenstehen. Eine solche Prüfung ist den Meldeämtern nur möglich, wenn der Sachverhalt hinreichend klar und substanzhaltig geschildert wird. Hierzu kann auch die von mir geforderte Vorlage von Unterlagen gehören.

§ 34 Abs. 2 HMG

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

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

Die Meldebehörde hat Betroffene über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten; dies gilt nicht, wenn der Datenemp-

fänger ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, glaubhaft gemacht hat.

Aus datenschutzrechtlicher Sicht ist es begrüßenswert, dass Kommunen offensichtlich aufgrund dieses Tätigkeitsberichtsbeitrages ihrer Verpflichtung zur Prüfung eines berechtigten oder rechtlichen Interesses vor Erteilung einer Melderegisterauskunft sorgfältig nachkommen. Die Erteilung einer Melderegisterauskunft aufgrund eines mir von der Rechtsanwaltskanzlei vorgelegten Anforderungsschreibens an eine hessische Kommune, das Informationen zu dem vertretenen Gläubiger sowie Art und Höhe der beizutreibenden Forderungen enthielt, wäre von mir im Übrigen aus datenschutzrechtlicher Sicht nicht beanstandet worden, auch wenn keine weiteren Unterlagen beigefügt worden sind. Letztlich muss sich aber die Meldebehörde von der Rechtmäßigkeit eines Auskunftsantrages überzeugen.

Ich empfehle Einwohnermeldeämtern, sich in Zweifelsfällen vor der Erteilung/Ablehnung einer Melderegisterauskunft mit meiner Dienststelle in Verbindung zu setzen.

3.3.9.6
Angabe der Dienstbezeichnung bzw. Gehaltsgruppe auf Zahlungsanordnungen

Im Landesbereich ist die Rechtsgrundlage für die Angabe der Dienstbezeichnung bzw. Gehaltsgruppe derjenigen Personen, die Zahlungsanordnungen unterzeichnen, weggefallen. Die Abfrage dieser Angaben in Zahlungsanordnungen ist nicht mehr zulässig. Im kommunalen Bereich fehlt noch eine einheitliche abschließende Regelung.

Mitarbeiterinnen einer Kommune baten um datenschutzrechtliche Prüfung, ob die Angabe der Dienstbezeichnung bzw. der Gehaltsgruppe auf Zahlungsanordnungen auch heute noch erforderlich und damit datenschutzrechtlich zulässig ist. Die in der Kommune verwendeten Formulare forderten diese Angaben von den Unterzeichnern.

Jahrzehnte währende Praxis wird selten hinterfragt. Dennoch bat ich das Referat Grundsatzfragen des Hessischen Finanzministeriums um Unterstützung bei der rechtlichen Überprüfung, da ich Zweifel an der Erforderlichkeit der Angaben hatte. Dabei wurde festgestellt, dass die Angabe der Dienstbezeichnung bzw. Gehaltsgruppe früher erforderlich war, weil nur Bediensteten ab einer bestimmten Besoldungs- oder Vergütungsgruppe zur Unterzeichnung von Zahlungsanordnungen berechtigt waren. Im Zusammenhang mit der Einführung der doppelten Buchführung in Hessen wurden die Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung zu den §§ 70 bis 72 und 74 bis 80 LHO 2007 erneuert, und hierbei ist die Vorschrift zur Nennung von

Dienstbezeichnung bzw. Vergütungsgruppe auf einer Zahlungsanordnung für die hessische Landesverwaltung weggefallen. Dies gilt sowohl für automatisierte Verfahren als auch für die Papierform von Zahlungsanordnungen. Nach einer Ressortabstimmung gilt diese Regelung bundesweit.

Stattdessen muss jeder Haushaltsbeauftragte in der hessischen Landesverwaltung ein Sicherheits- und Berechtigungskonzept erstellen, in dem alle haushaltsrechtlichen Befugnisse festgelegt werden. Den zuständigen Kassen werden Name, Amts- oder Dienstbezeichnung sowie eine Unterschriftenprobe aller Anordnungsberechtigten zur Verfügung gestellt. Die Angabe von Dienstbezeichnung oder Gehaltsgruppe auf einzelnen Zahlungsanordnungen hat sich damit erübrigt.

Die Regelungen der Landesverwaltung können jedoch nicht ohne weiteres auf den kommunalen Bereich übertragen werden. Nach § 11 der Verordnung über die Kassenführung der Gemeinden (GemKVO) regelt die Befugnis für die sachliche und rechnerische Feststellung sowie deren Form der Bürgermeister. Die früher geltende Verwaltungsvorschrift, die auch die Form der sachlichen und rechnerischen Feststellung im kommunalen Bereich regelte, ist bereits zum 31. Dezember 1997 nach den Regeln der Erlassbereinigung außer Kraft getreten und bisher nicht ersetzt worden. Informationen darüber, in welcher Weise Bürgermeister und Landräte die Befugnis zur sachlichen und rechnerischen Feststellung geregelt haben, liegen dem HMDIS nicht vor. Das Ministerium teilte mit, dass es beabsichtige, im Jahr 2013 eine neue Verwaltungsvorschrift zur GemKVO herauszugeben, da auch bei den Kommunen hierfür ein Bedarf gesehen werde. In diese Verwaltungsvorschrift solle ein Hinweis auf datenschutzrechtliche Regelungen aufgenommen werden. Bisher liegt mir noch kein Entwurf für diese Verwaltungsvorschrift zur Stellungnahme vor.

Die Mitarbeiterinnen der Kommune habe ich über die derzeit unklare Rechtslage informiert.

3.3.9.7
Stichprobenerhebung zum Einsatz von Videoüberwachung in Kommunen

Eine stichprobenartige Umfrage und anschließende Überprüfungen zum Einsatz von Videoüberwachungsanlagen haben gezeigt, dass im Zusammenhang mit den von Kommunen betriebenen Videoüberwachungen häufig die gleichen Probleme auftreten.

Über ein Jahrzehnt nach meiner letzten Umfrage zum Einsatz von Videoüberwachungsanlagen habe ich erneut eine stichprobenartige Umfrage durchgeführt. Um es vorweg zu sagen, die Videoüberwachung in Kommunen ist nicht in dem damals erwarteten Umfang angestiegen.

In diesem Jahr habe ich den Fragebogen an 57 von 426 hessischen Kommunen übersandt. Die Auswahl erfolgte nach dem Zufallsprinzip. Erfreulich war hier, dass die Fragebogen überwiegend zeitnah zurückgeschickt wurden, es waren lediglich wenige Mahnungen erforderlich.

Zehn der angeschriebenen Kommunen, also 17,5 % betreiben Videoanlagen. Zwei dieser Anlagen waren mir bereits bekannt. Die meisten der gemeldeten Videokameras sind in Schwimmbädern installiert. Aufgrund der gemeldeten Videoanlagen habe ich vier Kommunen überprüft, hierbei konnte ich im Einzelnen feststellen:

3.3.9.7.1
Videoüberwachung zur Sicherung von öffentlichen Gebäuden

Die Videoüberwachung von öffentlichen Gebäuden und öffentlichem Raum ist für hessische öffentliche Stellen nur unter den Voraussetzungen des § 14 Abs. 4 HSOG zulässig

§ 14 Abs. 4 HSOG

Die Gefahrenabwehrbehörden können mittels Bildübertragung offen beobachten und aufzeichnen:

1. zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,

2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,

3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.

Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechtes. Abs. 1 Satz 2 und 3, Abs. 3 Satz 2 und 3 sowie § 15 des Hessischen Datenschutzgesetzes gelten entsprechend.

§ 14 Abs. 4 HSOG erlaubt unter bestimmten Voraussetzungen den Videoeinsatz durch Gefahrenabwehrbehörden. Nach § 14 Abs. 4 HSOG gelten Inhaber des Hausrechts und damit auch Kommunen für kommunale Liegenschaften als öffentlich-rechtliche Gefahrenabwehrbehörden.

Nur in einer von mir überprüften Kommune wird der Außenbereich des Rathauses per Videokameras überwacht. Es werden allerdings nicht permanent Bilder aufgezeichnet. Die moderne Anlage macht es möglich, dass nur beim Betreten sogenannter Erfassungsfelder (direkter Eingangsbe-

reich des Rathauses und Umgebung des Brunnens) Videoaufnahmen ausgelöst werden. Die Bilder werden ausschließlich im PC des Administrators gespeichert und nur bei Vorkommnissen ausgewertet. Im Hinblick auf die separate Lage des Rathauses zwischen zwei Ortsteilen und immer wieder aufgetretenen Zerstörungen habe ich hier eine Videoüberwachung nach § 14 Abs. 4 Nr. 1 und 2 HSOG für zulässig gehalten. Unter datenschutzrechtlichen Gesichtspunkten ist es erfreulich, dass man auf eine permanente Bildaufzeichnung verzichtet.

In einer anderen Kommune wird der Eingangs- und Terrassenbereich eines Kulturzentrums videoüberwacht. Auch hier kam es immer wieder zu Zerstörungen, deren Folgen noch deutlich erkennbar waren. Der Vorraum des Kulturzentrums ist zwischen 8 Uhr und 18 Uhr regelmäßig zugänglich, weil sich hier auch die öffentliche Toilette des Ortes befindet. Die Kamera ist so eingestellt, dass die Toilettentüren selbst nicht beobachtet werden. Es kann lediglich festgestellt werden, wer das Gebäude betreten hat. Nach Installation der Kamera kam es zu keinen weiteren Vorfällen. Gegen die weitere Betreibung dieser Videokamera habe ich keine datenschutzrechtlichen Bedenken.

Die Terrasse dieses Kulturzentrums war ein beliebter Jugendtreff. Den regelmäßigen Verschmutzungen und Zerstörungen begegnete man zunächst mit der Installation einer ganztägig aktivierten Videokamera. Da auch diese häufiger Opfer der jugendlichen Aktivitäten wurde, hat die Gemeinde mittlerweile einen stabilen Zaun um das Außengelände des Kulturzentrums errichtet. Damit ist die installierte Videokamera nicht mehr erforderlich, ich habe ihren Abbau gefordert.

3.3.9.7.2
Videoüberwachung in Schwimmbädern

Betreiber von Schwimmbädern in Hessen haben verschiedene Rechtsformen: es gibt Schwimmbäder, die von Kommunen betrieben werden, und solche, die sich in privater Hand befinden. Für ein Schwimmbad ist die Anzahl der Besucher überlebenswichtig, alle Schwimmbäder stehen im Wettbewerb um die Besucher. Kommunale Schwimmbäder sind deshalb Wettbewerbsunternehmen. Als solche finden auf sie nach § 3 Abs. 6 HDSG die Vorschriften des BDSG Anwendung.

§ 3 Abs 6 HDSG

Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der Zweite Teil sowie §§ 34 und 36 dieses Gesetzes. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde sind im übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anwendbar.

Rechtsgrundlage für Videoüberwachungsanlagen von Kommunen in Schwimmbädern ist deshalb § 3 Abs. 6 HDSG i.V.m. § 6b BDSG.

§ 6b BDSG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Eine Beobachtung öffentlich zugänglicher Räume mit Videotechnik ist gemäß § 6b Abs. 1 BDSG zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkrete Zwecke zulässig. Hierbei dürfen keine schutzwürdigen Interessen der Betroffenen überwiegen.

Von acht Kommunen wurden mir Videoüberwachungsanlagen in Schwimmbädern gemeldet. In einigen Schwimmbädern werden hierbei nur Technikräume wie z.B. eine Chlordosieranlage über-

wacht. Diese Räume sind nicht öffentlich zugänglich und fallen damit nicht unter die Bestimmungen des § 6b BDSG. In anderen Schwimmbädern wird das Außengelände nur außerhalb der Öffnungszeiten durch Videokameras gesichert. In diesen Zeiten sind umzäunte und verschlossene Schwimmbadbereiche ebenfalls nicht öffentlich zugänglich. Eine solche Videoüberwachung kann daher auch keine schutzwürdigen Interessen der Betroffenen verletzen.

In den von mir überprüften Schwimmbädern erfolgte darüber hinaus die Videoüberwachung in folgenden Bereichen:

Fahrradständer

Im Bereich der Fahrradständer vor einem Schwimmbad war es häufiger zu Diebstählen von Fahrrädern oder Fahrradteilen gekommen. Zur Verhinderung weiterer Diebstähle wurde eine Videokamera installiert. Eigentumsschutz kann als berechtigtes Interesse im Sinne des § 6b BDSG gewertet werden. Da sich Betroffene nur kurzfristig zum Abstellen des Fahrrades im Bereich der Fahrradständer aufhalten, halte ich einen Einsatz von Videoüberwachung in Abwägung mit dem Rechtseingriff in die schutzwürdigen Belange der betroffenen Personen für verhältnismäßig.

In dem konkreten Fall zeigte jedoch ein Blick auf den Überwachungsmonitor, dass die Kamera nicht nur die Fahrradständer, sondern auch die Straße und sogar den gegenüberliegenden Hauseingang mit erfasste. Hier habe ich gefordert, dass die Kamera zeitnah so eingestellt wird, dass dieser öffentliche Bereich nicht mehr mit überwacht wird.

Freibadgelände

Im selben Schwimmbad überwachten zwei weitere Videokameras die gesamte Fläche der Schwimmbecken, der Rutschbahn sowie die umliegenden Grünflächen. Das Gelände ist für das Aufsichtspersonal gut einsehbar, schwerwiegende Beeinträchtigungen im Schwimmbadbereich lagen nicht vor. In öffentlich zugänglichen Räumen, in denen sich Menschen länger aufhalten und miteinander kommunizieren, stellt die ständige Videoüberwachung eine erhebliche Beeinträchtigung der Persönlichkeitsrechte dar. Ein Überwachungszweck nach § 6b Nr. 3 BDSG lag hier nicht vor. Deshalb habe ich den sofortigen Abbau dieser Kameras gefordert.

Dome-Kameras

Als problematisch stellten sich auch sogenannte Dome-Kameras heraus. Zwar waren diese Kameras nicht beweglich und überwachten nur zulässige Bereiche. Da man durch die dunkle Glaskugel aber nicht erkennen kann, welche Bereiche die Kamera tatsächlich erfasst, wurde in zwei Schwimmbädern der Eindruck erweckt, dass ein Umkleidebereich bzw. eine Herrendusche von

den Kameras erfasst werden kann. Auch wenn eine Überprüfung des Monitorbildes ergeben hat, dass diese Bereiche von den Kameras nicht eingesehen werden können, muss dies auch für die Besucher eindeutig erkennbar sein. Gerade bei sensiblen Bereichen wie Umkleiden oder Duschen, die zum Kernbereich der Privatheit gehören, muss auf den ersten Blick klar erkennbar sein, dass sie nicht von der Videoüberwachung erfasst sind. Dies ist nur durch Stabkameras zu erreichen. Andere Maßnahmen wie Abkleben oder Einhausen der Kameras, die ein genaues Hinsehen erfordern, genügen hier nicht. Deshalb habe ich den Austausch der Dome-Kameras in diesem Bereich gegen Stabkameras gefordert, deren Blickwinkel eindeutig erkennbar ist.

3.3.9.7.3
Monitoring

Für einige der von mir überprüften Videoüberwachungsanlagen konnte ich die Erforderlichkeit einer Aufzeichnung der Videobilder nicht erkennen und forderte deren sofortige Abschaltung.

In einer Stadtbücherei übertrugen die installierten Kameras ihre Bilder auf einen Monitor in einem Nebenraum, in dem die Bibliotheksmitarbeiterinnen häufiger Arbeiten zu verrichten haben und so trotzdem die eigentliche Bibliothek im Auge behalten können, um bei Bedarf einzugreifen. Für eine Aufzeichnung der Kamerabilder konnte ich aber keine Erforderlichkeit erkennen, da der Diebstahl von Büchern in den seltensten Fällen zeitnah festgestellt werden kann und daher auch die Aufklärung eines eventuellen Diebstahls durch die Videoaufzeichnungen nicht möglich ist.

In einem Schwimmbad diente eine Kamera im Eingangsbereich dazu, in schwierigen Situationen den Kassenmitarbeiterinnen die Unterstützung des Schwimmmeisters zu sichern. Auch hier genügte die Übertragung der Bilder auf den Monitor in der Kabine des Schwimmmeisters, die Aufzeichnung der Videobilder wurde auf meine Intervention hin beendet.

3.3.9.7.4
Speicherdauer

Die Aufbewahrungsdauer der Videoaufzeichnungen war für fast alle überprüften Videoanlagen zu lang und umfasste meistens einen Zeitraum von einer Woche bis zu einem Jahr. Die Erforderlichkeit einer derart langen Speicherungsfrist lässt sich nicht begründen. In allen Fällen habe ich die Daten verarbeitenden Stellen aufgefordert, die Speicherdauer auf 72 Stunden zu begrenzen, ein Zeitraum, innerhalb dessen der Zweck Videoüberwachung erreicht wird.

3.3.9.7.5
Auswertung der Videoaufnahmen

Bei der Videoüberwachung ist sicherzustellen, dass der Zugriff auf die Daten nur durch Berechtigte erfolgen kann (§ 10 Abs. 2 HDSG bzw. Anlage zu § 9 Satz 1 BDSG). In allen überprüften Kommunen konnte eine Auswertung der Videoaufnahmen bei Vorkommnissen nur vom jeweiligen Administrator veranlasst werden, weitere Personen hatten keine Möglichkeit, auf die Videobilder zuzugreifen. In einem Schwimmbad befand sich der entsprechende PC allerdings in einem Abstellraum mit Gartengeräten, zu dem mehrere Personen einen Schlüssel haben. Nach einer Wartungsarbeit am PC wurde vergessen, den Passwortschutz wieder zu aktivieren. Mir wurde sofortige Abhilfe zugesagt.

3.3.9.7.6
Hinweisschilder

Mit Hinweisschildern sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen deutlich erkennbar zu machen, da nach § 14 HSOG bzw. § 6b BDSG nur eine offene Videoüberwachung zulässig ist.

Einige Kommunen hatten offenbar erkannt, dass Videoüberwachungen keine Straftaten verhindern können, sie jedoch durchaus abschreckende Wirkung haben. Hier waren häufig mehr Hinweisschilder angebracht, als sie von mir gefordert worden wären. Bei anderen Kommunen mussten weitere Hinweisschilder gefordert werden, da nicht von allen Seiten beim Betreten der überwachten Bereiche ein Hinweis erfolgte. In einem Schwimmbad waren die Schilder zwar groß, aber weit über Augenhöhe angebracht, um sie vor Beschädigungen zu schützen. Hier habe ich gefordert, dass im Kassenbereich ein zusätzliches Schild in Augenhöhe angebracht wird.

Die wenigsten Hinweisschilder enthielten einen Hinweis auf einen für die Videoaufzeichnung verantwortlichen Ansprechpartner. Ich verlangte eine entsprechende Ergänzung der Piktogramme oder Schilder.

In einer Kommune wurde auf den Hinweisschildern das Überwachungsunternehmen als Ansprechpartner genannt, das für die Überwachung des Außenbereichs außerhalb der Öffnungszeiten zuständig war. Die Einschaltung eines Überwachungsunternehmens in diesem Kontext ist eine Auftragsdatenverarbeitung. Verantwortlich und damit auch auskunftspflichtig bleibt jedoch nach § 4

Abs. 1 HDSG die Daten verarbeitende Stelle, also die Kommune. Die Schilder müssen entsprechend geändert werden.

Diese Erfahrungen zeigen, dass Videoüberwachungsanlagen mich sicher auch die nächsten Jahre weiter beschäftigen werden. Im Hinblick auf die oft nicht unerheblichen Investitionskosten ist eine vorherige Abstimmung solcher Maßnahmen mit dem Hessischen Datenschutzbeauftragten zu empfehlen.

3.3.10 Wirtschaftsverwaltung

3.3.10.1
Zulässigkeit massenhafter Abfragen von Eigentümerdaten aus dem Liegenschaftskataster durch Makler

Massenhafte Auskünfte über Grundstückeigentümer an Makler bzw. Unternehmen der Immobilienvermittlung und -verwertung über ganze Straßenzüge oder Ortsteile zu reinen Akquisezwecken sind datenschutzrechtlich nicht zulässig.

In letzter Zeit erreichen mich verstärkt Eingaben von Bürgern, die darlegen, dass sie von Immobilienmaklern zwecks Grundstücksakquise kontaktiert würden. Die Makler erlangen die Kontaktdaten der Grundstückseigentümer, indem sie sich entsprechende Auskünfte aus dem Liegenschaftskataster erteilen lassen. Sie nutzen diese Eigentümerangaben, um Verkaufs- und Kaufobjekte für ihre Vermittlungs-/Maklertätigkeit zu gewinnen. Die Problematik betrifft also die Berechtigung von Maklern bzw. Unternehmen der Immobilienbranche, die Eigentümerdaten aus dem Liegenschaftskataster zu Gewerbezwecken abzufragen. Die dafür maßgebliche Vorschrift ist § 16 Hessisches Vermessungs- und Geoinformationsgesetz (HVGG).

§ 16 Abs. 1 bis 3 HVGG

(1) Jede Person oder Stelle kann die Datenbanken des öffentlichen Vermessungswesens als allgemein zugängliche Quellen einsehen sowie Auskünfte oder Ausgaben daraus erhalten.

(2) Abweichend von Abs. 1 stehen die Einsicht in die Namen, die Geburtsdaten und die Anschriften der Eigentümerinnen und Eigentümer sowie entsprechende Auskünfte und Ausgaben nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben. Entsprechendes gilt für die Daten der Bevollmächtigten. Das berechtigte Interesse ist darzulegen. Die

Empfänger dürfen diese Daten nur für den Zweck nutzen, der das berechtigte Interesse begründet und zu dessen Erfüllung die betreffenden Daten übermittelt wurden. Satz 3 gilt nicht für

1. dinglich Berechtigte,
2. Behörden des Landes und kommunale Gebietskörperschaften in Erfüllung ihrer Aufgaben,
3. Öffentlich bestellte Vermessungsingenieurinnen und Vermessungsingenieure sowie Notarinnen und Notare, soweit die personenbezogenen Daten im Einzelfall zur Erfüllung ihrer Aufgaben benötigt werden.

(3) Die digitalen Datenbanken des öffentlichen Vermessungswesens sollen mittels geeigneter, öffentlich verfügbarer Telekommunikationsmittel nutzbar sein.

Zweck dieser Bestimmung ist es, den Zugang zu den Datenbanken des öffentlichen Vermessungswesens grundsätzlich für jedermann zu eröffnen. Vom Öffentlichkeitsgrundsatz sind jedoch die im Liegenschaftskataster geführten Namen, Geburtsdaten und Anschriften der Eigentümerinnen und Eigentümer sowie deren Bevollmächtigten mit Rücksicht auf ihr Recht auf informationelle Selbstbestimmung ausgenommen. Hier stehen die Einsicht in die Eigentümerdaten bzw. die entsprechenden Auskünfte nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben. Unter einem „berechtigten Interesse“ versteht man im Allgemeinen jedes sachbezogene persönliche, wissenschaftliche, statistische, historische, rechtliche und auch wirtschaftliche Interesse, das über ein allgemeines, unspezifiziertes Informationsbedürfnis oder die reine Neugierde hinausgeht. Die Darlegung des berechtigten Interesses erfordert dabei eine plausible Schilderung der Tatsachen des Antragsanlasses. In jedem Falle ist aber eine konkrete Interessenabwägung erforderlich. Generalisierende Massenauskünfte sind datenschutzrechtlich unzulässig. Dies gilt auch bei automatisierten Abfragen.

Die automatisierten Abrufe werden durch die Kataster- und Vermessungsbehörden oder durch die von dieser mit der Verarbeitung der Daten beauftragten Stelle zum Zwecke der Verwendungskontrolle gem. § 17 HVGG protokolliert. Dabei werden die Benutzerkennung, der Abrufer, Datum und Uhrzeit, der Verwendungszweck und die Ordnungsmerkmale der abgerufenen Daten erfasst. Die Protokolle werden für die Dauer eines Jahres gespeichert.

Die Teilnahme an einem automatisierten Abrufverfahren über die Namen, Geburtsdaten und Anschriften der Eigentümerinnen und Eigentümer sowie deren Bevollmächtigten bedarf der Genehmigung (§ 17 Abs. 2 HVGG). Die Genehmigung wird auf Antrag von der oberen Kataster- und Vermessungsbehörde unter den Voraussetzungen erteilt, dass die beantragende Person ein berechtigtes Interesse hat und zusichert, die Grundsätze einer ordnungsgemäßen Datenverarbeitung und das Datenschutzrecht einzuhalten. Die Genehmigung wird unter Auflagen erteilt, die zur wirk-

samen Kontrolle der Zulässigkeit der Abrufe erforderlich sind. Die Genehmigung wird widerrufen, wenn Genehmigungsvoraussetzungen wegfallen. Sie kann u.a. widerrufen werden, wenn gegen Auflagen verstoßen wird.

Die Kontrolle der oben genannten Vorgaben soll die Liegenschaftsverwaltung bei den hierfür registrierten und zugelassenen Stellen regelmäßig durchführen. Dabei soll sie einerseits die Einhaltung der mit der Genehmigungserteilung verbundenen Auflagen sowie die Zulässigkeit der Abrufe überprüfen.

Anlässlich der Eingaben habe ich geprüft, ob solche Kontrollen vorgenommen werden. Dies ist der Fall; die Liegenschaftsverwaltung nimmt ihre Kontrolltätigkeit wahr.

Das Hessische Landesamt für Bodenmanagement und Geoinformationen hat die hier thematisierten Verstöße gerügt. Dabei hat es die betreffenden Makler und Unternehmen, die quasi nach dem Gießkannenprinzip Daten abgerufen haben, also Abrufe, die nicht auf einen konkreten einzelnen Geschäftsfall bezogen waren, in besonderem Maße auf die Einhaltung der datenschutzrechtlichen Vorgaben hingewiesen. Über die Problemstellung wurden im Übrigen alle dem Landesamt nachgeordneten Ämter für Bodenmanagement informiert und angewiesen, ihre Verfahrensweisen zur Auskunftserteilung entsprechend anzupassen.

3.3.11 Rundfunk

3.3.11.1
Einmaliger Meldedatenabgleich durch den ARD ZDF Deutschlandradio Beitragsservice (vormals GEZ)

Der einmalige bundesweite Meldedatenabgleich, den der Beitragsservice von ARD ZDF und Deutschlandradio seit dem Frühjahr 2013 vornimmt, führte zu einer Reihe von Beschwerden, die allerdings unbegründet waren.

Mit Inkrafttreten des Rundfunkbeitragsstaatsvertrages am 1. Januar 2013 (Art. 1 Fünfzehnter Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge – Fünfzehnter Rundfunkänderungsstaatsvertrag, GVBl. I S. 392) ist das Finanzierungssystem des öffentlichrechtlichen Rundfunks grundlegend geändert worden. Statt der früheren geräteabhängigen Rundfunkgebühr ist jetzt für jede Wohnung und jeden Betrieb vom Inhaber ein Rundfunkbeitrag zu entrichten. Eine gesetzliche Vermutungsregelung erleichtert die Ermittlung des Beitragsschuldners, denn als Inhaber einer

Wohnung wird jede Person vermutet, die dort nach dem Melderecht gemeldet ist (§ 2 Abs. 2 S. 2 Nr. 1 RBStV).

Die Umstellung der Rundfunkfinanzierung vom Gebühren- auf ein Beitragsmodell führte auch zu einer Umbenennung der GEZ in „ARD ZDF Deutschlandradio Beitragsservice“ – eine zu ironischer Betrachtung einladende Bezeichnung für eine Einrichtung, die Zwangsbeiträge einzieht. Dabei handelt es sich – wie schon bei der GEZ – um eine nicht rechtsfähige öffentlich-rechtliche Verwaltungsgemeinschaft der Landesrundfunkanstalten, des ZDF und des Deutschlandradios, die für die Rundfunkanstalten die Rundfunkbeiträge einzieht.

Um klären zu können, für welche Wohnung kein Rundfunkbeitrag errichtet wird, erhält der Beitragsservice für den Stichtag 3. März 2013 von allen Einwohnermeldeämtern in Deutschland Angaben zu Name, Doktorgrad, Familienstand, Geburtsdatum, aktuelle und vorherige Anschrift der Haupt- und Nebenwohnungen und Tag des Einzugs aller volljährigen Personen. Insgesamt übermitteln die Einwohnermeldeämter rund 70 Millionen Datensätze. Wegen der großen Menge erfolgt die Übermittlung jedoch nicht auf einmal, sondern in vier Tranchen, aufgeteilt auf März und September 2013 und 2014. Weitergegeben werden auch die Daten von Personen, auf deren Antrag hin eine Auskunftssperre im Melderegister eingetragen wurde. Ein Widerspruch ist – anders als etliche Beschwerdeführer fälschlich meinten – nicht möglich. Die staatsvertragliche Übermittlungsvorschrift hat Vorrang vor den melderechtlichen Auskunftssperren.

Der Beitragsservice gleicht die übermittelten Daten mit den vorhandenen Bestandsdaten ab. Dazu hat er zwölf Monate Zeit, gerechnet ab dem Übermittlungszeitpunkt für jede Tranche (§ 14 Abs. 9 S. 5 i.V.m. § 11 Abs. 5 S. 2 RBStV). Wird beim Abgleich festgestellt, das ein Meldedatensatz zur Klärung der Beitragspflicht nicht oder nicht mehr benötigt wird, wird er unverzüglich gelöscht. Spätestens im September 2015 müssen somit die letzten Meldedaten aus der im September 2014 übermittelten Tranche gelöscht sein. Daten bereits beim Beitragsservice gemeldeter Personen werden schon nach sechs Wochen gelöscht. Durch die Übermittlung in Tranchen und die fortlaufende Löschung ist ausgeschlossen, dass der Beitragsservice, wie in der Berichtserstattung in den Medien und in manchen Beschwerden befürchtet, gleichsam den Datenbestand eines bundesweiten zentralen Melderegisters erhält, was in der Tat dem melderechtlichen Modell dezentraler Register zuwiderlaufen würde.

Der einmalige Meldedatenabgleich erfolgt zusätzlich zu der regelmäßigen Meldedatenübermittlung an den Beitragsservice. Die hessischen Meldeämter wie auch die Meldeämter in den anderen Bundesländern übermitteln regelmäßig bei Abmeldungen, Anmeldungen und Todesfällen den gleichen Datensatz wie beim einmaligen Meldedatenabgleich an den Beitragsservice (§ 22 Meldedatenübermittlungsverordnung). Dieser Umstand war auch einer der Gründe, warum sich die

Datenschutzbeauftragten des Bundes und der Länder im Vorfeld gegen den einmaligen Meldedatenabgleich ausgesprochen haben. Darüber hinaus stehen dem Beitragsservice noch weitere Instrumente zur Ermittlung von Beitragsschuldnern zur Verfügung: Wer Inhaber einer Wohnung ist, muss dies der zuständigen Landesrundfunkanstalt anzeigen (§ 8 RBStV), die Landesrundfunkanstalt hat einen Auskunftsanspruch gegenüber jedem Beitragsschuldner (§ 9 RBStV), sie kann zur Feststellung, ob eine Beitragspflicht besteht, personenbezogene Daten bei öffentlichen und nichtöffentlichen Stellen ohne Kenntnis der Betroffenen erheben, und sie kann die nach dem Rundfunkgebührenstaatsvertrag gespeicherten Teilnehmerdaten weiterverwenden (§ 14 Abs. 6 RBStV).

§ 14 Abs. 9 RBStV

Um einen einmaligen Abgleich zum Zwecke der Bestands- und Ersterfassung zu ermöglichen, übermittelt jede Meldebehörde für einen bundesweit einheitlichen Stichtag automatisiert innerhalb von längstens zwei Jahren ab dem Inkrafttreten dieses Staatsvertrages gegen Kostenerstattung einmalig in standardisierter Form die nachfolgenden Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt:

1. Familienname,
2. Vornamen unter Bezeichnung des Rufnamens,
3. frühere Namen,
4. Doktorgrad,
5. Familienstand,
6. Tag der Geburt,
7. gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung, und
8. Tag des Einzugs in die Wohnung.

Hat die zuständige Landesrundfunkanstalt nach dem Abgleich für eine Wohnung einen Beitragsschuldner festgestellt, hat sie die Daten der übrigen dort wohnenden Personen unverzüglich zu löschen, sobald das Beitragskonto ausgeglichen ist. Im Übrigen darf sie die Daten zur Feststellung eines Beitragsschuldners für eine Wohnung nutzen, für die bislang kein Beitragsschuldner festgestellt wurde; Satz 2 gilt entsprechend. Die Landesrundfunkanstalt darf die Daten auch zur Aktualisierung oder Ergänzung von bereits vorhandenen Teilnehmerdaten nutzen. § 11 Abs. 5 Satz 2 und 3 gilt entsprechend.

Lediglich beim Erwerb von Adressdaten privater Personen hat der Gesetzgeber dem Beitragsservice eine temporäre Beschränkung auferlegt. Die GEZ hat jährlich ca. 90 Millionen Datensätze bei Adresshändlern erworben und damit Briefaktionen durchgeführt, um Gebührenpflichtige zu ermitteln. Bis zum 31. Dezember 2014 ist den Landesrundfunkanstalten wegen der Erlaubnis zum ein-

maligen Melddatenabgleich untersagt, Adressdaten privater Personen zu erwerben (§ 14 Abs. 10 RBStV).

Der Bayerische Verfassungsgerichtshof hat am 18. April 2013 einen Antrag auf vorläufige Aussetzung des einmaligen Meldedatenabgleichs abgelehnt (Az. Vf. 8-VII-12).

4. Aufsichtsbehörde nach § 38 BDSG

4.1 Ordnungswidrigkeiten und Meldepflichten

4.1.1.
Ahndung von Datenschutzverstößen als Ordnungswidrigkeit

4.1.1.1
Überblick zu den Bußgeldverfahren im Berichtsjahr

Im Berichtsjahr wurden 34 Bußgeldverfahren abgeschlossen. Darunter waren keine, die über den Einzelfall hinaus signifikante Bedeutung hatten.

Die Anzahl der in diesem Jahr bearbeiteten Verfahren unterschied sich nicht wesentlich von der der Vorjahre. Bei der Verteilung der Verfahren auf die unterschiedlichen Bußgeldtatbestände hat es Verschiebungen gegeben.

Aus den Katalogen des § 43 Abs. 1 und 2 BDSG ergeben sich eine Vielzahl von Tatbeständen, die als Ordnungswidrigkeit geahndet werden können.

§ 43 BDSG

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,
4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,
7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,
7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,
7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,
8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,
8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,
8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,
9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,
10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder
11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,
5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt oder Meinungsforschung verarbeitet oder nutzt,
6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder
7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

Die durchgeführten Verfahren betreffen jedoch meist nur einige wenige dieser Tatbestände: Nichterfüllung von Auskunftsansprüchen, Versäumnisse im Zusammenhang mit Werbewidersprüchen sowie unbefugte Verarbeitung von Daten insbesondere im Zusammenhang der Übermittlung von Daten.

Die Anzahl der Verfahren wegen Nichterfüllung der Auskunftsverpflichtung gegenüber der Aufsichtsbehörde aus § 38 Abs. 3 BDSG ist zurückgegangen.

§ 38 Abs. 3 BDSG

Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

Dies kann auch daran liegen, dass nunmehr bei ausbleibender oder nicht zufriedenstellender Reaktion auf Auskunftsersuchen vermehrt von der Möglichkeit Gebrauch gemacht wird, ein Zwangsgeld anzudrohen bzw. festzusetzen.

§ 76 HessVwVG

(1) Wird die Verpflichtung zu einer Handlung, die ein anderer als der Pflichtige nicht vornehmen kann (unvertretbare Handlung) oder zu einer Duldung oder Unterlassung nicht oder nicht vollständig erfüllt, so kann die Vollstreckungsbehörde den Pflichtigen zu der geforderten Handlung, Duldung oder Unterlassung durch Festsetzung eines Zwangsgeldes anhalten. Auch zu einer vertretbaren Handlung kann der Pflichtige durch Festsetzung eines Zwangsgeldes angehalten werden.

(2) Das Zwangsgeld beträgt mindestens 10 und höchstens 50000 Euro.

(3) Von der erneuten Androhung einer Zwangsgeldfestsetzung kann abgesehen werden, wenn
1. die Vollstreckung eines Zwangsgeldes wirkungslos geblieben ist,
2 das erneute Zwangsgeld in gleicher Höhe festgesetzt und
3. der Pflichtige bei Androhung des ersten Zwangsgeldes auf diese Möglichkeit hingewiesen worden ist.

Dieses Vorgehen hat offensichtlich in den meisten Fällen genau die beabsichtigte Wirkung. Den Daten verarbeitenden Stellen bzw. deren Verantwortlichen wird klar, dass die Nichtbeachtung von Aufforderungen der Aufsichtsbehörde zu erheblichen Konsequenzen führen kann.

Erteilt die Daten verarbeitende Stelle dann unverzüglich und umfassend die geforderten Auskünfte, sehe ich von der Ahndung im Bußgeldverfahren ab. Anders verhält es sich allerdings dann, wenn dieselbe Stelle wiederholt nicht ihrer Auskunftspflicht nachkommt.

Erstmals habe ich in diesem Jahr Bußgelder wegen nicht erfolgter Meldung zum Verlust personenbezogener Daten gem. § 42a BDSG verhängt (s. auch Ziff. 4.1.2).

Der Bußgeldrahmen des § 43 Abs. 3 BDSG wurde wie auch schon im Vorjahr bei weitem nicht ausgeschöpft. Das höchste verhängte Bußgeld betrug 6.750,00 Euro, zugrunde lag ein Verstoß gegen § 43 Abs. 1 Nr. 3 BDSG.

Elf Verfahren lagen Verstöße gegen die Tatbestände des § 43 Abs. 1 BDSG zu Grunde. Von diesen führten drei zu einem Bußgeldbescheid, acht Verfahren habe ich eingestellt.

Verstöße gegen § 43 Abs. 2 BDSG führten zu 23 Verfahren, von denen zwei zu einem Bußgeldbescheid führten und 21 mit einer Einstellung endeten.

Insgesamt wurden Bußgelder in Höhe von 12.250 Euro verhängt.

4.1.2
Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Betroffene sowie die zuständige Aufsichtsbehörde sind bei Verlust von personenbezogenen Daten und drohenden schwerwiegenden Beeinträchtigungen durch die verantwortliche Daten verarbeitende Stelle unverzüglich zu informieren. Die Verletzung der Meldepflicht ist ein Bußgeldtatbestand. Die Meldepflicht besteht auch in Skimming-Fällen.

Im Berichtszeitraum erreichte mich eine Vielzahl von Meldungen zum Verlust von personenbezogenen Daten, schwerpunktmäßig von Bank- und Kreditkarten. Nach § 42a BDSG ist die Meldung solcher Datenverluste oder unrechtmäßigen Kenntnisnahmen an die Aufsichtsbehörde vorgeschrieben, wenn schwerwiegende Beeinträchtigungen der Rechte oder Interessen der Betroffenen drohen.

§ 42a BDSG

Stellt eine nicht-öffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in

mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

4.1.2.1
Hackerangriffe

In zwei mir bekannt gewordenen Fällen sind Unternehmen nach Hackerangriffen dieser Pflicht zur Benachrichtigung nicht nachgekommen.

Aus den Medien sowie durch Austausch der Aufsichtsbehörden untereinander (§ 38 Abs. 1 S. 4 BDSG) habe ich erfahren, dass das System eines Auftragsdatenverarbeiters aus der Touristikbranche einem Hackerangriff zum Opfer gefallen war. Aufgabe dieses Unternehmens ist es, für Reisebüros und -veranstalter die Onlinebuchungen zu verarbeiten. Zu den abhandengekommenen Daten gehörten u.a. Namen sowie Kreditkarten- und Buchungsdaten der betroffenen Personen.

Auf Nachfrage der zuständigen Aufsichtsbehörde bei dem Unternehmen teilte mir dieses die Namen der betroffenen Reisebüros und -veranstalter mit und erklärte, dass es umgehend nach Feststellung des Hackerangriffs seine Auftraggeber über diesen Vorfall informiert und auf die Meldepflicht im Sinne des § 42a BDSG hingewiesen habe.

Wie ich anhand der mir überlassenen Liste feststellen konnte, waren zwei Unternehmen ihrer Pflicht zu Meldung sowohl gegenüber der Aufsichtsbehörde als auch gegenüber den Betroffenen nicht nachgekommen. Mit diesen habe ich mich in Verbindung gesetzt.

Erst nach meiner Aufforderung zur Stellungnahme wurden sämtliche Betroffenen über den Vorfall informiert.

Wegen Verstoßes gegen die Meldepflicht nach § 42a BDSG habe ich in beiden Fällen ein Bußgeld nach § 43 Abs. 2 Nr. 7 BDSG verhängt. Bei der Festsetzung des Bußgeldes wurde entsprechend gewürdigt, dass beide Unternehmen durch den Auftragsdatenverarbeiter schriftlich auf die Pflicht zur Meldung hingewiesen wurden.

§ 43 Abs. 2 und 3 BDSG

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

....

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

4.1.2.2
Skimming

Die Voraussetzungen für die Pflicht zur Meldung nach § 42a BDSG bei Datenpannen beschäftigt mich aufgrund des in Hessen stark ausgeprägten Bankensektors auch bei sogenannten Skimming-Fällen.

Hierbei werden zumeist an Geldautomaten sowohl der Magnetstreifen als auch die PIN von Bankkarten ausgelesen und mit diesen Daten gefälschte Karten hergestellt. Mit Hilfe dieser Karten wird im Anschluss entweder direkt am Geldautomat Bargeld abgehoben oder an Kartenterminals bargeldlos gezahlt. Dies erfolgt sowohl im In- als auch im Ausland.

Das „Abgreifen“ von Bankdaten erfüllt die Voraussetzungen der Meldepflicht nach § 42a BDSG, da personenbezogene Daten zu Bank- und Kreditkartenkonten (§ 42a Abs. 1 S. 1 Nr. 4 BDSG) Dritten unrechtmäßig zur Kenntnis gelangt sind und dadurch eine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen droht.

Der Gefahr der schwerwiegenden Beeinträchtigung wird oftmals seitens der Banken das Argument entgegengebracht, dass für die aus dem Skimming entstandenen Schäden ein Versicherungsschutz bestehe. Diese Auffassung teile ich nicht.

Ausschlaggebend für die Beurteilung ist, dass die Angreifer mit der Absicht handeln, den Kontoinhaber und nicht die Bank zu schädigen. Schon aus diesem Grund droht eine schwerwiegende Beeinträchtigung im Sinne des § 42a BDSG. Auch dass jeweils Betroffene bis zum Zeitpunkt der

Aushändigung einer Ersatzkarte nicht bargeldlos bezahlen oder kein Bargeld am Geldautomaten abheben können, stellt eine schwerwiegende Beeinträchtigung im Sinne dieser Vorschrift dar und begründet daher die Pflicht zur Meldung an die Aufsichtsbehörde.

In den letzten Jahren ist ein stetiger Anstieg der Meldung nach § 42a BDSG zu verzeichnen. Daraus abzulesen, es gäbe mehr “Datenpannen“, halte ich für spekulativ. Ich gehe vielmehr davon aus, dass die Regelungen zur Meldepflicht deutlich stärker in das Bewusstsein der Daten verarbeitenden Unternehmen gerückt sind.

4.1.3
E-Mail-Versand mit offenem Verteiler – Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG

Nach § 43 Abs. 2 Nr. 1 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Der E-Mail-Versand mit offenem Verteiler fällt hierunter. Diese Ordnungswidrigkeit kann im Anwendungsbereich des BDSG mit einem Bußgeld bis zu 300.000 Euro geahndet werden.

Im Berichtsjahr hatte sich die Bußgeldstelle u.a. mit der Frage des Versands von E-Mails mit offenem Verteiler zu befassen. Gerade durch die verstärkte Nutzung des elektronischen Weges für das Versenden von Informationen, Einladungen, Schreiben und ähnlichem an mehrere bis viele Adressaten mit einer E-Mail stößt man immer häufiger auf die Frage, wo die Adressen der Mailempfänger von Massenmails einzutragen sind, um auf der datenschutzrechtlich sicheren Seite zu sein. Der E-Mail-Kopf (Header) bietet drei Headerfelder, in die die E-Mail-Adresse eingetragen werden kann. In der Regel wird das „an“-Feld dafür genutzt, den Adressaten der E-Mail dort einzutragen. Das „cc“-Feld (cc = carbon copy) ist dafür gedacht, dort die E-Mail-Adressen einzutragen, die einen „Durchschlag“ von der E-Mail erhalten sollen, und das „bcc“-Feld (bcc = blind carbon copy) bedeutet, dass die dort eingetragenen Adressaten den anderen Adressaten bzw. Empfänger der E-Mail verborgen bleiben. Bei der Versendung von E-Mails mit offenem Verteiler ist Vorsicht geboten. Entscheidet man sich bei der Versendung von E-Mails für den falschen Weg, kann dies im Falle eines Ordnungswidrigkeitenverfahrens empfindlich hohe Bußgelder und einen Imageschaden für das Unternehmen zur Folge haben.

4.1.3.1
Bußgeldtatbestand § 43 Abs. 2 Nr. 1 BDSG

Der unzulässige E-Mail-Versand mit offenem Verteiler fällt unter den Tatbestand des § 43 Abs. 2 Nr. 1 BDSG. Ordnungswidrigkeiten nach § 43 Abs. 2 Nrn. 1 bis 4 BDSG sind solche, bei denen es sich um die Verletzung von gesetzlich vorgegeben Pflichten handelt, die sich unmittelbar auf den Umgang mit personenbezogenen Daten beziehen.

Die Verwendung von offenen E-Mail-Verteilern bei der Versendung von E-Mails an mehr als eine Person kann den Tatbestand des § 43 Abs. 2 Nr. 1 BDSG erfüllen.

§ 43 Abs. 2 Nr. 1 BDSG

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet.

Von offenen E-Mail-Verteilern spricht man immer dann, wenn in dem „an“-Feld oder „cc“-Feld der E-Mail die Adressaten dieser E-Mail mit ihren E-Mail-Adressen zu sehen sind. In einem Fall, der der Bußgeldstelle vorlag, waren im Rahmen einer Werbeaktion 100 E-Mail-Adressen im „an“-Feld offen gelistet und so für jeden Empfänger dieser E-Mail sichtbar.

4.1.3.1.1
Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche Verhältnisse wie z.B. Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession etc. oder sachliche Verhältnisse (z.B. Kfz-Kennzeichen). Einzelangaben sind Informationen, die sich auf eine bestimmte Person beziehen.

E-Mail-Adressen sind solche personenbezogenen Daten i.S.d. § 3 Abs. 1 BDSG oder zumindest personenbeziehbare Daten, wenn sich die Mailadressen auf eine bestimmte Person zurückführen lassen. Zu verneinen ist das bei anonymisierten E-Mail-Adressen, die i.d.R. keinen Personenbezug haben oder sog. Funktionsadressen, wie z.B. pressestelle@xxx.de. Ebenso wird ein Personenbezug für die Fälle zu verneinen sein, in denen Mail-Adressen an einen Firmennamen ohne Personenbezug anknüpfen.

Ein weiteres personenbezogenes Datum im Zusammenhang mit dem Mailversand im offenen Verteiler ist die Tatsache, dass mit der Versendung der Mail auch weitere Informationen an den Empfänger über die übrigen Empfänger weitergegeben werden. Das kann etwa die Tatsache sein, dass der Empfänger an einem bestimmten Produkt interessiert ist, eine bestimmte Dienstleistung in Anspruch nimmt, bzw. genommen hat oder dass jemand auch an einem bestimmten (ggf. sensiblen) Thema Interesse hat (z.B. Besuch einer gesundheitlichen Beratung). Die Versendung von E-Mails mit offenem Verteiler kann also in doppelter Hinsicht datenschutzrechtlich problematisch sein.

4.1.3.1.2
Nicht allgemein zugängliche Daten

Wenn diese personenbezogenen Daten allgemein zugänglich sind, ist § 43 Abs. 2 Nr. 1 BDSG nicht anwendbar. Allgemein zugänglich sind die Daten, die von jedermann zur Kenntnis genommen werden können, ohne dass der Zugang aus Gründen des Persönlichkeitsrechts rechtlich beschränkt ist (Gola/Schomerus, BDSG, § 43, Rz. 18 m.w.N.). Allgemein zugänglich sind solche E-Mail-Adressen, die einer nicht beschränkten Zahl von Personen bekannt sind oder die jeder vernünftigen Person ohne besondere Voraussetzungen oder Anstrengung zugänglich sind (Simitis/Ehmann, § 43 Rz. 54 m.w.N.). Das sind bspw. E-Mail-Adressen, die in öffentlichen Verzeichnissen geführt werden oder sonst jedermann ohne Zugangsbeschränkung im Internet zur Verfügung stehen. Die Frage wird allerdings beim Versand mit offenem Mail-Verteiler nur insoweit Relevanz entfalten, als man ggf. daran denken könnte, die Zahl der zu beanstandenden Fälle zu reduzieren und dadurch zu einem niedrigeren Bußgeld zu kommen. Denn i.d.R. werden beim Versand von Massen-Mails, so auch im o.g. Fall, immer solche E-Mail-Adressen dabei sein, die nicht allgemein zugänglich sind.

4.1.3.1.3.
Zulässigkeit der Übermittlung

Die Übermittlung von Daten unterliegt grundsätzlich dem Verbot mit Erlaubnisvorbehalt. Das heißt, die Übermittlung ist grundsätzlich verboten, außer das BDSG oder eine andere Rechtsvorschrift erlaubt dies oder ordnet es an bzw. der Betroffene hat in die Übermittlung eingewilligt (§ 4 Abs. 1 BDSG). Das bedeutet, dass der Versand von Massen-Mails mit offenem Verteiler mit den oben geschilderten personenbezogenen oder personenbeziehbaren Daten grundsätzlich unzulässig ist, außer es liegt eine Einwilligung zu dem Vorgehen seitens des Betroffenen vor, da es keine gesetzliche Grundlage gibt.

Allein die Einwilligung in die Zusendung von Werbung reicht hierfür nicht aus. Der Betroffene müsste zudem ausdrücklich in die Übermittlung seiner Daten an einen unbekannten und für ihn unüberschaubaren weiteren Personenkreis einwilligen. Das wird i.d.R. nicht gewollt sein. Anders wird dies bspw. in einem Verein zu sehen sein, wenn E-Mails innerhalb des Mitgliederkreises versandt werden und die einzelnen Mitglieder vorab in die Weitergabe der E-Mail-Adresse, der Kontaktdaten innerhalb des Vereins, eingewilligt haben.

4.1.3.2
Verantwortliche Stelle

Zur Verantwortung für den Datenschutzverstoß kann im Bußgeldverfahren zum einen die Mitarbeiterin, der Mitarbeiter gezogen werden, die bzw. der die E-Mail offen an alle Adressaten gesendet hat.

In Betracht kommt aber auch gem. § 30 OWiG die Verhängung eines Bußgeldes gegen die juristische Person, wenn eine vertretungsberechtigte Person oder ein Organ eine Ordnungswidrigkeit begangen hat, durch die entweder Pflichten des Unternehmens verletzt worden sind oder die zur Bereicherung des Unternehmens geführt haben oder führen sollten. Über den § 9 OWiG wird der Normadressatenkreis auch auf untere Hierarchieebenen ausgeweitet. Zu der unteren Hierarchieebene zählt z.B. das mittlere Management bzw. der Abteilungs- oder Filialleiter.

4.1.3.3
Der Bußgeldrahmen

Der Bußgeldrahmen für Ordnungswidrigkeiten i.S.d. § 43 Abs. 2 BDSG ist empfindlich groß. Im Fall des § 43 Abs. 2 Nr. 1 BDSG können Bußgelder bis zu 300.000 EUR (§ 43 Abs. 2 Nr. 1 BDSG) verhängt werden. Gegenüber Unternehmen besteht zudem die Möglichkeit der Gewinnabschöpfung. Einen solchen Fall habe ich bis dato noch nicht entscheiden müssen, vor einem Präzedenzfall schrecke ich aber keinesfalls zurück.

Der weite Bußgeldrahmen bedeutet außerdem, dass man es im Zusammenhang mit Datenschutzverstößen nach § 43 Abs. 2 BDSG mit einer langen Ahndungsverjährung zu tun hat. Verstöße nach § 43 Abs. 2 BDSG verjähren nach drei Jahren (§ 31 Abs. 2 Nr. 1 OWiG).

4.1.3.4
Prävention

Um solchen Risiken aus dem Weg zu gehen, sollte man bei der Verwendung von Computer-Programmen, die ein individuelles Versenden über das Feld „an“ ermöglichen, immer auch an dem PC, von dem versendet wird, prüfen, ob die erforderlichen Programme auf dem Rechner installiert sind, richtig laufen und ob die erforderlichen Voreinstellungen getroffen wurden.

Eine weitere Lösung ist es, beim Versenden von Massen-Mails, bzw. E-Mails an mehrere Personen die Empfänger alle in das „bcc“-Feld zu setzen und die E-Mail an sich zu adressieren.

Im vorliegenden Fall hatte die Firma im Vorfeld alles versucht, den Versand der Massen-E-Mail datenschutzrechtlich sicher durchzuführen. Allerdings war auf dem Rechner, von dem die E-Mail versendet werden sollte, die vorab geprüfte und erforderliche Einstellung nicht getätigt, sodass von den zehn E-Mail-Gruppen à 100 E-Mails eine mit offenem Mailverteiler versendet wurde.

Die Firma reagierte umgehend mit Ermittlung der Sachlage, Rücksprache mit dem für sie zuständigen IT-Dienstleister und einer gesonderten Anweisung, in der auf das Vorkommnis hingewiesen wurde und eine Handlungsanweisung enthalten war. Deswegen habe ich von einer Ahndung abgesehen (§ 47 OWiG).

4.2 Querschnitt nicht öffentlicher Bereich

4.2.1
Internationale Aktion zur Prüfung von Datenschutzerklärungen

Mit den meisten Websites und Smartphone-Apps werden personenbezogene Daten von deren Nutzern erhoben. In diesem Fall müssen die Anbieter in transparenter und verständlicher Weise darüber aufklären, welche Daten sie zu welchen Zwecken erheben und wie diese verarbeitet werden.

In einer vernetzten Welt haben viele Online-Dienste wie Websites und Apps einen internationalen Hintergrund und richten sich an Nutzer in mehreren Ländern. Somit treten auch bestimmte datenschutzrechtliche Probleme weltweit in gleicher Form auf. Aus diesem Grund fand im Berichtszeitraum erstmalig eine internationale Aktion zum Datenschutz im Internet statt, an der ich zusammen mit anderen Datenschutzaufsichtsbehörden aus der ganzen Welt teilgenommen habe. Thema der

Aktion war die Transparenz der Datenerhebung und -verarbeitung durch Websites und Smartphone-Apps. So wurden von den beteiligten Behörden Websites und Apps aus aller Welt daraufhin untersucht, ob sie über Datenschutzerklärungen verfügen, ob diese leicht auffindbar, verständlich und vollständig sind und ob es einem durchschnittlichen Verbraucher mit üblichem Aufwand möglich ist, sich einen Überblick über die Datenverarbeitung durch die Anbieter zu verschaffen. Daneben sollte die Aktion das Bewusstsein der Öffentlichkeit und der Diensteanbieter für den Datenschutz schärfen und die Kooperation der Datenschutzaufsichtsbehörden auf internationaler Ebene fördern.

Ich habe im Rahmen der Aktion anhand von international abgestimmten Kriterien die Datenschutzerklärungen von Websites größerer hessischer Unternehmen überprüft. Das Ergebnis dieser Überprüfung war dabei erfreulicherweise sehr positiv. Der Großteil der untersuchten Angebote verfügt über gute bis sehr gute Datenschutzerklärungen, anhand derer die Nutzer ohne großen Aufwand herausfinden können, welche Daten die Anbieter erheben und zu welchen Zwecken sie diese nutzen. Dagegen wurden nur bei wenigen Anbietern einzelne, meist unwesentliche Defizite festgestellt. Kurioserweise fanden sich die schlechtesten Datenschutzerklärungen ausgerechnet auf den Websites einer u.a. auf IT-Recht spezialisierten Rechtsanwaltskanzlei und einer Wirtschaftsauskunftei.

Das gute Abschneiden der hessischen Websites, insbesondere im Vergleich mit den Ergebnissen der Aufsichtsbehörden aus anderen Staaten, ist sicherlich auch auf die vorhandenen gesetzlichen Vorgaben in Deutschland zurückzuführen. So sind nach § 13 Abs. 1 TMG die Anbieter von Websites und Apps dazu verpflichtet, Informationen zur Datenverarbeitung bereitzustellen.

§ 13 Abs. 1 TMG

Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG […] in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Bei der Untersuchung fiel aber bspw. auch positiv auf, dass viele Anbieter Kontaktinformationen von speziell für den Datenschutz zuständigen Mitarbeitern angeben, obwohl es dazu keine gesetz-

liche Verpflichtung gibt. Auf diese Weise können die Nutzer bei datenschutzrechtlichen Problemen oder Fragen schnell und unkompliziert einen kompetenten Ansprechpartner erreichen.

Deutlich schlechter als die Ergebnisse meiner Überprüfung fielen leider die internationalen Resultate der Aktion aus. Viele der von anderen Aufsichtsbehörden überprüften Websites und Apps hatten gar keine Datenschutzerklärung, oder diese enthielten nur allgemeine Informationen ohne konkreten Bezug zur Datenerhebung und -verarbeitung auf der jeweiligen Website bzw. bei dem dahinterstehenden Unternehmen. Besonders große Defizite gab es bei den untersuchten Smartphone-Apps. Soweit diese überhaupt über Datenschutzerklärungen verfügten, was bei einem Großteil nicht der Fall war, waren diese überwiegend nicht konkret genug oder wiesen verschiedene andere inhaltliche Mängel auf.

Grundsätzlich sollten die Anbieter von Websites und Apps eine leicht auffindbare und verständliche Datenschutzerklärung auf ihren Angeboten zur Verfügung stellen. Ein Nutzer muss dieser entnehmen können, welche Daten bei der Nutzung der Website oder der App erhoben werden und zu welchen Zwecken diese verwendet werden. Regelmäßig anzusprechen sind daher z.B. der Einsatz von Cookies oder anderen Tracking-Technologien zu Zwecken der Werbung oder der Reichweitenanalyse, die Verwendung von Social-Plugins, die Erhebung von Daten mittels Webformularen und das Speichern von Nutzungsdaten zu statistischen Zwecken. Darüber hinaus ist es wünschenswert, wenn die Datenschutzerklärung auch Informationen zur sonstigen Verarbeitung von Daten durch das hinter der Website oder App stehende Unternehmen enthält und die Kontaktdaten eines für den Datenschutz zuständigen Ansprechpartners angegeben sind.

4.2.2
Videoüberwachung nach Bundesdatenschutzgesetz

Auf den ersten Blick scheinen Schultoiletten, Bäckereien, Friseursalons, Sauna- und Umkleidebereiche in Schwimmbädern und Fitnessstudios, Gästebereiche in Restaurants, Spielzeughubschrauber, eine Stadthalle und sogar der hessische Wald keine Gemeinsamkeiten zu haben. Eine Gemeinsamkeit gibt es dennoch: Der „ Wildwuchs“ an Videoüberwachungsanlagen nimmt kontinuierlich zu.

Die Ausführungen zur Videoüberwachung im privaten Bereich in meinem 41. Tätigkeitsbericht führten zu einer nicht unbeachtlichen medialen Aufmerksamkeit und zu einem beträchtlichen Anstieg der Zahl der Eingaben. Dies ist nicht zuletzt einem gesteigerten Gefährdungsbewusstsein der Bürgerinnen und Bürger angesichts stetig zunehmender Videoüberwachung geschuldet, insbesondere vor dem Hintergrund aktueller datenschutzrechtlicher Diskussionen. Auch die zunehmende Sensi-

bilisierung der Medien für das Thema Videoüberwachung ermutigt Bürgerinnen und Bürger, mitunter flächendeckende Videoüberwachungen in nahezu allen Lebensbereichen nicht mehr einfach nur hinzunehmen, sondern sich mit einer Eingabe an mich zu wenden.

4.2.2.1
Allgemeines

Das BDSG regelt in § 6b die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung).

§ 6b BDSG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

In den meisten Fällen, die an mich herangetragen wurden, kann nach Anhörung der für die Videoüberwachung verantwortlichen Stelle durch Neuausrichtung oder Umpositionierung der Überwachungsanlagen eine Einigung zum datenschutzkonformen Betrieb erzielt werden. Ist ein datenschutzkonformer Betrieb nicht möglich, wirke ich – ggf. unter Androhung eines Zwangsgeldes – darauf hin, dass die Kamera(s) entfernt werden.

§ 3 Abs. 7 BDSG

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Nach § 38 Abs. 3 BDSG haben mir die verantwortlichen Stellen auf Verlangen die notwendigen Auskünfte zu erteilen.

§ 38 Abs. 3 BDSG

Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

Kommt eine verantwortliche Stelle dieser Verpflichtung nicht, nicht vollständig oder nicht rechtzeitig nach, stellt dies eine Ordnungswidrigkeit dar und kann nach § 43 Abs. 3 BDSG mit einer Geldbuße bis zu 50.000 Euro geahndet werden. Hiervon musste ich lediglich in Einzelfällen Gebrauch machen.

4.2.2.2
Videoüberwachung öffentlich-zugänglicher Bereiche durch Privatpersonen

War für George Orwell in dessen Roman „1984“ der Ausspruch „Big Brother is watching you!“ noch düstere Zukunftsmusik, so ist dieser „Big Brother“ heute allgegenwärtig und begegnet uns immer öfter in der eigenen Nachbarschaft.

Öffentlich zugängliche Bereiche sind solche, die nach dem Willen der rechtlichen Besitzer der Öffentlichkeit zugänglich oder gewidmet sind. So kann beispielsweise der Bereich vor einem Geschäftsgebäude in Privatbesitz sein, dennoch handelt es sich um einen öffentlich zugänglichen

Bereich, wenn sich im Erdgeschoss des Gebäudes Einzelhandelsgeschäfte, ein Friseur und ein Restaurant befinden. Auf die Eigentumsverhältnisse kommt es insoweit nicht an. Bei Wohngebäuden einschließlich Grundstücken, Kellerräumen und Tiefgaragen ist regelmäßig davon auszugehen, dass diese nicht öffentlich zugänglich sind. Diebstahl, Vandalismus, Schutz vor Einbrüchen oder das „Phantom“, das nach Mitternacht Abfälle auf dem Grundstück entsorgt und schließlich als der gute Nachbar enttarnt wird – vermeintlich gute Gründe zur Installation einer Videoüberwachungsanlage gibt es reichlich und der Fantasie sind hierbei keine Grenzen gesetzt.

Videoüberwachung zur Wahrnehmung des privaten Hausrechts soll meist präventive Zwecke verfolgen. Hierbei sollen Personen von Rechtsverstößen innerhalb des vom Hausrecht umfassten Bereichs abgehalten werden. Die Beobachtungsbefugnis des Hausrechtsinhabers reicht grundsätzlich nur bis an die Grenzen des Grundstücks. Der öffentlich zugängliche Bereich (Gehweg, Straße, Parkplatz etc.) gehört nicht zu dem vom Hausrecht umfassten Bereich. Eine Überwachung dieser Bereiche mittels Videokamera durch Privatpersonen ist daher unzulässig.

Die verantwortlichen Stellen stützen sich jedoch nicht selten – ebenfalls zu präventiven Zwecken – auf ein besonderes berechtigtes Interesse, öffentlich zugänglichen Bereich zu beobachten. Das Vorliegen berechtigter Interessen ist jedoch zu verneinen, wenn die Videoüberwachung lediglich mit dem Ziel einer allgemeinen abstrakten Gefahrenvorsorge begründet wird (z.B. „nach dem Rechten sehen“ oder „zur Abschreckung“).

Die Gefahrenabwehr im öffentlichen Raum ist aber ausschließlich Sache der Polizei oder der Gefahrenabwehrbehörden, d.h. des Inhabers des öffentlich-rechtlichen Hausrechts. Nur diese dürfen dazu im Rahmen der Vorgaben des § 14 Abs. 3 und Abs. 4 HSOG Videokameras zur Beobachtung einsetzen und Aufzeichnungen fertigen.

Sofern Betreiber von Videoanlagen sich auf § 6b Abs. 1 Nr. 3 BDSG als Zulässigkeitsgrundlage berufen, müssen sie das Bestehen einer erheblichen Gefährdungslage substantiiert, z.B. durch die Vorlage entsprechender Strafanzeigen (unter Nennung des staatsanwaltlichen Aktenzeichens), darlegen. Des Weiteren muss die Videoüberwachung geeignet sein, solche Gefahrensituationen oder Straftaten generell zu verhindern und darf nicht lediglich der Beweissicherung dienen.

Problematisch sehe ich insbesondere die wachsende Zahl sogenannter Dome-Kameras oder auch Speed-Dome-Kameras (mit Zoom-Funktion, schwenkbar um 360 Grad). Es handelt sich hierbei um Kameras in einer halbrunden, meist getönten Kuppel aus Kunststoff. Dies allein rechtfertigt die Besorgnis einer Überwachung sämtlicher aus dieser Position sichtbarer Flächen, unabhängig von der jeweiligen Ausrichtung der (Speed-)Dome-Kamera. Es muss jederzeit erkennbar sein, welcher

Bereich von einer Dome-Kamera erfasst wird, insbesondere, wenn die Dome-Kamera so installiert ist, dass sie auch öffentlich zugängliche Bereiche erfassen kann.

Werden (Speed-)Dome-Kameras eingesetzt, wo öffentlicher Bereich im Sinne des § 6b BDSG im Fokus steht oder stehen könnte, wirke ich auf deren sofortigen Abbau oder aber eine äußerliche Verkleidung hin, sodass Betroffene auf vor Überwachung geschützter Flächen jederzeit sicher sein können, nicht überwacht zu werden.

Auch Kameraattrappen sind als Geräte zur Videoüberwachung zu werten. Insoweit verweise ich auf meine Ausführungen im 41. Tätigkeitsbericht, Ziff. 4.2.1, sowie in diesem Tätigkeitsbericht unter Ziff. 4.2.3.

4.2.2.3
Videokameras als Türspion

Auch der gute, alte Türspion fällt langsam aber sicher dem digitalen Fortschritt zum Opfer. Musste man beim klassischen Türspion noch zur Tür schreiten, um durch einen Blick festzustellen, ob einer Person Einlass gewährt wird oder nicht, so liefern heute Kameras mitunter hochauflösende Bilder des Besuchers direkt auf den Computer, den Fernseher oder gar mehrere im Haus platzierte Bildschirme. Allerdings sind diese Türspion-Kameras datenschutzrechtlich nicht immer unbedenklich, insbesondere dann, wenn Dome-Kameras im Eingangsbereich eines Einfamilienhauses oder gar im Briefkasten installiert sind und deren Aufnahmen automatisiert gespeichert werden.

Eine Videokamera im Klingeltableau einer Wohnanlage erachtet der Bundesgerichtshof in seinem Urteil vom 8. April 2011 (Aktenzeichen: V ZR 210/10) als zulässig, wenn die Kamera ausschließlich durch Betätigung der Klingel aktiviert wird, eine Bildübertragung allein in die Wohnung erfolgt, bei der geklingelt wurde, die Bildübertragung nach spätestens einer Minute unterbrochen wird und die Anlage nicht das dauerhafte Aufzeichnen von Bildern ermöglicht.

Hier habe ich die Erfahrung gemacht, dass keine der verantwortlichen Stellen mutwillig Kameras auf den öffentlichen Raum ausrichten wollte, im Fokus der Kameras stand stets der Eingangsbereich des eigenen Grundstücks.

Auf mein Anraten hin wurden die Kameras erkennbar auf den Eingangsbereich des eigenen Grundstücks ausgerichtet oder durch bauliche Maßnahmen so gestaltet, dass ein datenschutzkonformer Betrieb sichergestellt ist.

4.2.2.4
Videoüberwachung in Bäckereien

Im zurückliegenden Berichtszeitraum haben sich vermehrt Angestellte und Kunden von Bäckereien an mich gewandt, die auf teils flächendeckende Videoüberwachung in Bäckereien und deren Filialen hinwiesen. Die verantwortlichen Stellen erklärten erstaunlicherweise unisono, dass Bäckereien zu sogenannten „weichen Zielen“ zählten und somit für Raubüberfälle und Diebstähle nahezu prädestiniert seien, da früh morgens meist nur eine Person in den Filialen anwesend sei. Gewiss hat

jeder Arbeitgeber das Recht und die Pflicht, sein Personal zu schützen, jedoch rechtfertigt dies nicht eine mitunter flächendeckende Videoüberwachung der Beschäftigten z.B. durch Überwachung der Verkaufstheke, in Sozialräumen oder gar in Umkleidebereichen.

Um Gefahrensituationen vorzubeugen, halte ich eine Videokamera, die von hinten über den Kopf des Personals auf den Eingangsbereich gerichtet ist, für zulässig. An Lieferanteneingängen kann eine Videokamera im Außenbereich angebracht werden, sofern ein Verstoß gegen § 6b BDSG nicht vorliegt.

In einem Fall sah ich mich gezwungen, eine Anordnung nach § 38 Abs. 5 BDSG zur Beseitigung festgestellter Verstöße gegen das BDSG zu treffen. Hierbei handelte es sich um flächendeckende Videoüberwachung des Personals, des Café-Bereichs sowie der Sozial- und Umkleideräume einer Bäckereifiliale.

§ 38 Abs. 5 BDSG

Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

Daraufhin reichte die verantwortliche Stelle Klage gegen diesen Verwaltungsakt bei dem zuständigen Verwaltungsgericht ein. Erst während der Gerichtsverhandlung vor Ort nahm die verantwortliche Stelle die Klage zurück, die streitgegenständlichen Videokameras wurden entfernt.

4.2.2.5
Flugdrohnen mit integrierter Kamera

Ein auf einem fremden Grundstück abgestürzter Quadrocopter (Spielzeugflugdrohne) mit einer hochauflösenden HD-Kamera führte bei der Grundstückeigentümerin zu datenschutzrechtlichen Bedenken hinsichtlich deren Zulässigkeit.

Diese Flugdrohnen – auch unbemannte Luftfahrtsysteme genannt – erfreuen sich zunehmender Beliebtheit, lassen sich hiermit doch exzellente Panoramaaufnahmen anfertigen oder bequem Schäden an hohen Gebäuden feststellen. Problematisch wird der Einsatz einer Flugdrohne, sobald die Aufnahmen einen Personenbezug erkennen lassen oder aber gezielt öffentlich zugängliche Bereiche aufgenommen werden. Aufgrund zunehmender Beliebtheit dieser Flugdrohnen als auch der Tatsache, dass entsprechende Einsteigermodelle für wenig Geld zu erwerben sind, erreichen mich zunehmend Eingaben besorgter Bürger, die sich durch Flugdrohnen in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt fühlen.

Leider kann die verantwortliche Stelle in den meisten Fällen nicht ausfindig gemacht werden, da die die Flugdrohnen steuernden Person oftmals weit entfernt stehen und nicht identifiziert werden können. In dem o.a. Fall konnte ein Journalist eines regionalen Fernsehsenders als verantwortliche Stelle ausgemacht werden. Bei den Aufnahmen handelte es sich jedoch ausschließlich um Panoramaaufnahmen einer Stadt, welche unter das sogenannte „Medienprivileg“ des § 41 BDSG fielen. Die Presse wurde vom Gesetzgeber im Interesse der Pressefreiheit von der Anwendung des größten Teils der Vorschriften des BDSG ausgenommen. Diese Sonderstellung besteht jedoch nur bei ausschließlich journalistisch-redaktioneller oder literarischer Verarbeitungsabsicht.

§ 41 BDSG

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,

2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,

3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

4.2.2.6
Autokameras im öffentlichen Straßenverkehr

Motiviert durch entsprechende Beiträge in Funk und Fernsehen sowie Werbeanzeigen in Zeitschriften großer Automobil-Clubs installieren immer mehr Bürgerinnen und Bürger sogenannte Autokameras an den Front- und/oder Heckscheiben ihrer Fahrzeuge und sogar auf Motorradhelmen. Es sollen hiermit die schönsten Panoramarouten im Gebirge festgehalten oder einfach nur Verkehrssünder ertappt werden. Da es sich aber auch hier um eine unzulässige Beobachtung öffentlich zugänglicher Bereiche i.S.d. § 6b BDSG handelt, wirke ich konsequent auf die Deinstallation von in Fahrzeugen angebrachten Autokameras hin. Selbst wenn hierdurch Straftaten dokumentiert werden sollten, so darf dies nicht durch einen Eingriff in hochrangige Rechtsgüter, hier in Form des Allgemeinen Persönlichkeitsrechts, unbeteiligter Dritter geschehen. Ähnlich den Flugdrohnen steigt auch hier die Nachfrage, sodass ich davon ausgehe, dass auch bezüglich der Autokameras die Zahl der Eingaben steigen wird.

4.2.2.7
Videoüberwachung durch Tierbeobachtungskameras in hessischen Wäldern

Die Videoüberwachung durch Tierbeobachtungskameras in hessischen Wäldern hatte ich bereits in meinem 41. Tätigkeitsbericht, Ziff. 4.2.6, behandelt, jedoch finden sich immer wieder Tierbeobachtungskameras in Hessens Wäldern. § 24 HForstG erlaubt in Abs. 1 S. 1 grundsätzlich jedem das Betreten des Waldes, sodass der Wald – selbst in Privateigentum – als öffentlich-zugänglicher Bereich im Sinne des § 6b BDSG zu sehen ist.

§ 24 Abs. 1 S. 1 HForstG

Jeder darf Wald zum Zwecke der Erholung betreten. Vorschriften des öffentlichen Rechts, die das Betreten des Waldes in weiterem Umfange gestatten oder die das Betreten des Waldes einschränken, bleiben unberührt.

Trotz einer mit dem HMUELV (Oberste Jagdbehörde) getroffenen und an die entsprechenden Stellen (Jagdbehörden, Landesjagdverband) bekannt gemachten Vereinbarung, unter welchen Vo-

raussetzungen Tierbeobachtungskameras in öffentlich zugänglichen Bereichen des Waldes zulässig sind, erreichen mich diesbezüglich immer wieder Eingaben. Ein flächendeckender Einsatz von Tierbeobachtungskameras ist mir bislang nicht bekannt, dennoch platzieren einzelne Jagdausübungsberechtigte Geräte noch immer an Stellen, deren Beobachtung nach § 6b BDSG unzulässig ist.

Die verantwortlichen Stellen berufen sich grundsätzlich darauf, dass ausschließlich Jagdeinrichtungen gemäß § 22 HJagdG im Fokus der Tierbeobachtungskameras stünden, welche nach § 24 Abs. 3 Nr. 3 des HForstG nicht der Öffentlichkeit gewidmet und somit auch keine öffentlich zugänglichen Bereiche seien.

§ 22 HJagdG

(1) Jagdausübungsberechtigte dürfen auf land- und forstwirtschaftlich genutzten Grundstücken besondere Anlagen wie Jagdhütten, Ansitze oder Wildfütterungen nur mit Einwilligung der Grundstückseigentümer errichten. Der Eigentümer ist zur Einwilligung verpflichtet, wenn ihm die Duldung der Anlage zugemutet werden kann und er eine angemessene Entschädigung erhält, die auf Antrag die Jagdbehörde festsetzt.

(2) Jagdeinrichtungen sind von den ehemaligen Jagdausübungsberechtigten innerhalb von sechs Monaten nach Beendigung des Pachtverhältnisses zu entfernen, falls ihre Nachfolger sie nicht übernehmen.

Für erholungssuchende Betroffene ist jedoch regelmäßig nicht ersichtlich, ob er sich im öffentlichen Bereich oder nicht öffentlichen Bereich des Waldes aufhält. Beispielsweise sind Kirrungen für Betroffene nur schwer bzw. nicht als solche zu erkennen. Ein entsprechender Rückschluss kann auch nicht daraus folgen, dass an einer Stelle im Wald vermehrt Futtermittel oder Früchte ausgelegt sind. Eine datenschutzkonforme Videoüberwachung einer Kirrung ist somit nur möglich, wenn der überwachte Bereich für die Betroffenen Waldbesucher objektiv erkennbar, räumlich abgegrenzt und gem. § 6b Abs. 2 BDSG vor dem Betreten der überwachten Fläche entsprechende Hinweise nebst Angabe der verantwortlichen Stelle angebracht sind.

4.2.3
Verhaltenssteuerung durch Attrappen von Videokameras

Anlässlich einer Beschwerde stellte ich fest, dass einige Verkehrsunternehmen in Hessen mit Fahrzeugen im öffentlichen Verkehr unterwegs sind, in denen Kamera-Attrappen installiert sind. Die Beschwerde richtete sich dagegen, dass ein Hinweis auf die Maßnahme fehlte. Dem wurde abgeholfen.

Ein Kunde eines hessischen Verkehrsunternehmens machte mich darauf aufmerksam, dass einige Fahrzeuge dieses Unternehmens mit Videokameras ausgerüstet sind, auf die aber nur in manchen Fällen durch ein Hinweisschild aufmerksam gemacht wird. In anderen Fällen fehlte das Hinweisschild. Meine Prüfung hat ergeben, dass es sich in den Fällen, in denen der Hinweis fehlte, um Attrappen handelte.

Das Problematische dabei ist, dass in diesen Fahrzeugen genaugenommen keine Datenverarbeitung stattfindet, da die Attrappen nur den Anschein einer Videoüberwachung erregen, die tatsächlich nicht stattfindet.

Diese Attrappen sind wie echte Kameras zu behandeln. Dies ergibt sich aus Folgendem:

1. Strukturell ist die Verwendung von Attrappen mit einer polizeilichen Anscheinsgefahr vergleichbar. Nach der im Polizeirecht von Rechtsprechung und Schrifttum überwiegend vertretenen Meinung ist eine Anscheinsgefahr eine echte Gefahr. Entsprechend liegt in der „Beobachtung“ durch eine nicht als solche erkennbare Attrappe ein Eingriff in die informationelle Selbst-

bestimmung. Die Passagiere verlassen sich auf den von dem Verkehrsunternehmen gesetzten Schein und gehen davon aus, dass ihre personenbezogenen Daten verarbeitet werden.

2. Weiter ist von Bedeutung, dass der Beobachtungseffekt für den unwissenden Betroffenen der Gleiche ist wie bei der echten Kamera. Auch eine Attrappe veranlasst eine Verhaltensänderung, bewirkt den äußeren Druck zur Selbstkontrolle und greift damit in das Recht auf informationelle Selbstbestimmung ein.

3. Ein Verzicht auf die Beschilderung der „Videoüberwachung“ führte zu weiteren Beschwerden. Wegen der gesetzlichen Hinweispflicht nach § 6b Abs. 2 BDSG müsste ich den Beschwerdeführern offenbaren, dass es sich bei den installierten Kameras um Attrappen handelt und deswegen gar keine Datenverarbeitung stattfindet. Dieser Umstand, kein Schild = keine Datenverarbeitung, würde sich herumsprechen und die beabsichtigte, abschreckende Wirkung zunichte machen. Anlässlich dieser absehbaren Entwicklung würde sich dann die Frage nach der Tauglichkeit der Attrappen zur Gefahrenabwehr stellen.

Aus diesen Gründen halte ich es für erforderlich, dass auch bei der Installation von Attrappen sämtliche Voraussetzungen des § 6b BDSG für die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen erfüllt sein müssen.

§ 6b Abs. 1 und 2 BDSG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

Auch der Landesgesetzgeber von Rheinland-Pfalz teilt diese Wertung und hat zur Klarstellung in § 34 Abs. 6 LDSG Rheinland-Pfalz eine Sonderregelung für die Gleichbehandlung von Attrappen getroffen.

Zu den Voraussetzungen, die nach § 6b BDSG erfüllt sein müssen, zählt auch die Kenntlichmachung. Für diese müssen bei Attrappen dieselben Anforderungen, wie beim Einsatz funktionstüchtiger Kameras erfüllt werden. Zur Vermeidung einer zusätzlichen Fiktion wurde vorgeschlagen, als Hinweisschild statt des Schildes „Achtung Videoüberwachung“ das Piktogramm einer Kamera zu wählen und die verantwortliche Stelle zu bezeichnen.

Die Fahrzeuge wurden nachgerüstet und die Beachtung meiner Rechtsauffassung für die Zukunft zugesagt. Dem Beschwerdeführer wurde mitgeteilt, dass die Beschilderung nachgeholt wurde.

4.3 Kreditinstitute und Auskunfteien

4.3.1
Aufzeichnung von Telefonanrufen bei Kreditinstituten

Mich erreichten einige Beschwerden über die Aufzeichnung von Telefonanrufen durch Kreditinstitute. In keinem Fall lag ein Verstoß gegen datenschutzrechtliche Bestimmungen vor.

Erforderlich für die Zulässigkeit der Aufzeichnung von Telefonaten ist mindestens die Information des Anrufers über die Aufzeichnung, dessen Zustimmung zur Aufzeichnung sowie eine zumutbare alternative Möglichkeit zur Kontaktaufnahme, wenn eine Aufzeichnung nicht gewollt ist.

Unterbleibt die Information über die Aufzeichnung, kommt regelmäßig die Strafbarkeit der Aufzeichnung nach § 201 StGB in Betracht. In allen Fällen in meinem Zuständigkeitsbereich erfolgte eine Ansage mit einem Hinweis auf die nachfolgende Aufzeichnung des Telefonates.

In einem Fall wurde dem Anrufer in einer vor dem Telefonat abgespielten Ansage mit dem Hinweis auf die Aufzeichnung die Möglichkeit eingeräumt, der Aufzeichnung zu Beginn des Gespräches gegenüber dem Mitarbeiter des angerufenen Kreditinstitutes zu widersprechen. Erfolgte kein Widerspruch, wurde daraus auf eine Zustimmung zur Aufzeichnung geschlossen.

Ein solches Vorgehen ist datenschutzrechtlich zulässig. Durch die Fortführung des Gespräches in Kenntnis der Aufzeichnung und der bestehenden Widerspruchsmöglichkeit wird die Zustimmung durch schlüssiges Handeln (konkludent) erteilt. Im Widerspruchsfall wäre die Aufzeichnung abgebrochen worden. Darüber hinaus handelte es sich bei dem betroffenen Kreditinstitut um eine Filialbank. Es bestanden daher auch andere zumutbare Möglichkeiten zur Kommunikation, z.B. durch das persönliche Aufsuchen der Filiale.

In einem anderen Fall war die Zustimmung zur Aufzeichnung von Telefonaten durch die Vereinbarung des Telefonbankings erteilt worden. Durch eine von dem betroffenen Kreditinstitut irrtümlich versendete und nicht zutreffende Information über die Aufzeichnung von Telefonaten nahm der Beschwerdeführer an, dass auch über die Vereinbarung hinaus Anrufe aufgezeichnet würden. Dies war tatsächlich aber nicht der Fall.

Darüber hinaus war in einem Fall zu prüfen, wie lange derartige Aufzeichnungen gespeichert werden dürfen.

Hierbei konnte ich gemeinsam mit der Bundesanstalt für Finanzdienstleistungsaufsicht klären, dass die langen bank- und handelsrechtlichen Aufbewahrungsfristen für aufgezeichnete Telefonate keine Anwendung finden. Vielmehr sind telefonisch zustande gekommene Geschäfte grundsätzlich schriftlich oder in gleichwertiger Form zu bestätigen. In der Folge sind dann die Unterlagen aufzubewahren, welche ein aus dem Telefonat resultierendes Geschäft bestätigen oder dokumentieren, nicht aber die Aufzeichnung des Telefonates selbst.

Die Aufzeichnung des Telefonates kann jedoch für drei Monate, gerechnet ab der widerspruchsfreien Durchführung, Bestätigung oder Dokumentation des getätigten Geschäftes, aufbewahrt werden. Kommt es in der Folge zu Meinungsverschiedenheiten über den Inhalt des geführten Telefonates, darf die Aufzeichnung bis drei Monate nach endgültiger Klärung der Meinungsverschiedenheiten aufbewahrt werden. Eine längere Aufbewahrung ist datenschutzrechtlich nicht zu rechtfertigen.

4.3.2
Scoring von Handelsauskunfteien

Auch im aktuellen Berichtszeitraum erhielt ich wieder zahlreiche Beschwerden und Anfragen über das Scoring von Handelsauskunfteien. Mit Ausnahme eines Falles von unzulässiger Nutzung von Anschriftendaten war das betreffende Scoring nicht zu bemängeln.

Viele Handelsauskunfteien errechnen unter Verwendung von mathematisch-statistischen Verfahren aus den von ihnen gespeicherten oder aus einer Anfrage entnommenen Daten für eine angefragte Person einen Scoringwert. Dieser drückt in der Regel die Wahrscheinlichkeit aus, mit der die Rückzahlung eines gewährten Kredites zu erwarten ist. Als Kredit in diesem Sinne sind auch Vorleistungen, wie z.B. eine Lieferung oder Dienstleistung auf Rechnung, zu verstehen.

Das Scoring ist seit 2010 in § 28b BDSG gesetzlich geregelt.

§ 28b BDSG

Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,

2. im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,

3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,

4. im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

In der Mehrzahl der Beschwerden wurde bemängelt, dass ein konkretes Scoring den tatsächlichen Wahrscheinlichkeiten nicht entspricht. Hierbei wurde die Richtigkeit des aus den vorhandenen Daten errechneten Wahrscheinlichkeitswertes bestritten. Außerdem wurde bemängelt, dass individuelle Daten (z.B. Einkommens- und Vermögensverhältnisse) nicht berücksichtigt worden seien, die eine bessere Wahrscheinlichkeit begründen würden.

In allen Fällen habe ich geprüft, ob das beanstandete Scoring den vorstehenden gesetzlichen Anforderungen entsprach. In nahezu allen Fällen war dies gegeben. Allerdings sind meine Möglichkeiten in diesen Fällen darauf beschränkt, die Einhaltung der vorstehenden Regelung zu prüfen.

Wird ein wissenschaftlich anerkanntes mathematisch-statistisches Verfahren verwendet und sind die verwendeten Daten für die Berechnung des Wahrscheinlichkeitswertes erheblich, sind die Anforderungen an § 28b Nr. 1 BDSG erfüllt. Dabei ist es unerheblich, ob der absolut errechnete Wahrscheinlichkeitswert die tatsächlichen Verhälntnisse des konkreten Betroffenen richtig abbildet oder nicht. Die Errechnung des Wahrscheinlichkeitswertes kann auch nicht nach objektiven Kriterien überprüft werden, weil es dafür weder „richtige“ Referenzwerte noch objektive Verfahren zur

Überprüfung der Werte gibt. Deshalb kann auch ich weder die inhaltliche Richtigkeit der errechneten Werte prüfen noch Qualitätskriterien dafür aufstellen.

In allen Einzelfällen hat sich jedoch gezeigt, dass sich die errechneten Werte stichhaltig und nachvollziehbar begründen ließen, auch wenn dies auf den ersten Blick zweifelhaft war.

Auch die anderen Anforderungen von § 28b BDSG waren in der Regel erfüllt.

Die Forderung einzelner Beschwerdeführer, weitere persönliche Daten bei der Berechnung zu nutzen, um die Treffsicherheit des Scorings zu verbessern, sehe ich kritisch. Solche Daten, wie z.B. Daten zur konkreten Einkommens- oder Vermögenssituation, stehen in der Regel nicht zur Verfügung. Es ist auch datenschutzrechtlich nicht sinnvoll, die zusätzliche Sammlung dieser Daten durch Handelsauskunfteien zuzulassen, wenn dies nicht bereits durch andere Erlaubnistatbestände zugelassen ist. Darüber hinaus steht es den Kunden von Handelsauskunfteien frei, solche Daten von den jeweils Betroffenen mit deren Zustimmung zu erheben und zu nutzen. Dies wird z.B. bei Kreditvergaben durch Kreditinstitute praktiziert. Es sollte aber auf solche Fälle beschränkt bleiben, in denen ein hohes wirtschaftliches Risiko in längerfristigen Vertragsbeziehungen abzusichern ist.

Begrüßen würde ich außerdem eine größere Transparenz der Qualität von errechneten Wahrscheinlichkeitswerten. Dies könnte bspw. durch die Angabe der Anzahl von in dem Scoring verwendeter Einzeldaten, der Größe einer Vergleichsgruppe, dem Verhältnis zwischen personenbezogenen Daten zu Adressdaten, der Gewichtung von einzelnen Daten oder Datengruppen und durch die Angabe der Berechnungsgrundlagen erfolgen.

In einem betrachteten Fall jedoch wurde durch die betroffene Handelsauskunftei ein Scoring unter Verstoß gegen § 28b Nr. 3 BDSG durchgeführt. Bei der Untersuchung der verwendeten Berechnungsmethode habe ich festgestellt, dass ein ausschließlich auf Adressdaten basierender Wahrscheinlichkeitswert berechnet und übermittelt wurde. Zwar waren bei der Berechnung des Wahrscheinlichkeitswertes eine Vielzahl von Daten und ein anerkanntes mathematisch-statistisches Verfahren verwendet worden. Diese waren jedoch ausschließlich über die Adresse mit dem Betroffenen verknüpft und ließen daher nur eine eingeschränkte Beurteilung zu. Weitere Daten, die dem Betroffenen unmittelbar zugeordnet waren, wurden nicht verwendet.

Ein solch reines Geoscoring verstößt gegen § 28b Nr. 3 BDSG und ist deshalb unzulässig. Es wird den persönlichen Umständen des jeweils Betroffenen nicht in ausreichendem Umfang gerecht und darf deshalb isoliert weder berechnet noch übermittelt werden.

Ich konnte die betroffene Handelsauskunftei von der Unzulässigkeit der Berechnungsmethode überzeugen.

4.3.3
Speicherung der erteilten Restschuldbefreiung durch Auskunfteien

Im Berichtsjahr habe ich viele Beschwerden über die Speicherung und die Speicherungsdauer von erteilten Restschuldbefreiungen durch die Schufa Holding AG erhalten. Die Speicherung und die dabei durch die Schufa Holding AG angewandte Speicherungsdauer entsprechen jedoch der gesetzlichen Regelung. Daher lag in keinem Beschwerdefall ein Verstoß gegen datenschutzrechtliche Bestimmungen vor.

Nach der langen Dauer eines Verbraucherinsolvenzverfahrens mit einem sich anschließenden Restschuldbefreiungsverfahren halten viele Betroffene die damit verbundenen finanziellen Einschränkungen für überwunden. Sie stellen dann aber häufig fest, dass die Schufa Holding AG die erteilte Restschuldbefreiung gespeichert hat und dies Dritten auf Anfrage mitteilt. Die Schufa Holding AG speichert den Beschluss, mit dem die Restschuldbefreiung erteilt wird, für einen Zeitraum von drei Jahren. Dabei beginnt die Fristberechnung erst mit dem Jahr, welches auf die Restschuldbefreiung folgt. Daraus ergibt sich eine Speicherungsfrist von drei Jahren, zu dem fast ein weiteres Jahr hinzukommen kann. Diese Speicherungsfrist erscheint Betroffenen nach dem meist sieben Jahre laufenden Verfahren bis zur Erteilung der Restschuldbefreiung zu lang und zu einschränkend.

Diese Speicherung entspricht jedoch der gesetzlichen Regelung.

Auskunfteien wie die Schufa Holding AG beziehen die Information über die Eröffnung des Insolvenzverfahrens und die Erteilung der Restschuldbefreiung aus allgemein zugänglichen Quellen wie der Internetseite www.insolvenzbekanntmachungen.de. Die Entnahme der Informationen über die Veröffentlichung des jeweiligen Gerichtsbeschlusses, deren Speicherung und Übermittlung an Dritte im Rahmen der Auskunfteientätigkeit, ist gem. § 29 Abs. 1 Nr. 2 BDSG zulässig.

Bei der Erteilung der Restschuldbefreiung handelt es sich um einen erledigten Sachverhalt. Die Löschung der betreffenden Daten und damit die Speicherungsdauer richtet sich deshalb nach § 35 Abs. 2 Nr. 4 BDSG. Die Löschungspraxis der Schufa Holding AG folgt exakt der dortigen Fristberechnung und ist folglich zulässig, auch wenn sie die Betroffenen wirtschaftlich belastet.

Neben der Speicherdauer wird auch der Fristbeginn häufig als ungerecht empfunden. Die Modalitäten der Fristberechnung führen dazu, dass zum Jahresbeginn erlassene Beschlüsse beinahe ein Jahr länger gespeichert werden, als solche, die zum Jahresende erlassen werden. Dennoch ist auch dies zulässig, weil die Speicherungsdauer in § 35 Abs. 2 Nr. 4 BDSG eindeutig so geregelt ist. Diese Art der Fristberechnung entspricht auch der im Verjährungsrecht geregelten Fristberechnung. Hier wie dort führt sie zwar zu einer Ungleichbehandlung. Diese ist aber dennoch nicht grundrechtswidrig und muss daher von den Auskunfteien und mir beachtet werden. Für eine geänderte Fristberechnung wäre folglich eine gesetzliche Änderung erforderlich.

Eine gesetzliche Änderung, die zu einer taggenauen und für alle Fälle gleich langen Speicherungsfrist führt, würde ich begrüßen.

4.3.4
Vorlage von Ausweiskopien bei Auskunfteien zur Erlangung einer Selbstauskunft

Insbesondere von Auskunfteien werden zur Bearbeitung von Selbstauskünften an Betroffene nach § 34 BDSG immer wieder Kopien des Personalausweises angefordert. Sofern die eindeutige Identifizierung eines Auskunftsersuchenden die Vorlage einer solchen Kopie erfordert und die Kopie nur zu diesem Zweck verwendet wird, ist dies nicht zu bemängeln. Wenn die Kopie des Personalausweises zur Identifizierung aber nicht erforderlich ist, darf diese nicht angefordert werden.

Bereits in meinem 41. Tätigkeitsbericht (Ziff. 2.1.2) hatte ich das Thema Anforderung von Personalausweiskopien aufgeworfen und die Rahmenbedingungen dargestellt, unter denen eine solche Anforderung zulässig ist. Auch im Jahr 2013 habe ich immer wieder Beschwerden über das Einfordern von Personalausweiskopien durch die Schufa Holding AG und andere Auskunfteien erhalten. Fordert ein Betroffener von einer Auskunftei die Zusendung einer Auskunft über die von ihm gespeicherten Daten nach § 34 BDSG an, kommt es häufig vor, dass die Auskunft erst nach Vorlage einer solchen Kopie erteilt wird. Die Schufa Holding AG bittet bereits in dem von ihr bereit gestellten Bestellformular um Zusendung einer Kopie der Ausweispapiere.

Für Betroffene ist in vielen Fällen nicht erkennbar, warum die Ausweiskopie erforderlich sein soll. Insbesondere dann, wenn Betroffene bereits früher auf Anfragen ohne Vorlage einer Ausweiskopie Antworten erhalten haben, einen seltenen Namen führen oder in den letzten Jahren nicht umgezogen sind, führt dieses Vorgehen zu Beschwerden. Häufig wird dabei von Beschwerdeführern auf die Vorschrift des § 14 des PAuswG verwiesen, nach der das Erstellen einer Kopie des Personalausweises verboten sein soll.

§ 14 PAuswG ist die zentrale Datenschutznorm zum Personalausweis. Sie reglementiert den Umgang mit den Daten des Personalausweises. Die Vorschrift verbietet jedoch weder ausdrücklich die Anfertigung von Kopien des Personalausweises, noch soll sie die Verwendung des Personalausweises zu seinem eigentlichen Zweck, der Identifizierung und Legitimierung, verhindern. Daher stellt § 20 PAuswG auch ausdrücklich klar, dass der Ausweis als Identitätsnachweis und Legitimationspapier verwendet werden kann.

Wird eine Kopie des Ausweises im Rahmen der Auskunftserteilung verwendet, geschieht dies zur Vermeidung der Erteilung einer Auskunft mit Daten eines Dritten oder gegenüber einer nicht legitimierten Person. Die Verwendung des Ausweises erfolgt daher entsprechend seinem eigentlichen Zweck, der Prüfung der Identität desjenigen, der die Auskunft über seine Daten verlangt.

Die Kopie des Ausweises darf jedoch nicht verwendet werden, um daraus automatisiert Daten zu erheben und zu speichern; dies untersagt § 20 Abs. 2 PAuswG. Darüber hinaus sind die Ausweiskopien nur zur einmaligen Identifizierung zu verwenden und unverzüglich nach Auskunftserteilung zu vernichten. Ich habe derzeit keinen Hinweis darauf, dass Auskunfteien nicht entsprechend verfahren.

Soweit die Daten des Ausweises allerdings zur Identifizierung oder Legitimationsprüfung nicht erforderlich sind, können diese auf der Ausweiskopie geschwärzt werden. Für die Prüfung der Identität im Zusammenhang mit der Erteilung von Auskünften nach § 34 BDSG sind Angaben zur Nationalität, Augenfarbe und Größe, die 6-stellige Zugangsnummer oder der maschinenlesbare Bereich sowie das Passbild nicht erforderlich. Diese Angaben können deshalb geschwärzt werden.

Auch dann, wenn die Vorlage einer Ausweiskopie zur eindeutigen Identifizierung nicht erforderlich ist, darf diese nicht angefordert werden. Die Auskunft nach § 34 BDSG ist in diesen Fällen unverzüglich zu erteilen, so dass sich die verzögernde oder die Auskunft behindernde Anforderung einer Ausweiskopie verbietet. In einzelnen Beschwerdefällen, bei denen ein entsprechender Eindruck entstanden ist, wurden die betreffenden Auskunfteien auf die Unzulässigkeit ihres Vorgehens hingewiesen. Daraufhin erfolgte in aller Regel eine unverzügliche Auskunftserteilung. Zwangsmaßnahmen waren in keinem Fall erforderlich.

In vielen Fällen konnte dagegen der ursprünglich Vorwurf, die Ausweiskopien seien zur Identifizierung nicht erforderlich, entkräftet werden. Als nachvollziehbare Gründe für das Vorgehen konnte die fehlende Angabe des Geburtsdatums, Fehler in den Daten der betroffenen Auskunftei oder namensgleiche Personen in unmittelbarer geografischer Nähe ermittelt werden.

4.3.5
Telefonanruf durch Inkassounternehmen bei Nachbarn

Mich erreichte eine Beschwerde über den Telefonanruf eines Inkassounternehmens bei einem Nachbarn des Schuldners einer vom Inkassounternehmen bearbeiteten Forderung. Der Nachbar war darum gebeten worden, dem Schuldner eine Rückrufbitte zu übermitteln. Solche Anrufe sind datenschutzrechtlich nicht zulässig.

Ein Inkassounternehmen hatte beim Nachbarn des Schuldners angerufen. Dieser wurde darum gebeten, dem Schuldner eine Rückrufbitte zu übermitteln. Dabei wurde zwar der Inkassoauftrag nicht erwähnt. Es wurde jedoch der Name des Auftraggebers – eine Versicherung – und die Rückrufnummer mitgeteilt. Das Inkassounternehmen war der Auffassung, damit keine personenbezogenen Daten übermittelt zu haben.

Der Anrufer hatte zwar den Namen des Inkassounternehmens und weitere Einzelheiten zu dem Vorgang nicht mitgeteilt. Dennoch ließ sich anhand einer Recherche leicht ermitteln, dass die Telefonnummer, unter der um einen Rückruf gebeten wurde, zu einem Inkassounternehmen gehört. Unabhängig davon wurde dem Nachbarn bei dem Telefonanruf mitgeteilt, dass zwischen dem Beschwerdeführer und der Versicherung ein Vertragsverhältnis besteht, zu dem es offenbar Klärungsbedarf gibt.

Darin liegt die Übermittlung von personenbezogenen Daten an einen unbeteiligten Dritten, den Nachbarn. Diese Übermittlung ist weder für die Durchführung des Vertragsverhältnisses zwischen der Versicherung und dem Beschwerdeführer noch für die Erlangung eines möglicherweise geschuldeten Betrages durch das beauftragte Inkassounternehmen erforderlich.

Für die Kontaktaufnahme mit dem Schuldner stehen genügend andere Möglichkeiten zur Verfügung. Mit ihm kann schriftlich, per Telefon oder persönlich Kontakt aufgenommen werden. Bleiben diese Kontaktaufnahmen erfolglos, besteht die Möglichkeit der Zustellung von Schriftstücken sowie die gerichtliche Durchsetzung der Forderung.

Außerdem stehen einer solchen Übermittlung die Interessen des Betroffenen entgegen. Über diesen kann sich seinem sozialen Umfeld verbreiten, dass er Forderungen nicht begleichen will oder begleichen kann, auch wenn es sich dabei nur um Gerüchte handeln sollte.

Dem betroffenen Inkassounternehmen wurde die Rechtslage erläutert. Daraufhin hat es schriftlich bestätigt, derartige Anrufe künftig zu unterlassen.

4.4 Werbung und Adresshandel

4.4.1
Ethnomarketing

Eine Auswertung von Namen nach ethnischer und rassischer Herkunft oder Religionszugehörigkeit der Betroffenen für Werbezwecke ist unzulässig. Das Verbot darf nicht durch begriffliche Verschleierung umgangen werden.

Unter der Überschrift „Ethnomarketing“ offerierte ein in der Datenanalyse und im Adresshandel tätiges Unternehmen personenbezogene Daten zur ethnischen Herkunft von über 15 Millionen in Deutschland lebenden Konsumenten. Interessenten konnten außerdem ihren vorhandenen Kundendatenbestand im Hinblick auf die wahrscheinliche ethnische Zugehörigkeit des jeweiligen Kunden analysieren lassen. Das Unternehmen warb damit, es könne sowohl für jeden Straßenabschnitt Deutschlands als auch auf Personenebene Wahrscheinlichkeiten der Zugehörigkeit zu den folgenden „Kulturkreisen“ ausweisen: deutsch – italienisch – türkisch – griechisch – spanisch – Balkan – osteuropäisch – nordasiatisch – afrikanisch (südlich der Sahara) – außereuropäisch-islamisch – süd-/ost-/südostasiatisch (Indien/Vietnam) – sonstige (Benelux, Frankreich, Großbritannien, Nordeuropa, USA, Kanada) – Spätaussiedler aus der früheren Sowjetunion. Die Zuordnung einer Person erfolge aufgrund einer Vor- und Nachnamenanalyse und eines Abgleichs mit amtlichen Informationen zur Anzahl der Ausländer. „Wer …weiß, wo die unterschiedlichen ethnischen Gruppen wohnen, ist klar im Vorteil!“ lautete die Werbebotschaft, und weiter hieß es, „Erkenntnisse aus der Analyse können sofort vertrieblich nutzbar gemacht werden, zum Beispiel für Postwurfsendungen oder zur Selektion kulturkreisbezogener Zielgruppenadressen…“.

Im Laufe des datenschutzrechtlichen Überprüfungsverfahrens bestritt das Unternehmen, eine Zuordnung nach ethnischen, rassischen oder religiösen Kriterien vorzunehmen, sondern lediglich nach „Kulturkreisen“, die es wechselnd auch als „Sprachkreise“ oder „Sprach- und Kulturräume“ bezeichnete. Die Zuordnung außereuropäisch-islamischer Kulturkreis wollte das Unternehmen in „außereuropäisch-arabischstämmiger Sprachraum“ ändern.

Die angebotene Dienstleistung war rechtswidrig. Das Bundesdatenschutzgesetz erlaubt die Erhebung, Verarbeitung und Nutzung bestimmter sensitiver Daten wie Angaben über die rassische und ethnische Herkunft oder religiöse Überzeugungen nur sehr eingeschränkt (§§ 3 Abs. 9, 28 Abs. 6 bis 9 BDSG).

§ 3 Abs. 9 BDSG

Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

§ 28 Abs. 6 bis 9 BDSG

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuchs genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt

oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 2 Nummer 2 Buchstabe b gilt entsprechend.

Das Regierungspräsidium Darmstadt hatte als Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich vor einigen Jahren zugestanden, dass bei einer Auswertung von Namen nach Sprachzugehörigkeit für Werbezwecke der Schutzbereich des § 3 Abs. 9 nicht berührt sei, solange die ausgewählten Personen nicht eindeutig einer Ethnie zugeordnet werden können. In der Regel ist mit einer Sprachzuordnung keine Zuordnung zur ethnischen Herkunft verknüpft. Der Begriff „ethnische Herkunft“ ist im ethnologischen Sprachgebrauch durch mehrere Merkmale definiert: Bestimmend sind Religion, Sprache, Abstammung, Herkunft aus oder Ansässigkeit in einer bestimmten geografischen Region, Teilhabe am sozialen Zusammenhang der ethnischen Gruppe, Selbstdefinition als Mitglied der ethnischen Gruppe, Praktizieren der gemeinsam geteilten Kultur der ethnischen Gruppe oder Wissen um diese Kultur. Da die Sprache bei der Bestimmung der ethnischen Herkunft nur ein Element ist, lässt sich aus ihr allein nicht auf die ethnische Herkunft der Person schließen.

Das Angebot beschränkte sich jedoch – entgegen der Meinung des Unternehmens – nicht auf eine Zuordnung zu einem Sprachraum. Es gibt weder einen osteuropäisch-nordasiatischen, afrikanischen (südlich der Sahara) noch einen süd-/ost-/südostasiatischen Sprachraum. Ein osteuropäisch-nordasiatischer Raum würde von Polnisch im Westen bis Jakutisch im Nordosten reichen. Allein in Russland gibt es schätzungsweise 100 Sprachfamilien. Wenn man sich nicht auf die beiden Sprachräume frankophon und anglophon beschränkt, gibt es in Afrika (südlich der Sahara) ca. 2000 Sprachen. Wenig einleuchtend ist auch die Kategorisierung süd-/ost-/südasiatischer Sprachraum mit Sprachen wie z.B. Hindi, Taglog, Koreanisch, Thai, Vietnamesisch, Japanisch oder Chinesisch.

Die als Sprach- oder Kulturkreiszuordnung bezeichnete Kategorisierung vermittelte vielmehr den Eindruck einer verdeckten Klassifizierung nach ethnischen und rassischen Kriterien: Slawen, Eu-

rasier, Mongolenvölker, Asiaten, Schwarzafrikaner. Bezeichnenderweise schlug das Unternehmen daher auch die Kategorie arabischstämmiger (Araber) Sprachraum vor. Dass es sich bei „islamisch“ um eine Zuordnung zu einer Religion handelte, war offensichtlich. Das Unternehmen verarbeitete mithin sensitive Daten gem. § 3 Abs. 9 BDSG.

Der Gesetzgeber hat die Verarbeitung der in § 3 Abs. 9 aufgezählten Datenarten an besonders restriktive Anforderungen geknüpft. Diese Beschränkungen dürfen nicht dadurch umgangen werden, dass die Datenarten in andere Datenarten umdefiniert werden, um so dem Anwendungsbereich des § 3 Abs. 9 zu entgehen. Das geschieht, wenn Ethnie und Rasse definitorisch im Begriff Kulturraum, der sich wiederum durch beliebige räumliche Beschränkung oder Erweiterung auf eine Ethnie oder Rasse reduzieren lässt, versteckt werden. Ein Kulturkreis (Kulturraum) kann, muss aber keineswegs weiträumig sein. Der Begriff kann einen globalen (westlicher oder östlicher Kulturkreis), aber auch seinen sehr regionalen Bezug haben (hessischer Kulturraum). Die Bezeichnung Ethnomarketing, mit dem das Unternehmen warb, war durchaus eine adäquate Beschreibung der mit dem Produkt verbundenen Intention, nämlich Werbung, die auf eine nach ethnischen und/oder rassischen Merkmalen definierte Gruppe ausgerichtet ist, zu ermöglichen.

Die Zuordnung erfolgte ohne Wissen und Einwilligung der Betroffenen. Da die Anforderungen des § 28 Abs. 6 bis 9 BDSG nicht erfüllt waren, war sie rechtswidrig. Das Unternehmen hat die Werbung für das Produkt aus seiner Webseite entfernt.

4.4.2
Nutzungsbasierte Internetwerbung/Tracking

Anbieter von Internetwerbung dürfen mit Hilfe von Tracking-Tools (z.B. Cookies) pseudonyme Nutzungsprofile erstellen, mittels derer Werbung gezielt an bestimmte Personen ausgeliefert werden kann. Die Anbieter müssen die betroffenen Nutzer jedoch darüber aufklären und ihnen eine effektive Möglichkeit bieten, der Profilbildung entgehen zu können.

Bei den Werbetreibenden erfreut sich nutzungsbasierte Onlinewerbung enormer Beliebtheit. Im Gegensatz zu herkömmlicher Werbung, die breit gestreut an alle Nutzer eines Mediums verteilt wird, spricht nutzungsbasierte Werbung direkt die Zielgruppe des jeweils beworbenen Produkts an. Voraussetzung dafür ist jedoch, dass in erheblichem Umfang Daten über die Internetnutzer gesammelt werden.

In diesem Zusammenhang erreichte mich eine Beschwerde über einen Anbieter von Internetwerbung. Dieser soll unter Umgehung bestimmter Einstellungen im Browser des Beschwerdeführers Daten über diesen gesammelt und ihm daraufhin nutzungsbasierte Werbung angezeigt haben.

Internetwerbung wird i.d.R. durch eigenständige Dienstleister angeboten, die als Mittler zwischen den Website-Betreibern und den Werbetreibenden auftreten. Sie betreiben eigene Werbenetzwerke, mittels derer sie auf einer Vielzahl von Webseiten Werbebanner ihrer Kunden schalten können. Um dabei nutzungsbasierte Werbung ausliefern zu können, müssen die Werbeanbieter aus der Masse der Internetnutzer einzelne Personen individualisieren und sie anhand ihres Nutzungsverhaltens in bestimmte Zielgruppen einordnen. Dazu markieren sie mit Hilfe bestimmter technischer Maßnahmen (z.B. durch Setzen von Cookies) die Rechner der Besucher von Websites, die mit dem jeweiligen Werbenetzwerk zusammenarbeiten. Anhand dieser eindeutigen und individuellen Markierung ist ein Rechner (und damit mittelbar die Person, die diesen regelmäßig nutzt) für den Werbeanbieter identifizierbar und wiedererkennbar (sog. Tracking). Hat der Anbieter einen Rechner einmal auf diese Weise „gebrandmarkt“, kann er stets registrieren, wenn mit diesem Rechner eine Website aufgerufen wird, die mit seinem Werbenetzwerk zusammenarbeitet. Auf diese Weise entsteht bei einem entsprechend weitreichenden Werbenetzwerk ein recht detailliertes Bild der Vorlieben und Interessen eines Nutzers anhand der von ihm besuchten Websites. Mit den Daten dieses Profils kann der Werbeanbieter dem Nutzer dann die entsprechende Werbung anzeigen, die seinen Vorlieben entspricht.

In dem mir vorgelegten Fall handelte es sich bei der Werbung um sog. Retargeting. Bei dieser Werbeform werden dem Nutzer Waren aus einem Onlineshop angepriesen, die er sich dort zwar bereits angesehen hat, diese aber letztlich doch nicht gekauft hatte. Diese Werbeform verspricht eine besonders hohe Wahrscheinlichkeit, dass ein Kunde, der sich für ein bestimmtes Produkt bereits interessiert hat, doch noch dazu zu bewegt wird, dieses auch zu kaufen.

Nach § 15 Abs. 3 TMG ist das Erstellen von Nutzungsprofilen mittels Tracking zu Werbezwecken unter bestimmten Bedingungen zulässig. Es muss insbesondere pseudonym stattfinden, der Anbieter darf das Profil also nicht so anlegen, dass es einer bekannten oder bestimmbaren Person direkt zuordenbar ist. Zudem muss der Nutzer z.B. in Form eines Datenschutzhinweises darauf hingewiesen werden, dass Tracking-Tools zu Werbezwecken eingesetzt werden. Auch muss der Anbieter dem Nutzer die Möglichkeit bieten, dem Tracking wirksam zu widersprechen und sich diesem entziehen zu können.

§ 15 Abs. 3 TMG

Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern

der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Durch entsprechende Einstellungen im Browser kann jeder Internetnutzer das Setzen von Drittanbieter-Cookies, also auch solche von Werbeanbietern, unterbinden. Diese Option bietet allerdings keinen sicheren Schutz vor Tracking, da es neben herkömmlichen Cookies auch andere Tracking-Methoden gibt, die nicht durch Einstellungen im Browser verhindert werden können.

Auch der Beschwerdeführer machte geltend, dass er das Setzen von Drittanbieter-Cookies angeblich durch die entsprechende Browser-Einstellung unterbunden habe. Dennoch sei ihm auf der Website einer Zeitung personalisierte Werbung für ein bestimmtes Produkt angezeigt worden, das er zuvor in dem beworbenen Webshop betrachtet hatte.

Bei einer umfassenden Überprüfung des betreffenden Werbeanbieters und seiner für das Tracking genutzten Methoden konnte der Verdacht des Beschwerdeführers nicht bestätigt werden. Der Anbieter betreibt das Tracking in zulässiger Weise mittels Cookies und hält die gesetzlichen Vorgaben diesbezüglich ein. Insbesondere informiert er die Nutzer gut verständlich über die Funktion und die Hintergründe von nutzungsbasierter Werbung und Tracking und gibt ihnen – sogar auf mehreren Wegen – die Möglichkeit, das Tracking zu verhindern. Es konnte auch nicht festgestellt werden, dass der Anbieter die Einstellungen im Browser umgeht, um gegen den ausdrücklichen Willen des Nutzers Cookies setzen zu können.

Auch die weitere Entwicklung des Themas dürfte spannend bleiben. Aufgrund einer bereits in Kraft getretenen europäischen Richtlinie (Art. 5 Abs. 3 der Richtlinie 2002/58/EG i.d.F. der Richtlinie 2009/136/EG) dürfen Cookies nur noch verwendet werden, wenn die Betroffenen vorher darüber informiert wurden und dem ausdrücklich zugestimmt haben. Über die Umsetzung dieser Anforderung in der Praxis besteht allerdings noch Uneinigkeit.

4.5 Versicherungen

4.5.1
Bestandsübertragungen bei selbstständigen Versicherungsvermittlern

Werden Versicherungsverträge durch die Versicherung auf einen neuen selbstständigen Versicherungsvertreter übertragen (Bestandsübertragung), ist hierfür die Einwilligung des jeweiligen Versi-

cherten erforderlich. Dies gilt auch dann, wenn dem neuen Versicherungsvermittler die Daten bereits vor der Übermittlung bekannt gewesen sind.

4.5.1.1
Der Anlass

Ein Versicherungskonzern hat mich um datenschutzrechtliche Beratung betreffend folgenden Sachverhalt gebeten:

Die Versicherungsunternehmen des Konzerns würden mit selbständigen Versicherungsvermittlern zusammen arbeiten, die sich vermehrt mit der Bitte um Bestandsübertragungen bzgl. der durch sie vermittelten Versicherungsverträge an die Versicherungsunternehmen wenden würden.

Im konkreten Fall sei es so, dass eine GmbH & Co KG, eines ihrer Versicherungsvermittlungsunternehmen, darum bitte, dass ihr Versicherungsvertragsbestand von der Versicherung auf einen Einzelunternehmer übertragen werde. Der Einzelunternehmer sei der Gesellschafter der Komplementär-GmbH der Kommanditgesellschaft gewesen. Für die Versicherung stelle sich die Frage, ob es in einer solchen Konstellation um eine Datenübermittlung an Dritte gehe, wenn also die Versicherung den Vertragsbestand an den Einzelunternehmer weiterleite, und ob in diesem Fall von den betroffenen Versicherungsnehmern eine Einwilligung eingeholt werden müsse.

Im Übrigen sei generell zweifelhaft, so der Versicherungskonzern, ob Angestellte, Gesellschafter oder Geschäftsführer/Vorstände eines Unternehmens oder einer juristischen Person, auf die der Bestand zukünftig übertragen werden solle, Dritte im Sinne des BDSG seien, wenn diese bereits Einblick in die personenbezogenen Daten der Versicherungsnehmer gehabt hätten.

4.5.1.2
Rechtliche Bewertung

Bei der Frage, ob eine Übermittlung von personenbezogenen Daten vorliegt, ist für das Datenschutzrecht nicht von Belang, ob und inwieweit dem Empfänger die personenbezogenen Daten bereits bekannt sind.

Empfänger ist jede Person oder Stelle, die Daten erhält (§ 3 Abs. 8 S. 1 BDSG).

Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergeben werden (§ 3 Abs. 4 Nr. 3a BDSG).

Dritter ist jede verantwortliche Stelle, d.h. jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Werden, um auf den anfragenden Versicherungskonzern zurückzukommen, Versicherungsverträge eines selbständigen Versicherungsvermittlers auf einen neuen Versicherungsvermittler übertragen und damit verbunden personenbezogene Daten der Versicherungsnehmer weitergegeben, liegt darin, ohne dass irgendwelche Vorkenntnisse des neuen Versicherungsvermittlers eine Rolle spielen, eine datenschutzrechtliche Übermittlung.

Eine Datenübermittlung bedarf, soll sie zulässig sein, einer datenschutzrechtlichen Rechtfertigung. Denn Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG).

Finden Bestandsübertragungen zwischen Versicherungsunternehmen statt, sind hierfür nicht die Einwilligungen der versicherten Personen erforderlich; die Zulässigkeit derartiger Bestandsübertragungen ist in § 14 Versicherungsaufsichtsgesetz (VAG) speziell und ausführlich geregelt (näher hierzu etwa OLG Köln, Urteil vom 20. Januar 2012, Recht und Schaden 2013/364).

§ 14 Abs. 5 VAG

Die Rechte und Pflichten des übertragenden Versicherungsunternehmens aus den Versicherungsverträgen gehen mit der Bestandsübertragung auch im Verhältnis zu den Versicherungsnehmern auf das übernehmende Versicherungsunternehmen über.

Im vorliegenden, vom anfragenden Versicherungskonzern beschriebenen Kontext ist eine gesetzliche Rechtsgrundlage, die die Übermittlung von personenbezogenen Versichertendaten gestatten würde, jedoch nicht ersichtlich.

Von daher bleibt im Hinblick auf selbständige Versicherungsvermittler nur der Weg, Einwilligungen der Versicherten einzuholen (§ 4a BDSG).

Zulässig und sinnvoll ist, wenn Versicherungsvermittler schon beim Vertragsschluss vom Versicherungsnehmer für zukünftige Bestandsübertragungen generell die Einwilligung einholen und für den

konkreten Fall einer zukünftigen Bestandsübertragung ein Informations- und Widerspruchsrecht des Betroffenen einräumen (näher hierzu Rausch/Fleck/Becker, Der unabhängige Versicherungsmakler, S. 122 ff., 282 f.).

Diese skizzierte Rechtslage habe ich dem Versicherungskonzern mitgeteilt.

4.5.2
Anforderung von ärztlichen Unterlagen durch Versicherungen und Einsichtsrecht des Versicherungsnehmers

Versicherungen sind befugt, ärztliche Unterlagen von bei ihnen versicherten Personen anzufordern, wenn dies zur Beurteilung der Leistungspflicht der Versicherung erforderlich ist. In ärztliche Unterlagen, die den Versicherungen vorliegen, hat der Betroffene nunmehr selbst ein Einsichtsrecht.

4.5.2.1
Die gängige Versicherungspraxis

Mehrfach hatte ich Anfragen, die die übliche Praxis von Versicherungen betreffen, ärztliche Unterlagen zwecks Prüfung ihrer Leistungspflicht anzufordern.

Bspw. verlangte eine Krankenversicherung von ihrem Versicherten vor Erstattung der Arztrechnung den ärztlichen Befundbericht sowie Röntgen- und MRT-Bilder. In einem anderen Fall verknüpfte die Krankenversicherung die Begleichung einer Arztrechnung mit der Aushändigung der kompletten Patientenakte. Eine Reiserücktrittsversicherung verlangte eine Komplettkopie sämtlicher ärztlicher Unterlagen eines Facharztes für Neurologie und Psychiatrie betreffend seiner Patientin, der er wegen einer schweren depressiven Verstimmung absolute Reiseunfähigkeit bescheinigt hatte.

4.5.2.2
Versicherungsvertragsgesetzliche Rahmenbedingungen

Die datenschutzrechtliche Bewertung wird im vorliegenden Kontext in erster Linie durch versicherungsvertragsgesetzliche Regelungen geprägt.

So bestimmt § 14 Versicherungsvertragsgesetz (VVG) ganz generell, dass Geldleistungen der Versicherung erst dann fällig werden, wenn deren Leistungspflicht hinreichend geklärt ist.

§ 14 Abs. 1 VVG

Geldleistungen des Versicherers sind fällig mit der Beendigung der zur Feststellung des Versicherungsfalles und des Umfanges der Leistung des Versicherers notwendigen Erhebungen.

Dieser Regelung korrespondiert § 31 VVG, der die Auskunftspflicht des Versicherungsnehmers festlegt.

§ 31 Abs. 1 VVG

Der Versicherer kann nach dem Eintritt des Versicherungsfalles verlangen, dass der Versicherungsnehmer jede Auskunft erteilt, die zur Feststellung des Versicherungsfalles oder des Umfanges der Leistungspflicht des Versicherers erforderlich ist.

Speziell was die Erhebung von Gesundheitsdaten bei Dritten betrifft, hat der Gesetzgeber in das neue Versicherungsvertragsgesetz 2008 eine Vorschrift erstmalig aufgenommen: § 213 VVG.

§ 213 VVG

(1) Die Erhebung personenbezogener Gesundheitsdaten durch den Versicherer darf nur bei Ärzten, Krankenhäusern und sonstigen Krankenanstalten, Pflegeheimen und Pflegepersonen, anderen Personenversicherern und gesetzlichen Krankenkassen sowie Berufsgenossenschaften und Behörden erfolgen; sie ist nur zulässig, soweit die Kenntnis der Daten für die Beurteilung des zu versichernden Risikos oder der Leistungspflicht erforderlich ist und die betroffene Person eine Einwilligung erteilt hat.

(2) Die nach Abs. 1 erforderliche Einwilligung kann vor Abgabe der Vertragserklärung erteilt werden. Die betroffene Person ist vor einer Erhebung nach Abs. 1 zu unterrichten; sie kann der Erhebung widersprechen.

(3) Die betroffene Person kann jederzeit verlangen, dass eine Erhebung von Daten nur erfolgt, wenn jeweils in die einzelne Erhebung eingewilligt worden ist.

(4) Die betroffene Person ist auf diese Rechte hinzuweisen, auf das Widerspruchsrecht nach Abs. 2 bei der Unterrichtung.

Das Bundesverfassungsgericht hat sich in einer jüngeren Entscheidung mit dem Thema Schweigepflichtentbindungserklärung in der Versicherungswirtschaft befasst (Beschluss vom 17. Juli 2013, 1 BvR 3167/08 , Beck RS 2013, 54218). Das Gericht weist darauf hin, dass es auch schon vor Inkrafttreten des § 213 VVG, also in der Zeit vor 2008, nicht zulässig gewesen sei, Schweigepflichtentbindungserklärungen zu verlangen, die die betroffenen Stellen „umfassend" zur Auskunftserteilung ermächtigen sollen. Das Versicherungsunternehmen müsse einerseits den Eintritt des Versicherungsfalls prüfen können, andererseits müsse aber die Übermittlung von persönlichen Daten auf das hierfür Erforderliche begrenzt bleiben.

Vor diesem rechtlichen Hintergrund stellt sich im Hinblick auf die Versicherungspraxis die Frage, welche Erhebung von Gesundheitsdaten für die Beurteilung der Leistungspflicht des Versicherers – jeweils im konkreten Fall – erforderlich ist.

4.5.2.3
Notwendigkeit der Erhebung von Gesundheitsdaten durch den Versicherer

Mit dem Thema der erforderlichen Erhebung von Gesundheitsdaten hat sich in jüngerer Zeit das OLG München näher befasst (Urteil vom 6. September 2012, Az. 14 U 4805/11, DuD 2012, 908 ff.). Das Gericht legt einführend dar, dass die Zulässigkeit der Einsichtnahme des Versicherers in die Patientenakte nur mit Blick auf den konkreten Fall zu beurteilen sei, also weder die Zulässigkeit noch die Unzulässigkeit einer solchen Einsichtnahme generalisierend festgestellt werden könne.

Anschließend führt das Gericht zutreffend aus, dass soweit im Einzelfall das berechtigte Informationsbedürfnis des Versicherers durch bloße Auskünfte des Versicherungsnehmers und seiner Ärzte im Rahmen der Schweigepflichtentbindung nicht befriedigt werden könne, der Versicherung, die auch die Interessen der Versichertengemeinschaft wahrzunehmen habe, nur der Weg der Ablehnung der Leistung bleibe. Gegebenenfalls habe das die Folge, dass der Versicherungsnehmer im zeit- und kostenaufwendigen Gerichtsprozess den Versicherungsfall und die Notwendigkeit jeder einzelnen Leistung nachzuweisen habe. Damit sei aber weder den Interessen des Versicherungsnehmers noch des Versicherers gedient. Deshalb, so das OLG München zutreffend, sei im Rahmen der Notwendigkeit und Zumutbarkeit nach Sinn und Zweck der §§ 31, 213 VVG auch ein Anspruch auf Einsicht in die Patientenkartei gerechtfertigt. Einer Einsicht des Versicherers in das

Patientenblatt des Versicherungsnehmers stehe das Recht des Versicherungsnehmers auf informationelle Selbstbestimmung nur ausnahmsweise entgegen (ebenda S. 909 rechte Spalte).

Über diese Sach- und Rechtslage habe ich anfragende Bürgerinnen und Bürger informiert. Mit dem Thema „Löschung von Gesundheitsdaten bei Versicherern“ habe ich mich bereits in meinem 41. Tätigkeitsbericht, Ziff. 4.1.5 befasst.

4.5.2.4
Einsichtsrecht der versicherten Person: Verbesserung der Rechtsposition des Versicherungsnehmers

Datenschutzrechtlich hat sich die Rechtsposition der Versicherungsnehmer deutlich verbessert. War es bislang so, dass Versicherungsnehmer gegenüber dem Versicherer nur über einen Arzt oder Rechtsanwalt Auskunft und Einsicht in ärztliche Gutachten oder Stellungnahmen verlangen konnten, die der Versicherer bei der Prüfung seiner Leistungspflicht über die Notwendigkeit einer medizinischen Behandlung eingeholt hatte, § 202 S. 1 a.F. VVG, ist diese Einschränkung nunmehr nicht mehr gegeben: Diese Rechte kann der Versicherungsnehmer nun unmittelbar selbst ausüben:

§ 202 Satz 1 VVG

Der Versicherer ist verpflichtet, auf Verlangen des Versicherungsnehmers oder der versicherten Person Auskunft über und Einsicht in Gutachten oder Stellungnahmen zu geben, die er bei der Prüfung seiner Leistungspflicht über die Notwendigkeit einer medizinischen Behandlung eingeholt hat.

Ausgelöst wurde diese Verbesserung der Rechtsposition durch eine Petition beim Deutschen Bundestag (Bericht des Petitionsausschusses über seine Tätigkeit im Jahr 2012, BTDrucks. 17/13660, S. 22).

In der Begründung des Gesetzentwurfs der Bundesregierung (zur Änderung versicherungsrechtlicher Vorschriften, BTDrucks. 17/11469, zur Neufassung des § 202 VVG, S. 14) wird ausgeführt, Ausgangspunkt sei das Recht des Versicherten auf informationelle Selbstbestimmung. Dem mündigen Versicherungsnehmer könne es überlassen bleiben, eigenverantwortlich zu entscheiden, ob er Gutachten oder Stellungnahmen einsehen möchte, die seine gesundheitliche Situation betreffen.

Allerdings unterliegt dieses Recht gewissen Schranken.

§ 202 Satz 2 VVG

Wenn der Auskunft an oder der Einsicht durch den Versicherungsnehmer oder die versicherte Person erhebliche therapeutische Gründe oder sonstige Gründe entgegenstehen, kann nur verlangt werden, einem benannten Arzt oder Rechtsanwalt Auskunft oder Einsicht zu geben.

Diese Fallgestaltung, so die Begründung des Gesetzentwurfs (ebenda S. 14), dürfte insbesondere für die Bereiche Psychiatrie und Psychotherapie von Bedeutung sein. Eine persönliche Einsichtnahme könnte mit der Gefahr einer gesundheitlichen Schädigung des Versicherungsnehmers verbunden sein. Dies gelte auch mit Blick auf die Auskunft. Damit der Versicherer entscheiden könne, ob eine persönliche Einsichtnahme aus therapeutischen Gründen abzulehnen sei, werde er zweckmäßigerweise den Arzt, der sich gutachtlich geäußert oder Stellung genommen hat, auch um eine Stellungnahme zu der Frage der unmittelbaren Einsicht bitten (ebenda S. 14).

§ 202 VVG in der neuen Fassung ist am 1. Mai 2013 in Kraft getreten (BGBl. I S. 932).

4.6 Verkehr und Energieversorgung

4.6.1
Datenerhebung beim Kauf einer Gruppenfahrkarte bei der Deutschen Bahn AG

Beim Kauf einer Gruppenfahrkarte bei der Deutschen Bahn AG wurde generell ein Formular ausgehändigt, was den Anschein erweckte, dieses müsse für den Kauf der Fahrkarte ausgefüllt werden. Es handelte sich um Daten, die nur beim Abschluss einer – nicht obligatorischen – Reiseversicherung erforderlich sind. Auf meine Intervention hin hat die Deutsche Bahn AG den Vordruck geändert und weist auf den Zweck des Formulars hin.

Dem Reiseleiter eines Vereines, der eine Gruppenreise organisieren wollte, wurde vom Serviceteam der Deutschen Bahn AG ein Vordruck vorgelegt, in dem er die Namen und das Alter der Gruppenreisenden aufführen sollte. Das Formular war überschrieben mit „Teilnahmeliste zur ERV“. Die einzelnen Angaben waren als Pflichtfelder angeführt:

Teilnehmerliste zur ERV			
		Bitte senden Sie uns die ausgefüllte Teilnehmerliste innerhalb der nächsten 7 Tage zurück. (*Pflichtfelder) Per Fax : 01805 / 99 55 55 oder Gruppenreisen@dbdialog.de	
*Kundennummer:		*Hinfahrt am:	
*Auftragsnummer:		*Rückfahrt am:	
lfd. Nr.:	*Nachname(ausgeschrieben)	*Vorname(ausgeschrieben)	*Alter/Begleiter/Lehrkraft
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Er fragte mich, ob das mit datenschutzrechtlichen Bestimmungen vereinbar ist, und bat gegebenenfalls um Korrektur dieser Praktik.

Seine Kritik war berechtigt. Der Zweck der Datenerhebung wurde nicht erklärt. Die Abkürzung „ERV“ ist nicht allgemein geläufig. Auch war nicht ersichtlich, weshalb die Angaben verpflichtend sein sollen.

Ich forderte die Deutsche Bahn zur Stellungnahme auf, warum diese Angaben beim Kauf einer Gruppenfahrkarte erforderlich sein sollen. Dabei stellte sich heraus, dass es sich bei der „Teilnahmeliste zur ERV“ um das Angebot handelte, einen Versicherungsvertrag mit der Europäischen Reiseversicherung (ERV) – ein Reiseversicherer der ERGO-Versicherungsgruppe – abzuschließen. Der Abschluss dieser Reiseversicherung ist aber keine Voraussetzung für das Ausstellen der Fahrkarte bzw. des Gruppenfahrscheins. Die Deutsche Bahn AG sei lediglich aufgrund einer ver-

traglich eingegangenen Kooperation mit der Europäischen Reiseversicherung verpflichtet, ihren Kunden bei der Buchung einer Gruppenreise den Versicherungsschutz der ERV anzubieten.

Für den Abschluss einer solchen Versicherung werden die erhobenen Daten tatsächlich benötigt. Anzahl und Alter der Reisenden sind erforderlich, um den Tarif zu berechnen und die Police auszustellen.

Die namentliche Aufzählung ist erforderlich, da nur für die aufgeführten Personen der Versicherungsschutz gilt. Um „Pflichtfelder“ handelte es sich natürlich nur für den Fall, dass der Abschluss einer Versicherung gewünscht wird.

Das Formular wurde meinen Anforderungen angepasst, so dass ersichtlich ist, dass es sich um Angaben für die Reiseversicherung handelt. Der Zweck dieser Datenerhebung, dem Kunden eine Reiseversicherung anzubieten, wird künftig in einem vorangehenden Verkaufsgespräch eingehend erläutert.

Erst danach erhalten die Kunden bei Bedarf das Formular. Dieses Verfahren begegnet keinen datenschutzrechtlichen Bedenken mehr. Der Vordruck wird bundesweit eingesetzt. Den Reiseleiter habe ich entsprechend informiert.

4.6.2
Erhebung personenbezogener Daten beim Online-Ticketkauf unter Verwendung eines Personalausweises als Identifikationsdokument

Beim Onlinekauf eines Bahntickets werden Daten erhoben, die beim Fahrkartenkauf am Bahnschalter nicht erhoben werden. Die Erforderlichkeit dieser Datenerhebung haben Bahnkunden angezweifelt. Meine Prüfung führte nicht zu einer Beanstandung des Verfahrens.

In einer Reihe von Eingaben beanstandeten Kunden der Deutschen Bahn AG die Vielzahl von Daten, die beim Erwerb eines Online-Tickets erhoben werden. Vor allem der Vergleich zum Direktkauf am Schalter verstärkte die Zweifel der Petenten. Denn dort wird nur das Datum und das Fahrtziel, evtl. Angaben über den gewünschten Zug und den gewünschte Sitzplatz erhoben. In beiden Fällen handelt es sich auf den ersten Blick um denselben Vorgang: Kauf eines Tickets für eine Fahrt mit der Deutschen Bahn.

Beim Kauf eines Online-Tickets am heimischen PC werden jedoch gegenüber dem Fahrkartenkauf am Bahnschalter Daten zur Identifikation und zum Identifikationspapier erhoben. Außerdem

muss genau das Identifikationspapier bei der Fahrt mitgeführt werden, über das beim Ticketkauf nähere Angaben gemacht werden.

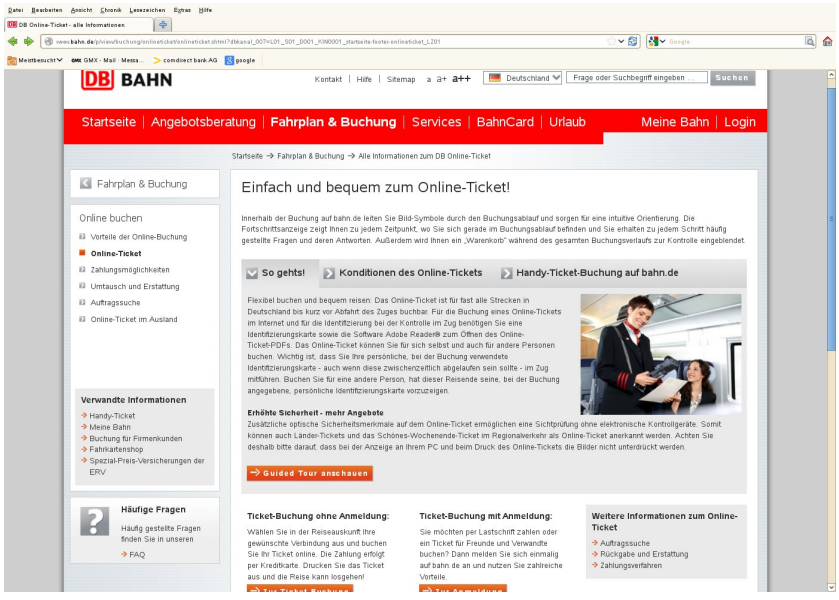
Festgehalten ist das Verfahren in den allgemeinen Geschäftsbedingungen der Deutschen Bahn AG zum Online-Ticketkauf:

Nr. 600/I des Tarifverzeichnisses Personenverkehr Bedingungen für den Internet-Verkauf von Fahrkarten
(gültig seit 15.12.2013)

6.3 Nutzung des Online-Tickets
6.3.1 Das Online-Ticket ist als persönliche Fahrkarte nicht übertragbar und gilt nur in Verbindung mit der bei der Buchung angegebenen ID-Karte. Bei Alleinreisen müssen Reisender und ID-Karten-Inhaber identisch sein. Bei Mehrpersonen-Fahrkarten muss bei der Buchung angegeben werden, welche Person ID-Karten-Inhaber ist. Die Person muss an der Reise teilnehmen.

Kann bei der Fahrkartenprüfung kein auf den Namen des Reisenden lautendes Online-Ticket und/oder keine auf den Namen des Reisenden lautende ID-Karte vorgelegt werden, liegt eine Reise ohne gültige Fahrkarte vor.

Die Umsetzung dieser Vorgaben wird auf dem Internetauftritt der Deutschen Bahn AG ausführlich und zutreffend beschrieben: http://www.bahn.de/p/view/buchung/onlineticket/onlineticket.shtml?dbkanal_007=L01_S01_D001_KIN0001_startseite-footer-onlineticket_LZ01. Auf der dort angebotenen Guided-Tour wird die Vorgehensweise Schritt für Schritt erklärt.



Danach wird deutlich, dass es sich beim Kauf eines Online-Tickets und dem Kauf einer Fahrkarte am Bahnschalter nicht um denselben Vorgang handelt. Dies rechtfertigt einen unterschiedlichen Umfang der Datenverarbeitung und eine differenzierte datenschutzrechtliche Bewertung. Ein Online-Ticket ist eine Fahrtberechtigung, die nicht auf einem Wertpapier wie z.B. einem Fahrschein ausgegeben wird. Stattdessen druckt der Käufer oder die Käuferin das Ticket selbst aus. Es könnte beliebig kopiert werden, oder es könnten Mehrausdrucke von dem als E-Mail zugesandten Online-Ticket hergestellt werden. Daher muss sichergestellt werden, dass es nur einmal verwendet wird. Alle weiteren Maßnahmen dienen dem Schutz vor einer missbräuchlichen Verwendung.

Die Maßgabe, dass das Ticket nur in Verbindung mit der bei der Buchung angegebenen Identifikationskarte gilt, dient dem Zweck, dem mehrmaligen Gebrauch weitgehend entgegenzuwirken, und damit berechtigten Interessen der Deutschen Bahn AG. Es ist datenschutzrechtlich zulässig, dass sie die geforderten Daten erhebt und nur bei Übereinstimmung der Daten der Identifikationskarte (Gültigkeitsdatum und die letzten vier Ziffern der Ausweisnummer) und des Namens des Reisenden auf beiden Dokumenten von einer gültigen Fahrkarte ausgeht.

Auch der Aufdruck des Namens und der Anschrift des Käufers ist datenschutzrechtlich nicht zu beanstanden. Diese Daten sind bei einer ausbleibenden Zahlung oder späteren Rücklastschrift erforderlich, um die Forderung der Deutsche Bahn AG auf den Kaufpreis durchzusetzen.

Aufgrund dieser Besonderheiten des Online-Tickets wurde die Erforderlichkeit der Erhebung der abgefragten personenbezogenen Daten von mir akzeptiert. Für die von einigen Käufern geäußerte Befürchtung einer zweckwidrigen oder missbräuchlichen Verwendung dieser Informationen durch die Deutsche Bahn AG habe ich bislang keine Anhaltspunkte.

4.6.3
Funktionsweise des DB-Navigators 2.1.8

Die App „DB-Navigator 2.1.8 für Android-OS“ greift auf den Standort, den Kalender und die Kontaktdaten des Gerätes zu. Gegen diese Software bestehen gleichwohl keine datenschutzrechtlichen Bedenken. App-Anbieter sollten ihre Software detailliert und aktuell beschreiben, damit Missverständnisse vermieden werden.

In den vergangenen Monaten erreichten mich mehrere Beschwerden bzgl. der Funktionsweise der App DB-Navigator 2.1.8 für Android-OS.

Apps sind Programme für Smartphones und Tablet-Computer.

Die Beschwerdeführer erklärten, diese App greife auf den Standort, den Kalender und die Kontaktdaten des Gerätes zu. Sie hatten den Verdacht, dass ihre persönlichen Daten verdeckt ausspioniert werden.

Es war deshalb zu klären, ob diese App unzulässig personenbezogene Daten verarbeitet oder die Bedeutung und Funktionsweise von systeminternen Berechtigungen – die eine App und Android-OS benötigt – von den Betroffenen missverstanden wird. Die Prüfung des Sachverhaltes veranlasste mich zusätzlich zu einer generellen Betrachtung der Problematik.

4.6.3.1
Persönliche Daten auf Smartphones und Tablet-Computern

Smartphones und Tablet-PCs sind leistungsfähige Computer, deren Daten für Angreifer und die Wirtschaft zum Teil viel interessanter sind als Daten klassischer Personal-Computer, weil sie noch mehr personenbezogene Daten von ihren Besitzern, deren Freunden und anderen Personen preisgeben können.

Zum Beispiel:
- Kontakte (Namen, Telefonnummern, E-Mail-Adressen, Anschriften, Geburtsdaten, usw.)
- Geräteinformationen (Rufnummer, eindeutige Geräte-ID)
- Fotos, Musik, Videos, Dokumente usw.
- Nachrichteninhalte von SMS, E-Mails usw.
- Aufenthaltsorte
- Kalender/Termine
- Telefonate (vergleichbar mit einem Einzelverbindungsnachweis)
- Informationen zum Surfverhalten (Anmeldedaten, Passwörter, Chroniken, Lesezeichen usw.).

Diese Daten lassen sich für wirtschaftliche Zwecke sehr gut nutzen. Deshalb versuchen Gerätehersteller, Provider und vor allem App-Anbieter diese Daten zu erhalten. „Heimtückische“ Apps übertragen diese sogar einfach ungefragt, unverschlüsselt und nicht anonym auf die eigenen Server. Datenschutzgerechte Apps übertragen nur die Daten, die zum Betrieb der App erforderlich sind und nur nach Rückfrage mit dem Betroffenen.

4.6.3.2
Android App-Berechtigungen

Damit Apps nicht eigenmächtig auf alle Daten zugreifen können, existieren unter Android-OS systeminterne Berechtigungen. Dadurch soll der Benutzer erkennen können, welche persönlichen Daten eine App verarbeiten will. Die benötigten Berechtigungen werden im Idealfall vor der Installation zur Zustimmung oder Ablehnung angezeigt. Stimmt der Benutzer den Berechtigungen nicht zu, lässt sich die App nicht installieren.

Teilweise verlangen Apps nach Berechtigungen, die sie zur Funktionserfüllung nicht benötigen. In solchen Fällen rate ich zur Vorsicht. Es besteht die Gefahr, dass die eigenen Daten unberechtigt als Ware gehandelt werden.

Typischerweise erscheinen für Apps des Öfteren Updates. Gründe dafür sind Fehlerbeseitigungen, Sicherheitsupdates und Weiterentwicklung der Funktionalität. Updates werden i.d.R. über den Google Play Store installiert. Benötigt die neue Version der App Berechtigungen, die ihr Vorgänger noch nicht benötigt hat, muss der Nutzer diesen und den bisher benötigten Berechtigungen noch einmal explizit zustimmen.

4.6.3.3
Der DB Navigator und seine Berechtigungen

In seiner Kern-Funktionalität bietet der DB Navigator eine Reiseauskunft für ICE, S-Bahn, Bus und Straßenbahn. Dazu benötigt die App die Angabe von

- Datum und Uhrzeit der Abfahrt bzw. Ankunft und
- Startpunkt („von“) sowie Zielort („nach“) der Reise (Straße, Hausnummer, Ort).

Zum Ausfüllen der Felder „von“ und „nach“ können neben manueller Eingabe auch Adressen aus den Android-OS-Kontakten oder der aktuelle Standort des Gerätes verwendet werden. Sind alle Felder ausgefüllt, liefert eine anschließende Suche passende Verbindungen basierend auf den Fahrplänen. Nach dem Wählen der gewünschten Verbindung kann diese gebucht werden. Zusätzlich besteht die Möglichkeit, diese Verbindung mit Reiseverlauf im Android-OS-Kalender von der App eintragen zu lassen, inklusive einer Benachrichtigung zur Erinnerung vor Fahrtbeginn.

Der DB-Navigator 2.1.8 benötigt also folgende Rechte:

- genauer Standort (GPS- und netzwerkbasiert),
- ungefährer Standort (netzwerkbasiert),

- Kontakte lesen,
- Kalendertermine lesen,
- Kalendertermine hinzufügen,
- Netzwerkverbindungen abrufen,
- voller Netzwerkzugriff und
- Verknüpfungen installieren.

Detaillierte Beschreibungen der einzelnen Berechtigungen können im Internet und in den Einstellungen (unter Einstellungen/Apps/alle und gewünschte App auswählen) des Gerätes nachgelesen werden. In dieser Ansicht werden verschiedene Informationen aufgelistet, insbesondere alle zugelassenen Berechtigungen.

Nachfolgend drei Textbeispiele:

Genauer Standort (GPS- und netzwerkbasiert)

„Ermöglicht der App, Ihre genaue Position anhand von GPS-Daten oder über Netzwerkstandortquellen wie Sendemasten oder WLAN zu ermitteln. Standortdienste müssen auf Ihrem Gerät verfügbar und aktiviert sein, damit die App sie verwenden kann. Apps können Ihren Standort anhand dieser Daten ermitteln und verbrauchen eventuell zusätzliche Akkuleistung."

Kontakte lesen

„Ermöglicht der App, auf Ihrem Tablet gespeicherte Daten zu Ihren Kontakten einschließlich der Häufigkeit zu lesen, mit der Sie bestimmte Personen angerufen, an sie eine E-Mail gesendet oder auf andere Weise mit ihnen kommuniziert haben. Diese Berechtigung ermöglicht Apps das Speichern Ihrer Kontaktdaten und schädliche Apps können Kontaktdaten ohne Ihr Wissen weitergeben."

Kalendertermine hinzufügen

„Ermöglicht der App, Termine, die Sie auf Ihrem Telefon ändern können, hinzuzufügen, zu entfernen und zu ändern, einschließlich der von Freunden und Kollegen. Damit kann die App Nachrichten senden, die so erscheinen, als stammten sie vom jeweiligen Kalenderinhaber, oder Termine ohne Wissen des Inhabers ändern."

4.6.3.4
Ergebnis

Viele Bürgerinnen und Bürger sind oft zu Recht kritisch, wenn Apps auf ihre persönlichen Daten zugreifen. In den letzten Jahren sind viele Fälle des Missbrauchs bekannt geworden. Im Moment

sorgt der aktuelle NSA Skandal zusätzlich für Verunsicherung.

Außerdem sind viele Berechtigungen so definiert, dass Sie mehrere einzelne Rechte zusammenfassen. Benötigt die App davon aber nur ein Teilrecht, muss trotzdem die Zugriffsberechtigung für alle eingeräumt werden, da die zusammengefassten Rechte nicht teilbar sind. Für den Benutzer ist es aber nicht ersichtlich, warum der Zugriff auf die in der Berechtigung zusammengefassten nicht benötigten Rechte erlaubt werden soll.

Gleichzeitig sind die detaillierten Beschreibungen der Berechtigungen so formuliert, dass möglichst viele – so genannte „schädliche“ – Anwendungsfälle beschrieben werden. Viele Nutzer glauben dann, dass die App, die gerade installiert werden soll, alle beschriebenen Rechte nutzt.

Ausschlaggebend für die datenschutzrechtliche Bewertung ist aber nicht nur die Verwendung dieser Berechtigungen, sondern die Frage, wie die dadurch verfügbaren persönlichen Daten auch tatsächlich verarbeitet werden. Bei dieser Bewertung war nicht nur der Konzerndatenschutzbeauftragte der Deutschen Bahn AG behilflich, sondern auch die Beschreibung der App im Google Play Store. Diese beschreibt detailliert, warum die App welche Berechtigungen benötigt. Die Angaben des Konzerndatenschutzbeauftragten und die Beschreibung im Google Play Store decken sich mit der Softwarefunktionalität des DB Navigators 2.1.8. Zudem erklärt der Konzerndatenschutzbeauftragte, dass für die Reiseauskunft die ausgefüllten Felder (s.o.) an einen Server der Deutschen Bahn AG übertragen werden. Danach ermittelt der Server die Verbindungen und sendet sie an das Gerät. Danach bleiben keine Daten aus der Reiseauskunftanfrage auf dem Server gespeichert. Sonstige Daten werden weder an einen Server der Deutschen Bahn AG noch an einen Server eines Dritten übermittelt. Ich habe keine Anhaltspunkte gefunden, die den Aussagen des Konzerndatenschutzbeauftragten widersprechen.

Deshalb bestehen für die Version 2.1.8 des DB-Navigators für Android-OS keine datenschutzrechtlichen Bedenken. Dieser Fall zeigt deutlich die Wichtigkeit der Transparenz als eines der „neuen Datenschutzziele“ (s.a. M. Rost, A. Pfitzmann: Datenschutz-Schutzziele – revisited, DuD, 2009 S. 353). Deshalb sollten App-Anbieter im Google Play Store detailliert beschreiben, welche Berechtigungen für die Softwarefunktionalität benötigt werden und wie die dadurch gewonnen Daten verarbeitet werden. Diese Beschreibung sollte immer auf dem aktuellen Versionsstand basieren. Durch veraltete Beschreibungen entstehen andernfalls Missverständnisse.

4.6.4
Das „Call a Bike“-Angebot der Deutschen Bahn AG

Für das Ausleihen von Fahrrädern bietet die Deutsche Bahn AG das Angebot "Call a Bike" an. Mit einer Kundennummer, die mit dem eigenen Geburtsdatum beginnt, kann man u.a. an Entleihterminals Fahrräder ausleihen. Auf die Option, das Geburtsdatum nicht zu diesem Zweck zu verwenden, wurde nur unzureichend aufmerksam gemacht. Dem wurde abgeholfen.

Ein Bürger fragte mich, ob ich es für zulässig erachte, dass in der Kundennummer, die man nach der Registrierung zu dem Angebot „Call a Bike“ erhält, das eigene Geburtsdatum aufgeführt ist. Diese Kundennummer soll an Entleihterminals und im Internet benutzt werden. Sie wird auch am Telefonservice des Buchungssystems IVR (Interactive Voice Response) der Bahn abgefragt.

Die nach der Registrierung bei dem „Call a Bike“-System vergebene zehnstellige Nummer besteht am Anfang aus dem Geburtsdatum, dem dann vier zufällig generierte Ziffern folgen (TTMMJJ + 4 weitere Ziffern). Durch die Benutzung des Geburtsdatums soll – so die Deutsche Bahn AG – die Sicherheit einer zehnstelligen Kundennummer mit den Vorzügen einer für den Kunden leicht merkbaren Zahlenkombination kombiniert werden.

Die Bestrebungen der Deutschen Bahn AG, die Zahlenkombination dem menschlichen Gedächtnis zugänglicher zu machen, sind durchaus nachvollziehbar. Das Merken einer zehnstelligen Nummer bereitet vielen Menschen Schwierigkeiten. Problematisch erschien mir jedoch, dass die Betroffenen anscheinend kein Wahlrecht zwischen einer personenbezogenen und einer nicht personenbezogenen Kundennummer hatten. Letzteres gebietet aber der Grundsatz der Datensparsamkeit, nämlich so wenig personenbezogene Daten wie möglich zu nutzen (§ 3a BDSG).

In der von mir angeforderten Stellungnahme des Konzerndatenschutzes hieß es, dass auch eine solche Verfahrensweise durchaus vorgesehen ist und dass auf Wunsch des Kunden eine alternative zehnstellige Kundennummer ohne personenbezogenen Bestandteil zur Verfügung gestellt werden kann. Die Bediensteten hatten es lediglich versäumt, auf diese Möglichkeit hinzuweisen.

Die verantwortliche Stelle wurde aufgefordert, zukünftig deutlicher auf die Möglichkeit dieser alternativen Kundennummer hinzuweisen und damit dem Grundsatz der Datenvermeidung und Datensparsamkeit gemäß § 3a BDSG besser zu genügen. Dies wurde mir zugesagt. In dieser Konstellation ist die freiwillige Verwendung des Geburtsdatums in einer Kundennummer unproblematisch. Den Eingeber habe ich entsprechend informiert.

4.6.5
Anruferidentifikation durch Energieversorger bei telefonischen Anfragen

Die Daten verarbeitende Stelle muss, bevor sie bei einem telefonischen Kundenkontakt personenbezogene Daten nennt, überprüfen, ob der Gesprächspartner tatsächlich die Person ist, für die sie sich ausgibt.

Regelmäßig beschweren sich Betroffene über das Abfragen von personenbezogenen Daten am Telefon. Beispielsweise rufen sie bei ihrem Energieversorger an und wünschen eine Erläuterung ihrer Energierechnung, oder sie wünschen ihre monatliche Abschlagszahlung zu erhöhen oder zu reduzieren.

Die Unternehmen befinden sich in solchen Fällen in einem Dilemma. Einerseits müssen sie sich kunden- und serviceorientiert verhalten, sonst wenden sich die Kunden einem anderen Unternehmen zu. Das steht aber im Raum, wenn sie immer auf einer persönlichen Vorsprache im Servicebüro des Unternehmens oder auf einer schriftlichen Kontaktaufnahme bestehen. Andererseits können sie nicht einfach auf Zuruf von „irgendjemandem“ z.B. im Wege des Lastschriftverfahrens abzubuchende Abschlagszahlungen verändern, ohne sicher zu sein, dass sie auch tatsächlich mit der Person sprechen, für die sich der Gesprächspartner ausgibt. Denn in dem Gespräch lässt es sich nicht vermeiden, dass personenbezogene Daten – etwa über persönliche Verbrauchsdaten oder bisherige Abschlagszahlungen – ausgetauscht werden. Zudem verhalten sie sich gem. § 43 Abs. 2 Nr. 1 BDSG ordnungswidrig, wenn sie unzulässig einem anderen als dem Betroffenen personenbezogene Daten übermitteln. Sie haben daher grundsätzlich ein berechtigtes Interesse daran, den Anrufer eindeutig zu identifizieren.

§ 43 Abs. 2 Nr. 1 BDSG

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

…

Um sicherzustellen, dass der Anrufer derjenige ist, für den er sich ausgibt, darf das Unternehmen zu den ihm vorliegenden persönlichen Angaben Fragen stellen. Zur Identifikationsprüfung dürfen also persönliche Daten zwecks Abgleich abgefragt werden. Bestimmte Anforderungen an das Identifikationsverfahren stellt das Gesetz nicht; abstrakt kann nur verlangt werden, die im Geschäftsverkehr erforderliche Sorgfalt einzuhalten, um fahrlässige unbefugte Übermittlungen zu

vermeiden. Welche Fragen und wie viele Fragen gestellt werden können, ist branchenspezifisch und kann nicht durch allgemeine Aussagen festgelegt werden. Die Zählernummer ist zum Beispiel auf dem Zähler selbst abgedruckt und daher nur bedingt als Identifizierungsmerkmal geeignet. Da die Zähler in vielen Mehrfamilienhäusern oft für alle Bewohner mehr oder weniger zugänglich sind, sollen Daten erfragt werden, die nur dem tatsächlichen Kunden bekannt sind. In diesem Zusammenhang können auch das Geburtsdatum und eventuell die Kontodaten abgefragt werden. Die Erfahrung zeigt aber, dass die Fragen nach den Bankdaten oft auf Unverständnis stoßen, da sie der Allgemeinmeinung – man gibt am Telefon keine Bankverbindung an – zuwiderlaufen. Manche Energieversorger sind extra bemüht, zusätzlich zum Namen und Kundennummer ein weiteres Datum abzufragen, das nicht auf der Rechnung steht. Der Hintergrund dieser Bemühungen ist, dass das Rechnungsschreiben oder sonstige Post eventuell über den Hausmüll zur Kenntnis einer dritten Person gelangen kann. Die Tatsache des Abgleichs der vorliegenden Daten zum Zwecke der Anruferidentifizierung soll den Kunden auch jeweils erklärt werden.

Die Überprüfung der Richtigkeit des Identifizierungsverfahrens lässt sich für mich nur schwer gestalten. Lediglich in den Fällen, in denen Daten erfragt werden, die dem Unternehmen bislang nicht bekannt sind – Daten, die sich also nicht für eine Identitätsprüfung eignen – kann ich aufsichtsrechtlich einschreiten. Ansonsten sind solche Fragen, auch die nach der Bankverbindung, zulässig.

4.7 Handel, Handwerk, Selbstständige und Gewerbebetriebe

4.7.1
Beauftragung eines Steuerberaters – Funktionsübertragung oder Auftragsdatenverarbeitung?

Berufsrechtliche Vorschriften stehen der Anwendbarkeit des allgemeinen Datenschutzrechts nicht immer entgegen. So ist bei der Auslagerung von steuerlichen Tätigkeiten an einen Steuerberater stets im Einzelfall zu beurteilen, ob datenschutzrechtlich eine Auftragsdatenverarbeitung nach § 11 BDSG oder eine unabhängige eigenverantwortliche Tätigkeit i.S.v. § 57 StBerG vorliegt.

Im Berichtsjahr häuften sich Eingaben mit der Frage, wie die Übertragung steuerlicher Tätigkeiten an einen Steuerberater datenschutzrechtlich zu beurteilen ist.

Steuerberater und ihre Gehilfen unterliegen eigenen bereichsspezifischen Berufsvorschriften nach dem Steuerberatungsgesetz bzw. ihrer Berufsordnung, die u.a. die besondere Vertrauensbeziehung zu ihren Mandanten absichern sollen. So legt § 57 Abs. 1 StBerG den Steuerberatern auf,

ihre Tätigkeit im Rahmen ihres Auftrages unabhängig und eigenverantwortlich zu erbringen. Ihre Berufsordnung fordert, dass sie keine Bindungen eingehen dürfen, die ihre berufliche Entscheidungsfreiheit gefährden können.

§ 57 Abs. 1 StBerG

Steuerberater und Steuerbevollmächtigte haben ihren Beruf unabhängig, eigenverantwortlich, gewissenhaft, verschwiegen und unter Verzicht auf berufswidrige Werbung auszuüben.

Gemäß § 1 Abs. 3 BDSG verdrängen diese speziellen Regelungen des Berufsrechts die allgemeinen Datenschutzvorschriften.

§ 1 Abs. 3 BDSG

Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

Allgemeines Datenschutzrecht wird jedoch nicht verdrängt, wo der Steuerberater nicht eigenverantwortlich tätig wird, sondern eine untergeordnete Hilfstätigkeit im Sinne von § 6 Nr. 3 und 4 StBerG ausübt.

§ 6 Nr. 3 und 4 StBerG

Das Verbot des § 5 gilt nicht für

1. ...
2. ...
3. die Durchführung mechanischer Arbeitsgänge bei der Führung von Büchern und Aufzeichnungen, die für die Besteuerung von Bedeutung sind; hierzu gehören nicht das Kontieren von Belegen und das Erteilen von Buchungsanweisungen,
4. das Buchen laufender Geschäftsvorfälle, die laufende Lohnabrechnung und das Fertigen der Lohnsteuer-Anmeldungen, soweit diese Tätigkeiten verantwortlich durch Personen erbracht werden, die nach Bestehen der Abschlussprüfung in einem kaufmännischen Ausbildungsberuf oder nach Erwerb einer gleichwertigen Vorbildung mindestens drei Jahre auf dem Gebiet des Buchhaltungswesens in einem Umfang von mindestens 16 Wochenstunden praktisch tätig gewesen sind.

Eine spezielle Regelung zur Auftragsdatenverarbeitung trifft das Steuerberatungsgesetz nicht. Dementsprechend ist die Anwendung von § 11 BDSG (Verarbeitung personenbezogener Daten im Auftrag) durch das Berufsrecht nicht ausgeschlossen.

Diese datenschutzrechtliche Beurteilung entspricht auch der vergleichbaren Rechtslage, wenn ein Auftraggeber direkt einen gewerblichen Dienstleister mit der Ausführung der Hilfstätigkeit beauftragt, ohne einen Steuerberater dazwischen zu schalten.

Es ist somit stets im Einzelfall zu prüfen, ob die ausgelagerte Tätigkeit eine weisungsabhängige Ausführung von Hilfstätigkeiten nach § 11 BDSG oder die Übernahme einer selbstständigen und eigenverantwortlichen Aufgabe i.S.v. § 57 StBerG (sog. Funktionsübertragung) darstellt. Anhaltspunkt für eine sachgerechte Entscheidung in der Praxis kann die Antwort auf die Frage sein:
Kann die Tätigkeit statt an einen Steuerberater/Steuerbevollmächtigten auch an einen gewerblichen Auftragnehmer übertragen werden?
Lautet die Antwort „ja“, dann ist von einer Datenverarbeitung im Auftrag gemäß § 11 BDSG auszugehen.

In jedem Fall muss den Beteiligten klar sein, welche der beiden Ausführungsformen letztlich vereinbart wird und welche Rechte, Pflichten und Konsequenzen sie damit eingehen:
Bei der Funktionsübertragung wird der Steuerberater zur verantwortlichen Stelle, § 3 Abs. 7 BDSG. Er erhält vom Auftraggeber die Nutzungsrechte an den Daten zu dem im Mandatsvertrag bestimmten Verarbeitungszweck. Er hat die Zulässigkeit und Richtigkeit der Datenverarbeitung und die Gewährleistung des Datenschutzes sicherzustellen. Er ist Adressat der Betroffenenrechte bzgl. Auskunft, Löschung, Berichtigung von Daten (§§ 6 bis 8 BDSG), meiner Kontroll- und Aufsichtsmaßnahmen nach § 38 BDSG und Pflichtiger nach § 42a BDSG (Informationspflicht bei unrechtmäßiger Kenntniserlangung).

Liegt eine Auftragsdatenverarbeitung vor, steht der Auftraggeber dafür ein, dass die oben aufgeführten datenschutzrechtlichen Pflichten auch beim Auftragnehmer eingehalten werden. Nach § 11 Abs. 2 bis 5 BDSG hat er den Auftragnehmer sorgfältig auszuwählen und schriftlich zu beauftragen. Der Auftragnehmer muss mindestens den Datenschutzstandard erfüllen, den der Auftraggeber selbst einzuhalten verpflichtet ist.

Der Auftraggeber muss sich zudem vor Beginn der Datenverarbeitung – und auch regelmäßig während der Laufzeit des Vertragsverhältnisses – davon überzeugen, dass beim Auftragnehmer die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden.

Das Muster eines Vertrages für eine Auftragsdatenverarbeitung steht auf meiner Internetseite zum Abruf zur Verfügung. (http://www.datenschutz.hessen.de/ft-auftragsdatenverarbeit.htm).

4.7.2
Datenschutzgerechtes Verfahren beim Online-Weiterverkauf personalisierter Konzerttickets

Eintrittskarten für ein Konzert können beim Kauf personalisiert werden. Im Falle der Übertragung des Tickets auf eine dritte Person (Umpersonalisierung) darf der Veranstalter keine elektronische Vorlage von Personalausweiskopien zur Identifizierung des bisher Berechtigten verlangen.

Anlässlich einer Eingabe zur Abwicklung von Ticketverkäufen durch einen Konzertveranstalter mit Sitz in Berlin bat mich der Berliner Beauftragte für Datenschutz und Informationsfreiheit, die Verkaufspraxis des in Hessen ansässigen Vertriebspartners des Veranstalters zu prüfen. Hintergrund war, dass der Vertriebspartner die Tickets für das Konzert eines besonders beliebten Künstlers „personalisiert“ verkaufte und in bestimmten Fällen des Weiterverkaufs vom Käufer verlangte, den Personalausweis zu scannen und an ihn per E-Mail zu versenden. Der Bitte nach Überprüfung bin ich gerne nachgekommen.

Der Vertriebspartner war, wie zuvor auch schon der Konzertveranstalter, sehr an der datenschutzrechtlichen Bewertung des Ticketing-Systems interessiert und legte bereitwillig die praktizierte Verfahrensweise offen.

Der Verkauf der Eintrittskarten erfolgte im Internet über die Ticketverkaufsplattform des Vertriebspartners. Zwischen ihm und dem Konzertveranstalter besteht ein Auftragsdatenvertrag nach § 11 BDSG. Darin sind der Ablauf des Verfahrens, die technisch-organisatorischen Sicherheitsmaßnahmen sowie die Rechte und Pflichten der Vertragspartner geregelt. Der Vertriebspartner handelt im Namen und auf Weisung des Konzertveranstalters, der als verantwortliche Stelle für die Einhaltung der datenschutzrechtlichen Vorschriften haftet.

Er vermittelt den Kaufvertrag zwischen Käufer und Veranstalter und wickelt das Verfahren sowohl beim Erstkauf als auch beim Weiterverkauf gegenüber dem Kunden ab. Die Entscheidung, ob und in welchen Fällen Eintrittskarten personalisiert werden, obliegt dem Veranstalter, der diese Entscheidung wiederum zusammen mit dem Management des Künstlers trifft. Der Vertriebspartner setzt diese Vorgabe um.

Bei personalisierten Konzertkarten ist der Name der berechtigten Person, die die Veranstaltung besuchen will, auf dem Ticket aufgedruckt. Entsprechend der vereinbarten Geschäftsbedingungen hat nur diese Person das Besuchsrecht für das Konzert. Bei Einlass wird vom Veranstalter kontrolliert, ob das Ticket gültig ist und die Person auch berechtigter Inhaber ist. Verkauft der Erstkäufer oder Inhaber seine Eintrittskarte an einen Dritten weiter, muss auch das Besuchsrecht auf den neuen Inhaber übertragen werden, was der Zustimmung des Ticketausgebers (Veranstalter) bedarf. Diese erfolgt nach Prüfung durch Eintrag des Namens des neuen Inhabers auf dem Ticket durch den Vertriebspartner (Umpersonalisierung). Damit soll ausgeschlossen bzw. zumindest erschwert werden, dass Tickets gewerblich oder in nicht autorisierten Internetauktionen missbräuchlich und überteuert gehandelt werden. In den Geschäftsbedingungen verbietet der Veranstalter u.a. den Weiterverkauf zu gewerblichen Zwecken oder um Gewinn zu erzielen. Der neue Inhaber erhält durch die Umpersonalisierung das Recht, die Veranstaltung zu besuchen, und kann die Einlasskontrolle passieren.

Der Weiterverkauf eines solchen Tickets kann über die vom Vertriebspartner eigens eingerichtete Ticketbörse erfolgen. Der Verkäufer stellt das Ticket als Verkaufsangebot ein. Der Verkauf darf allerdings nur maximal zum Originalpreis des Tickets zzgl. der Vorverkaufsgebühr erfolgen. Sobald es verkauft ist, wird der Verkäufer informiert, dem Käufer ein neues personalisiertes Online-Ticket ausgestellt und damit auch das Nutzungsrecht übertragen. Das ursprüngliche Online-Ticket wird gesperrt und der Verkaufspreis dem Konto des Verkäufers oder seinem Kreditkartenkonto gutgeschrieben.

Wurde ein Ticket außerhalb der Ticketbörse an einen Dritten weitergegeben, z.B. durch Verschenken, musste sich der Erstkäufer im Ticketportal anmelden und dort die "Umpersonalisierung" durchführen lassen. In der entsprechenden Rubrik musste er Namen und Email-Adresse von sich sowie der Person, der das Ticket übertragen werden sollte, angeben. Weiter wurde der Betroffene aufgefordert, eine Kopie des Personalausweises “hochzuladen”, aus dem die Identität des bisherigen Ticket-Inhabers hervorging. Je nach Sachverhalt konnte dies sein eigener Personalausweis sein oder aber auch der der bislang berechtigten (dritten) Person. Der Käufer war mitunter gezwungen, einen fremden Personalausweis zu kopieren und die Kopie elektronisch zu versenden. Der Vertriebspartner prüfte sodann, ob der auf dem Online-Ticket angegebene Name mit dem Namen auf dem Personalausweis übereinstimmte, die Person also auch tatsächlich existierte. Wenn dies der Fall war, wurde das Online-Ticket zur Umpersonalisierung freigegeben. Nach Umpersonalisierung des Tickets wurde dem Erwerber per E-Mail ein auf seinen Namen ausgestelltes Online-Ticket an dessen vom Erstkäufer angegebene Adresse übersandt. Gleichzeitig mit Versand des neuen Online-Tickets an den Erwerber wurde das bisherige Online-Ticket gesperrt. Nach der Übertragung berechtigte es nicht mehr zum Einlass. Diese Vorgehensweise war datenschutzrechtlich im wesentlichen korrekt.

Rechtsgrundlage für die Erhebung und Verarbeitung von Vor- und Nachname und E-Mail-Adresse des Käufers, bzw. Ticketinhabers ist § 28 Abs. 1 Satz 1 BDSG.

§ 28 Abs. 1 Satz 1 BDSG

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

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Nach dieser Vorschrift ist die Verarbeitung personenbezogener Daten erlaubt, soweit sie zu eigenen Geschäftszwecken erfolgt und zur Durchführung des Vertrages mit dem Betroffenen erforderlich ist.

Beide Kriterien waren bzgl. der Erhebung von Namen und E-Mail-Adressen erfüllt. Sie waren zur Abwicklung eines geordneten Ticketverkaufs erforderlich. Die Form des personalisierten Ticketverkaufs wird – trotz erhöhten wirtschaftlichen Aufwands – dann eingesetzt, wenn die Beliebtheit der auftretenden Künstler eine hohe Schwarzmarktquote befürchten lässt. Diese Vorgabe wird vom Künstler selbst, seinem Management und dem Konzertveranstalter getroffen, wenn vorauszusehen ist, dass das Interesse an den Konzertkarten größer sein wird als das verfügbare Kartenkontingent. Ausreichende Erfahrungen zeigen, dass ohne entsprechende Maßnahmen ein regelrechter Ticketzweitmarkt für bis zu 25% der Gesamttickets entsteht, der zudem für die interessierten Käufer nicht immer erkennbar ist. Die gewerblichen Tickethändler erwerben Tickets in erheblichen Mengen, die eine künstliche Verknapptheit bewirken. Der dadurch entstehende Preisdruck führt dazu, dass Kunden im Internet für „Restkarten“ einen viel zu hohen Preis zahlen, oft ohne zu erkennen, dass es sich weder um eine autorisierte Verkaufsstelle noch um offizielle Preise handelt. Das Preisgefüge wird verzerrt, es kommt zu Beschwerden, das Image von Künstler und Veranstal-

ter wird beschädigt. Im vorliegenden Fall wollten Konzertagentur und Künstler den zumeist jugendlichen Fans einen Eintrittspreis bieten, der angemessen und nicht über Gebühr belastend ist. Um Missbräuche und Verfälschungen beim Ticketverkauf durch gewerbliche Tickethändler zu verhindern, war die besondere Vorgehensweise der Personalisierung erforderlich.

Ohne die Personalisierung der Eintrittskarten wären die Einhaltung der angebotenen Preisstruktur, die geordnete Abwicklung des Ticketverkaufs und damit auch der Geschäftszweck durch etwaigen Schwarzmarkthandel gefährdet.

Soweit allerdings für die Umpersonalisierung eines Tickets die elektronische Übermittlung der Kopie des Personalausweises des Erstkäufers oder früheren Inhabers zum Nachweis seines berechtigten Besitzes an der Eintrittskarte Voraussetzung war, war die Datenübermittlung nicht zulässig.

Seit der Neufassung des Personalausweisgesetzes vom 22. Dezember 2011 ist das Verbot der automatisierten Speicherung des Personalausweises geregelt. Bzgl. des Kopierens von Personalausweisen findet sich zwar keine ausdrückliche Verbotsnorm. Allerdings gibt es in Spezialgesetzen (Geldwäschegesetz, Telekommunikationsgesetz u.a.) ausdrückliche Vorschriften, wann eine Kopie verlangt werden darf. Für sonstige Bedarfsfälle hat das Bundesministerium des Innern Rahmenbedingungen formuliert, wann die Erstellung einer Kopie sicherheits- und datenschutzrechtlich zulässig ist. Entscheidendes Kriterium ist dabei zuerst, ob überhaupt die Erforderlichkeit für eine Kopie gegeben ist (Näheres siehe auch 41. Tätigkeitsbericht, Ziff. 2.1.2).

Vorliegend stellte sich nach Rücksprache mit den Beteiligten heraus, dass jedes andere amtliche Ausweisdokument den Nachweiszweck ebenso erfüllt, wobei alle nicht erforderlichen Daten vom Betroffenen möglichst geschwärzt werden sollen. Der Veranstalter und der Vertriebspartner haben daraufhin den zwischen ihnen bestehenden Auftragsdatenvertrag und die Datenschutzerklärung entsprechend angepasst. Bei zukünftigen Vorverkäufen werden keine Personalausweisdaten mehr über Internet erhoben. Der Nachweis kann durch jedes andere kopierfähige Ausweisdokument, z.B. Führerschein erfolgen. Der Betroffene wird ausdrücklich darauf hingewiesen, dass keine Kopie des Personalausweises verwendet werden soll.

Die Darstellung der sicherheitstechnischen Architektur des Verfahrens war ansonsten nicht zu beanstanden. Die Verbindung für die Datenübermittlung ist ausreichend abgesichert. Sämtliche Daten werden nach dem Konzertbesuch gelöscht.

4.7.3

Zulässigkeit der Erhebung personenbezogener Daten bei der Rückgabe von gebrauchten Tonerkassetten an ein großes Elektronikunternehmen

Im Rahmen der Produktverantwortung gem. § 23 Kreislaufwirtschaftsgesetz sind Unternehmen, die Produkte herstellen oder vertreiben, u.a. verpflichtet, nach Gebrauch der Erzeugnisse verbleibende Abfälle zurückzunehmen und umweltverträglich zu verwerten oder zu beseitigen. Die Erhebung der im Rahmen des Rücknahmeverfahrens erforderlichen personenbezogenen Daten ist zulässig.

Mich erreichte die Eingabe eines Bürgers, der die Frage aufwarf, ob für die Rücksendung gebrauchter Tonerkassetten die geforderte Registrierung auf der Homepage des Unternehmens unter Angabe von Vorname, Name, Adresse und E-Mail-Adresse zulässig sei.

Gleichzeitig befürchtete der Petent, dass auf einem Chip in der zurückgegebenen Tonerkassette Informationen über Art und Umfang der Nutzung gespeichert würden, die dann mit seiner Person verknüpft werden könnten. In diesem Zusammenhang hielt er einen Hinweis in der Datenschutzerklärung des Unternehmens, dass diese Verknüpfung nicht erfolgt, für erforderlich.

Nach Einholung entsprechender Auskünfte bei dem Elektronikunternehmen konnte ich dem Petenten mitteilen, dass die Erhebung seiner personenbezogenen Daten bei der Registrierung auf dessen Homepage auf der Grundlage des § 28 Abs. 1 Nr. 2 BDSG zulässigerweise erfolgt.

§ 28 Abs. 1 BDSG

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

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle

offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Das berechtigte Interesse des Unternehmens an der Erhebung der Daten ist begründet, weil nach § 23 Abs. 2 Nr. 5 KrWG das Unternehmen im Rahmen der Produktverantwortung verpflichtet ist, die nach Gebrauch eigener Erzeugnisse verbleibenden Abfälle zurückzunehmen und umweltverträglich zu verwerten oder zu beseitigen. Da die Rückname der Erzeugnisse nur für eigene Produkte gilt und zudem kostenlos erfolgt, liegt es aus wirtschaftlichen Gründen im Interesse des Unternehmens sicherzustellen, dass nur die eigenen Erzeugnisse angenommen und Fremdprodukte abgelehnt bzw. zurück gesendet werden können.

Für die Rücksendung ist die Angabe von Name und Adresse des Absenders notwendig, weshalb diese Daten bei der Registrierung anzugeben sind. Außerdem würde eine anonymisierte Rückgabe es leicht ermöglichen, in missbräuchlicher Weise den Rücknahmeservice des Unternehmens zu nutzen, um bspw. andere Abfälle, Chemikalien oder – wie bereits erwähnt – Drittprodukte auf diesem Wege „loszuwerden“.

Die Erhebung der E-Mail-Adresse ist für Rückfragen zur ordnungsgemäßen Abwicklung des Rücknahmeverfahrens erforderlich.

Ein Grund, wonach die schutzwürdigen Interessen des Betroffenen am Ausschluss der Verarbeitung gegenüber den berechtigten Interessen der verantwortlichen Stelle überwiegen, war für mich in diesem Zusammenhang nicht ersichtlich.

Das Unternehmen hat darüber hinaus nachvollziehbar dargelegt und versichert, dass die „Registrierungsdaten“ zweckgebunden nur zur ordnungsgemäßen Abwicklung des Rücknahmeverfahrens genutzt werden und keine Verknüpfung dieser personenbezogenen Daten mit den Informationen, die auf einem Chip der Tonerkassette gespeichert werden (Anzahl der Seiten der gedruckten Punkte und der Zeit des Motors, Produktionsdatum, Fabrik-ID, Tonernummer) erfolgt. Somit werden auch keine Rückschlüsse auf das Kundenverhalten gezogen.

Ein ausdrücklicher Hinweis in der Datenschutzerklärung, dass keine Verknüpfung der bei der Registrierung erhobenen personenbezogenen Daten mit den Informationen, die auf dem Chip der Tonerkassette gespeichert sind, stattfindet, wird im BDSG nicht verlangt.

Nach § 4 Abs. 3 Nr. 2 ist die verantwortliche Stelle verpflichtet, über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung zu informieren.

§ 4 BDSG

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist
der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

Das Unternehmen erläutert in seiner Datenschutzerklärung in sieben Punkten, zu welchen Zwecken es die erhobenen Kundendaten nutzt. Der Kunde kann also zunächst davon ausgehen, dass eine Nutzung zu anderen Zwecken nicht stattfindet. Gegenteilige Erkenntnisse sind nicht bekannt.

Das Unternehmen kann nicht verpflichtet werden, in seiner Datenschutzerklärung zu erläutern, welche Datennutzungen **nicht** erfolgen.

Ein Verstoß gegen datenschutzrechtliche Bestimmungen konnte also nicht festgestellt werden.

4.7.4
Kundendaten auf defektem, zurückgegebenem Notebook

Wird der Kaufvertrag über technisches Gerät mit einem Speichermedium, hier: Notebook, rückabgewickelt, muss der Verkäufer sicherstellen, dass etwaige darauf gespeicherte personenbezogene Daten des Käufers unwiederbringlich gelöscht sind, bevor es nach Reparatur durch Dritte genutzt wird bzw. erneut in den Handel gelangt.

Eine Petentin erwarb in der Filiale eines großen Elektrofachmarkts ein Notebook. Sie richtete darauf verschiedene E-Mail-Konten ein und ließ das Gerät auch zu ihrer Apple-ID bei Apple registrieren. Aufgrund eines Akku-Defektes konnte sie das Gerät jedoch nur kurz in Betrieb nehmen. Sie brachte es daher bereits am nächsten Tag wieder zu dem Elektrofachmarkt zurück. Der Verkäufer ging auf das Rückgabeersuchen der Petentin ein und zahlte den Kaufpreis zurück. Noch in ihrem Beisein überprüfte er, dass sich keine personenbezogenen Daten der Petentin auf dem Gerät befanden. Er prüfte auch, ob eine Registrierung bei Apple vorhanden war, was ggf. ein gebührenpflichtiges Zurücksetzen zur Folge gehabt hätte. Der Mitarbeiter konnte jedoch keine Verknüpfung des Geräts mit einer Apple-ID feststellen. Mit der Rückabwicklung des Kaufvertrages war die Angelegenheit für die Petentin zunächst erledigt. Bereits einige Wochen später erhielt sie jedoch eine E-Mail von einem Kunden desselben Elektrofachmarktes. Dieser hatte dort das von ihr zurück gegebene – zwischenzeitlich reparierte – Notebook als Neuware erworben. Bereits beim ersten Anschalten musste der neue Besitzer feststellen, dass es auf den Namen der Petentin bei Apple registriert war. Er konnte Einsicht in ihre alten und in einige neue Mails nehmen, obwohl diese von der Petentin über passwortgeschützte Mailkonten abgelegt waren. Der neue Besitzer informierte die Petentin darüber, dass ihre Daten und Konten offensichtlich nicht ordnungsgemäß gelöscht wurden. Die Petentin änderte daraufhin zunächst alle Passwörter und ließ ihre Kreditkarte, deren Daten im Rahmen der App-Stores verwendet wurden, sperren. Sie vereinbarte mit dem neuen Besitzer einen Termin im Elektrofachmarkt. Das Notebook wurde erneut zurück gegeben, und in Anwesenheit der Petentin und des neuen Besitzers wurden durch einen Mitarbeiter des Elektrofachmarktes alle Daten und Konten gelöscht.

Die Petentin informierte mich über den Vorfall mit der Bitte, dafür Sorge zu tragen, dass sich solche Vorfälle in dem Unternehmen künftig nicht mehr ereignen.

Ich habe den Elektrofachmarkt zu diesem Sachverhalt zur Stellungnahme aufgefordert. Insbesondere interessierte mich, wie es dazu kommen konnte, dass die Daten der Petentin auf dem Notebook noch vorhanden waren, welche Regelungen das Unternehmen hinsichtlich der Löschung von Nutzerdaten bei Rückgabe von Geräten mit Speichermedien getroffen hat und welche Maßnahmen das Unternehmen zu ergreifen gedenkt, damit solche Fehlleistungen wie im Fall der Petentin künftig vermieden werden.

Aus welchen Gründen das reparierte Notebook der Petentin wieder in den Verkauf gelangte, ohne das die Nutzerdaten ordnungsgemäß gelöscht waren, konnte das Unternehmen im Nachhinein nicht mehr aufklären.

Der betriebliche Datenschutzbeauftragte des Unternehmens erläuterte detailliert den sogenannten Clearingprozess (Datenlöschung) bei zurückgegebenen Geräten mit Speichermedien, auf denen noch Nutzerdaten gespeichert sein könnten.

Dabei obliegt es den Geschäftsführern der einzelnen Filialen zu entscheiden, ob der Clearingprozess von kompetenten Mitarbeitern im Filialmarkt durchgeführt oder ob der zertifizierte Dienstleister eingeschaltet wird, mit dem die Zentrale einen Vertrag nach § 11 BDSG abgeschlossen hat.

Bei Beauftragung des Dienstleisters kann nach Darstellung des betrieblichen Datenschutzbeauftragten mit ziemlicher Sicherheit ausgeschlossen werden, dass Geräte zurückkommen, auf denen die Nutzerdaten nicht ordnungsgemäß gelöscht wurden.
Für die Mitarbeiter in den Filialen hat das Unternehmen im Intranet im sogenannten Service-Handbuch die einzelnen Schritte des Clearingprozesses hinterlegt.

Wenn der Mitarbeiter diesen Weisungen folgt, ist ebenfalls auszuschließen, dass Nutzerdaten nicht ordnungsgemäß gelöscht werden. Hierin liegt jedoch ein Schwachpunkt, da je nach fachlicher Kompetenz des Mitarbeiters und Ausmaß der Beachtung des Handbuches Fehler wie im vorliegenden Fall nicht mit hinreichender Sicherheit ausgeschlossen werden können. Hinzu kommt, dass die Tatsache der ordnungsgemäßen Löschung nicht eindeutig nachvollziehbar gemacht ist.

Deshalb habe ich den betrieblichen Datenschutzbeauftragten aufgefordert, dafür Sorge zu tragen, dass die Geschäftsführer der einzelnen Filialen in entsprechenden Schulungen sensibilisiert, künftig nur zuverlässige und kompetente Mitarbeiter mit dem Clearingprozess beauftragt werden und die erfolgreiche Durchführung des Löschvorgangs durch entsprechende Hinweise in den Unterlagen oder am Gerät nachvollziehbar gemacht wird. Im Zweifel ist ein Clearing durch den zur Verfügung stehenden Dienstleister zu bevorzugen.

Das Verhalten, dass ein Mitarbeiter des Unternehmens die Nutzerdaten der Petentin nicht ordnungsgemäß gelöscht hat und damit ihre Daten an einen Dritten übermittelt wurden, habe ich als Verstoß gegen die Bestimmungen des BDSG ausdrücklich beanstandet.

4.8 Beschäftigtendatenschutz

4.8.1
Freunde des Bewerbers

Die Datenverarbeitung auf der Grundlage einer Einwilligung ist im Beschäftigungsverhältnis besonders problematisch. Aufgrund der Abhängigkeit des Arbeitnehmers von seinem Arbeitgeber mangelt es oft an der für eine wirksame Einwilligung erforderlichen Freiwilligkeit.

Sowohl nach den einschlägigen Vorschriften des BDSG als auch nach denen des HDSG ist die Einwilligung des oder der Betroffenen eine mögliche Grundlage für die Verarbeitung personenbezogener Daten. Voraussetzungen für die Wirksamkeit einer solchen Einwilligung sind, dass der Betroffene umfassend über die Verarbeitung seiner personenbezogenen Daten informiert wird und er in Kenntnis dessen aus freien Stücken in die Verarbeitung einwilligt.

§ 4a Abs. 1 Sätze 1 und 2 BDSG

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

§ 7 Abs. 2 Sätze 4 bis 6 HDSG

... 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.

Muss der Betroffene Nachteile befürchten, wenn er die Einwilligung nicht erteilt, ist in der Regel davon auszugehen, dass keine freie Entscheidung, wie sie vom Gesetz gefordert ist, vorliegt, was

die Einwilligung unwirksam macht. Die Datenverarbeitung kann auf eine solche Einwilligung nicht gestützt werden.

Im Bereich des Beschäftigtendatenschutzes wird die Problematik der Freiwilligkeit von Einwilligungserklärungen besonders offenbar. Auch wenn es in der Arbeitswelt immer wieder Situationen gibt, in denen tatsächlich von freiwilligen Einwilligungen seitens der Beschäftigten ausgegangen werden kann, so sind diese sicherlich die Ausnahme. In den meisten Fällen wird der Beschäftigte auf Grund seines Abhängigkeitsverhältnisses gegenüber dem Arbeitgeber einen gewissen Druck verspüren, in eine vom Arbeitgeber gewünschte Datenverarbeitung einzuwilligen. Dies gilt nicht erst dann, wenn bereits ein Beschäftigungsverhältnis besteht, sondern auch schon im Vorfeld, etwa im Rahmen der Bewerbung.

Konkret hat sich die Mutter eines Schülers an mich gewandt, der sich auf eine Lehrstelle bei einem Unternehmen beworben hatte, das Versicherungen vermittelt. Nach mehreren Runden des Auswahlverfahrens erhielt der Schüler eine Einladung zur nächsten Runde mit der nachdrücklich geäußerten „Bitte“, die Kontaktdaten von 100 Freunden mit zu bringen. Mutter und Sohn sahen sich in der Zwangslage, einerseits eine Lehrstelle finden zu müssen und andererseits „kein gutes Gefühl“ bei der Weitergabe der geforderten Kontaktdaten zu haben.

Da Mutter und Sohn es im konkreten Fall nicht für gänzlich ausgeschlossen hielten, dass es sich bei dieser Aufforderung um einen Test bezüglich der Sensibilität der Bewerber in puncto Datenschutz handeln könnte, sind wir so verblieben, dass der Sohn nur die Daten der Freunde, die ihm hierzu ihr Einverständnis erteilt hatten, zu dem nächsten Termin des Auswahlverfahrens mitnehmen wollte. Die zu den geforderten 100 Freunden fehlende Anzahl wollte er damit erklären, dass er für diese keine entsprechende Einwilligung seiner Freunde erhalten habe.

Über die Reaktion in der Firma bin ich leider nicht mehr informiert worden. Ich empfinde es ausdrücklich als lobenswert, dass der junge Mann unterstützt von seiner Mutter nicht bereit war, der Aufforderung des potenziellen Arbeitgebers kritiklos zu folgen und offensichtlich das nötige datenschutzrechtliche Bewusstsein hatte, um diesem Ansinnen zu begegnen, auch wenn eine gewisse Wahrscheinlichkeit dafür sprach, dass er hiermit seine Aussichten auf einen Ausbildungsplatz in diesem Unternehmen verschlechterte.

4.9 Gesundheitswesen

4.9.1
Datenschutz in der Arztpraxis

Im Berichtszeitraum habe ich aufgrund von Anfragen von Ärzten und Patienten Stellung genommen zur datenschutzgerechten Ausgestaltung der Datenverarbeitung in Arztpraxen und auch stichprobenhaft Prüfungen vorgenommen. Gegenstand der Diskussionen waren sowohl Fragen zu Umfang, Zweck und Art und Weise der Datenverarbeitung wie auch zu den angemessenen Datensicherheitsmaßnahmen.

Auf Anfragen und Beschwerden und bei stichprobenhaften Prüfungen habe ich zu Einzelfragen wie folgt Stellung genommen:

4.9.1.1
Routinemäßige Erstellung eines Fotos des Patienten

Der Arzt ist nach § 630f Abs. 2 BGB berechtigt und verpflichtet, die Behandlung des Patienten zu dokumentieren. Das neue Patientenrechtegesetz von 2013 enthält eine Regelung zum Umfang der Behandlungsdokumentation.

§ 630f Abs. 2 BGB

Der Behandelnde ist verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen.

Auch das Anfertigen von Fotografien kann im Einzelfall für die Durchführung einer Behandlung erforderlich sein und ist dann Bestandteil der Behandlungsdokumentation. Mit diesen Fotografien kann beispielsweise ein Heil- oder Behandlungsverlauf (etwa von Wunden) nachvollziehbar dokumentiert werden.

Allerdings erhielt meine Dienststelle in diesem Jahr eine Reihe von Anfragen, die andere Situationen betrafen. Den Beschwerden zufolge waren die Patienten bereits vor dem Beginn ihrer Be-

handlung fotografiert worden. Dies geschah in der Weise, dass am Empfangstresen ein Foto von ihrem Gesicht angefertigt wurde. Gespeichert wurde das Foto anschließend in der Patientenakte.

Die Nachfragen der Patienten zum Zweck des Fotos wurden von den Arzthelferinnen teils sehr lapidar mit einem „benötigen wir halt“ o.Ä. abgetan. In einem Fall, der einen Zahnarzt betraf, wurde aufgrund der Verweigerung des Lichtbildes sogar eine Behandlung abgelehnt.

Aufgrund der Beschwerden habe ich zunächst versucht zu klären, welchen Zweck der jeweilige Arzt mit den Fotos verfolgt. Die Antworten waren unterschiedlich. Überwiegend wird die Anfertigung entsprechender Patientenfotos damit begründet, dass hierdurch in Einzelfällen eine Verwechslungsgefahr ausgeschlossen werden oder der Arzt sich leichter an einen Patienten erinnern kann. Dies komme insbesondere bei einer Namensgleichheit mehrerer Patienten zum Tragen. Nicht nur bei der Aufnahme des Patienten, sondern auch bei internen Besprechungen oder bei der Anfertigung von Befunden könne man sich mittels des Fotos besser an einzelne Fälle erinnern.

In meinen Stellungnahmen habe ich zunächst klar zum Ausdruck gebracht, dass eine gesetzliche Grundlage für ein entsprechendes Vorgehen nicht existiert. Die Erstellung von Fotos zur Identifizierung des Patienten ist im Regelfall zur Durchführung der Behandlung nicht erforderlich. Sollte sich eine Praxis dennoch hierzu entschließen, bedarf dieses Vorgehen einer rechtswirksamen, d.h. insbesondere einer „informierten“ Einwilligung des Patienten. Es gilt insoweit die Regelung des § 4a Abs. 1 BDSG.

§ 4a Abs. 1 BDSG

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Die Patienten sind deshalb im Aufnahmebogen über den Sinn und Zweck des Fotos und die Art und Weise der weiteren Verwendung desselben zu informieren. Die Einwilligung bedarf der Schriftform. Es muss auch klar erkennbar sein, dass die Einwilligung freiwillig ist und sie abgelehnt oder auch später widerrufen werden kann.

Ebenso habe ich einen Zahnarzt darauf hingewiesen, dass ich eine Ablehnung der Behandlung im Falle der Verweigerung des Patientenfotos generell als unzulässig ansehe. Die Gründe, mit denen

der Zahnarzt/die Zahnärztin eine Behandlung ablehnen kann, sind in § 2 Abs. 5 der Berufsordnung für hessische Zahnärztinnen und Zahnärzte abschließend aufgezählt:

§ 2 Abs. 5 Berufsordnung für hessische Zahnärztinnen und Zahnärzte

Der Zahnarzt kann die zahnärztliche Behandlung ablehnen, wenn
a) eine Behandlung nicht gewissenhaft und sachgerecht durchgeführt oder
b) die Behandlung ihm nach pflichtgemäßer Interessenabwägung nicht zugemutet werden kann oder
c) er der Überzeugung ist, dass das notwendige Vertrauensverhältnis zwischen ihm und dem Patienten nicht besteht.

Diese Gründe sind bei der vorliegenden Situation nicht gegeben.

Aufgrund meiner Stellungnahmen haben die betroffenen Praxen entweder eine informierte Einwilligung der Patienten vorgesehen oder von der Anfertigung von Fotos abgesehen.

4.9.1.2
Papierdokumentation und/oder elektronische Dokumentation der Behandlung?

Zahlreiche Anfragen habe ich erhalten zu der Frage, ob und ggfs. unter welchen Voraussetzungen künftig auf eine Papierdokumentation der Behandlung verzichtet werden kann. In vielen Arztpraxen werden inzwischen die eigene Befunde (auch oder nur noch) elektronisch gespeichert. Fremdbefunde (etwa Labordaten) und Gutachten kommen teils elektronisch per Datenfernübertragung beim Arzt an, teils nach wie vor per Post oder Fax und werden dann eingescannt. Willenserklärungen/Einwilligungen der Patienten liegen häufig (auch) noch in Papierform vor. Nach meiner Erfahrung haben Arztpraxen oft ein großes Interesse daran, möglichst wenige Dokumente in Papierform zu archivieren.

So wird von Ärzten häufig die Frage gestellt, wie sie ihre Behandlung bei elektronischer Speicherung rechtssicher dokumentieren können.

Wenn **die eigenen Befunde** elektronisch dokumentiert werden, stellen sich neue Fragen, die geklärt werden müssen: Erforderlich ist ein Rollen- und Berechtigungskonzept für den Zugriff auf die Patientendaten sowie entsprechende technisch-organisatorische Datensicherheitsmaßnahmen. Darüber hinaus stellt sich insbesondere die Frage, wie Manipulationsgefahren begegnet wird. Sind

z.B. nachträgliche Änderungen/Ergänzungen der Behandlungsdokumentation revisionssicher im PVS-System dokumentiert?

In der Berufsordnung ist festgelegt, dass eine elektronische Dokumentation grundsätzlich zulässig ist und sie bestimmte Anforderungen erfüllen muss.

§ 10 Abs. 5 Berufsordnung für die Ärztinnen und Ärzte in Hessen

Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien bedürfen besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Ärztinnen und Ärzte haben hierbei die Empfehlungen der Ärztekammer zu beachten.

Das neue Patientenrechtegesetz enthält eine Regelung, die Manipulationen verhindern soll.

§ 630f Abs. 1 BGB

Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies ist auch für elektronisch geführte Patientenakten sicherzustellen.

Wenn z.B. **in Papierform eingegangene Fremdbefunde oder Einwilligungen der Patienten** elektronisch dokumentiert werden sollen, gibt es ebenfalls neue Fragen:

Wie werden Manipulationsgefahren beim Einscannen ausgeschlossen? So könnte z.B. ein eingescanntes Dokument einen Inhalt und eine Unterschrift aus zwei verschiedenen Dokumenten enthalten, ohne dass dies später nachvollzogen werden kann.

Das grundsätzliche Problem besteht darin, dass bei einer elektronischen Dokumentation die Möglichkeit verloren geht, Manipulationen festzustellen, z.B. zu prüfen, ob die elektronischen Dokumente ein korrektes Abbild des Originals sind. So ist etwa bei einem Papierdokument grundsätzlich eine Überprüfung durch einen Schriftsachverständigen denkbar, nicht jedoch bei einem elektronisch gespeicherten bzw. bei einem eingescannten elektronischen Dokument.

Es ist daher bei elektronischen Dokumenten kein sog. Urkundenbeweis i.S.v. § 416 ZPO möglich.

§ 416 ZPO

Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.

Für elektronisch gespeicherte Dokumente gelten vielmehr gem. § 371 Abs. 1 ZPO die Regelungen des Augenscheinbeweises.

§ 371 Abs. 1 ZPO

Der Beweis durch Augenschein wird durch Bezeichnung des Gegenstandes des Augenscheins und durch die Angabe der zu beweisenden Tatsachen angetreten. Ist ein elektronisches Dokument Gegenstand des Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten.

Die elektronisch gespeicherte Behandlungsdokumention unterliegt daher z.B. im Haftungsprozess der freien Beweiswürdigung durch das Gericht.

§ 286 Abs. 1 ZPO

Das Gericht hat unter Berücksichtigung des gesamten Inhalts der Verhandlungen und des Ergebnisses einer etwaigen Beweisaufnahme nach freier Überzeugung zu entscheiden, ob eine tatsächliche Behauptung für wahr oder für nicht wahr zu erachten sei. In dem Urteil sind die Gründe anzugeben, die für die richterliche Überzeugung leitend gewesen sind.

Lediglich auf elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden nach § 371a Abs. 1 ZPO die Vorschriften über die Beweiskraft privater Urkunden entsprechend Anwendung. Diese Möglichkeiten werden allerdings von den niedergelassenen Ärzten derzeit kaum genutzt.

Das dadurch bestehende Prozessrisiko für den Arzt kann reduziert werden durch technisch-organisatorische Maßnahmen, die eine möglichst fälschungssichere Organisation der elektronischen Dokumentation sicherstellen (z.B. durch entsprechende schriftliche Vorgaben zum Ablauf des Scannens und dessen Dokumentation). Die Bundesärztekammer und die Kassenärztliche Bundesvereinigung haben in ihren Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis von 2008 (Deutsches Ärzteblatt Heft 19, 9. Mai 2008 A 1026,

http://www.bundesaerztekammer.de/page.asp?his=0.7.47.6188) auch hierzu Empfehlungen veröffentlicht (4.4.1 und 4.4.2).

Grundsätzlich handelt es sich bei der Frage, welche Anforderungen an eine revisions- und manipulationssichere Behandlungsdokumentation gestellt werden sollten, primär nicht um eine datenschutzrechtliche, sondern um eine arztrechtliche Frage. Aus datenschutzrechtlicher Sicht kann lediglich auf die Problematik hingewiesen werden. Letztendlich ist es insbesondere Aufgabe der Landesärztekammern, gegenüber den Ärzten Empfehlungen auszusprechen. Auf meine Nachfrage hat die Landesärztekammer Hessen zur aktuellen Situation in den Arztpraxen nicht Stellung genommen, hat aber darauf hingewiesen, dass gegenwärtig die o.a. Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung überarbeitet werden und auch dieses Thema dabei erneut aufgegriffen wird. Wann die überarbeiteten Empfehlungen vorliegen, sei jedoch noch nicht absehbar. Bis dahin erscheint eine Hybridspeicherung zumindest von Teilen der Behandlungsdokumentation eine gute Möglichkeit, Risiken zu vermeiden.

Hinweisen möchte ich noch auf ein Projekt der Landesärztekammer Hessen. Die Landesärztekammer Hessen führt einen elektronischen Arztausweis ein, der es erlaubt, elektronische Dokumente mit einer qualifizierten elektronischen Signatur zu versehen (http://www.laekh.de/presse/pressemitteilungen/aktuelle-pms/presse_2013_02_13_sichere_arztbriefe.html). Damit kann insbesondere ein Arztbrief als elektronisches Dokument rechtssicher signiert werden. Als Empfänger kann man einen solchen Arztbrief problemlos in eine elektronische Behandlungsdokumentation einbinden. Allerdings würde sich das Problem des Medienbruchs ergeben, wenn der (ausgedruckte) Arztbrief in eine Papierdokumentation eingefügt wird. In diesem Fall könnte kein Urkundenbeweis geführt werden.

Der neue Arztausweis und die einhergehende Infrastruktur wird noch eine weitere Neuerung mit sich bringen. Ärzte können dann untereinander verschlüsselte e-Mails versenden, wodurch eine unbefugte Kenntnisnahme verhindert würde. Dadurch würden erhebliche Datensicherheitsprobleme bei der Kommunikation zwischen Ärzten beseitigt.

4.9.1.3
Verwendung von AGBs in Arztpraxen – zulässiger Inhalt

Einige Arztpraxen geben ihren Patienten allgemeine Geschäftsbedingungen zur Kenntnis. Auch zu diesem Thema hat meine Dienststelle Anfragen und Beschwerden erhalten.

Eine Bürgerin beschwerte sich z.B. darüber, dass sie von einer Praxis nach ihrem Besuch einen Newsletter erhielt, ohne diesbezüglich je eine Einwilligung erteilt zu haben.

Näheres hierzu konnte ich den Allgemeinen Geschäftsbedingungen der Praxis entnehmen:
„Der Patient willigt mit Abschluss des Behandlungsvertrages ausdrücklich darin ein, zu Informations-, Termin-, Recall- und medizinischen Zwecken von der Praxis schriftlich, fernmündlich oder per Telefax, SMS oder E-Mail kontaktiert zu werden."

Wie sich herausstellte, wurden die AGB in der Praxis für die Patienten zur Kenntnisnahme ausgelegt. In dem übersandten Anmeldungsbogen war lediglich der Passus „Es gelten unsere Allgemeinen Geschäftsbedingungen (AGB, siehe Aushang)" enthalten.

Eine Aushändigung der Allgemeinen Geschäftsbedingungen an die Patienten erfolgte dahingegen nicht.

Dieses Vorgehen wurde von mir beanstandet, weil es nicht die Anforderungen des § 4a BDSG erfüllt.

§ 4a Abs. 3 BDSG

Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Meine Beanstandung bezog sich auf die folgenden Regelungen:

– Der Patient ist damit einverstanden, dass seine Behandlungsdaten und Befunde durch den Arzt an seinen Hausarzt/weiterbehandelnden Arzt/sein weiterbehandelndes Krankenhaus zu Dokumentations- und Weiterbehandlungszwecken, auch auf elektronischem Wege, übermittelt werden können. Er ist des Weiteren damit einverstanden, dass bei dem Hausarzt/ vorbehandelnden Arzt/vorbehandelnden Krankenhaus vorliegende Behandlungsdaten und Befunde durch den Arzt, auch auf elektronischem Wege, angefordert werden können, soweit diese für die Behandlung erforderlich sind.

– Der Patient willigt mit Abschluss des Behandlungsvertrages in die Weitergabe seiner Daten zum Zwecke der ärztlichen Information und Rechnungsstellung an für die Durchführung labormedizinischer oder pathologisch-anatomischer Leistungen beauftragte Ärzte ein. Er erklärt sich mit Abschluss des Behandlungsvertrages ausdrücklich mit der Beauftragung dieser Ärzte

für medizinisch notwendige Untersuchungen einverstanden und willigt in die Bezahlung der dadurch entstehenden Honorare ein.

– Der Patient willigt mit Abschluss des Behandlungsvertrages ausdrücklich darin ein, zu Informations-, Termin-, Recall- und medizinischen Zwecken von der Praxis schriftlich, fernmündlich oder per Telefax, SMS oder E-Mail kontaktiert zu werden.

– Der Patient willigt mit Abschluss des Behandlungsvertrages in die Weitergabe seiner Daten zum Zwecke der Rechnungsstellung an die der Schweigepflicht unterliegende Privatärztliche Abrechnungsstelle PRIVA GmbH in 63688 Gedern ein.

Entsprechende Bedenken werden auch in einem Urteil des OLG Düsseldorf vom 04. März 1994 wiedergegeben (Az.: 22 U 257/93, NJW 1994, 2421).

Dem Gericht zufolge kann eine stillschweigende Einwilligung der Patienten in die Übermittlung ihrer Daten an eine Verrechnungsstelle nicht aufgrund eines Aushangs im Wartezimmer des Arztes, in welchem auf eine solche Übung hingewiesen wird, angenommen werden.

Das Gericht hält einen solchen Aushang nicht für ausreichend. Zum einen kann nicht beurteilt werden, ob er von seinem Inhalt her überhaupt geeignet war, die Patienten hinreichend zu informieren und ihnen, wie für ein wirksames Einverständnis im Sinne von § 203 Abs. 1 Nr. 1 StGB unerlässlich, eine im Wesentlichen zutreffende Vorstellung davon zu vermitteln, worin sie einwilligen, und sie in die Lage zu versetzen, Bedeutung und Tragweite ihrer Entscheidung zu überblicken. Zum anderen kann gerade bei Personen, die als Patienten eine Arzt- oder Zahnarztpraxis aufsuchen, nicht ohne weiteres davon ausgegangen werden, dass sie sämtlichen Aushängen im Wartezimmer Aufmerksamkeit schenken.

Im Übrigen ist in dem besagten Urteil auch festgehalten, dass es im Hinblick auf die ärztliche Schweigepflicht dem Arzt obliegt, die Zustimmung des Patienten in eindeutiger und unmissverständlicher Weise einzuholen. Vor diesem Hintergrund wäre es auch nicht ausreichend gewesen, wenn die Allgemeinen Geschäftsbedingungen an die Patienten ausgehändigt worden wären. Zur eigenen Sicherheit des Arztes – insbesondere zu Dokumentationszwecken – war bezüglich der angeführten Regelungen eine handschriftliche Erklärung einzuholen.

Auf meine Anfrage teilte die Landesärztekammer Hessen mit, dass sie meine Rechtsauffassung teilt. Die aufgezeigten Regelungen waren auch nach Ansicht der Kammer nicht mit § 4a BDSG zu vereinbaren. Konkret wurden die fehlende Bestimmtheit der Einwilligungserklärung sowie die fehlenden Voraussetzungen des § 4a Abs. 1 S. 4 BDSG bemängelt.

Als unzulässig habe ich auch einen Passus in den AGB bzw. im Anmeldebogen angesehen, der darauf „hinweist“ oder die Einwilligung vorsieht, dass die Behandlungsunterlagen an einen möglichen Praxisnachfolger weitergegeben werden. Ein „Hinweis“ kann keine Rechtsgrundlage sein für eine Weitergabe der Behandlungsunterlagen an den Praxisnachfolger. Und eine solche Einwilligung kann nicht als „informierte“ Einwilligung bewertet werden, da der Umfang der Behandlungsunterlagen, der Zeitpunkt der Übergabe und insbesondere der konkrete Empfänger der Daten dem Patienten zum Zeitpunkt der Unterschrift nicht bekannt sind.

4.9.1.4
Ausgestaltung der Einwilligung in die Weitergabe von Patientendaten an eine Ärztliche Verrechnungsstelle

4.9.1.4.1
Übermittlung von Patientendaten an private Abrechnungsdienste

Die Weitergabe von Patientendaten an externe ärztliche Verrechnungsstellen erfordert grundsätzlich eine schriftliche Einwilligung des Patienten. Bei der Ausgestaltung des Formulars ist zu beachten, dass

– klar erkennbar ist, an welches private Unternehmen zu welchem Zweck welche Daten in welchem Umfang übermittelt werden,
– die Erklärung für den Fall, dass sie zusammen mit anderen Erklärungen abgegeben wird, deutlich hervorgehoben wird und
– darauf hingewiesen wird, dass die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann.

Eine weitere Besonderheit ist für den Fall zu beachten, dass ein Befund an einen Laborarzt geht, der wiederum seinerseits über eine externe Verrechnungsstelle abrechnet.

Meist wird der Patient in diesen Fällen den Laborarzt nicht persönlich kennen. Der Erstbehandler hat daher regelmäßig über die spätere Weitergabe aufzuklären und im Vorfeld der Behandlung die Einwilligung des Patienten einzuholen. Hier gilt der Grundsatz, dass sofern die Weitergabe von patientenbezogenen Daten an einen Konsiliararzt (z.B. Laborarzt) ohne hinreichend bestimmte Einwilligung des Patienten nicht erlaubt ist (siehe hierzu LG Düsseldorf, Urteil vom 03. November 1995, Az.: 20 S 58/95), die Weitergabe an eine ärztliche Verrechnungsstelle durch den Konsiliararzt ohne Einwilligung des Patienten angesichts von § 203 Abs. 1 Nr. 6 StGB erst recht unzulässig ist.

4.9.1.4.2
Einschaltung von Inkassobüros und sonstige Vereinbarungen mit Patienten

Immer häufiger finden sich in Musterformularen betreffend die externe Abrechnung einer Arztpraxis auch Klauseln zur Einschaltung von Inkassobüros. Im Falle einer Zahnarztpraxis habe ich dies zum Anlass genommen, mich genauer mit einem solchen Formular zu beschäftigen.

Ebenso wie für den Bereich der externen Abrechnung gilt auch für den Fall der Forderungsabtretung an Inkassounternehmen der Grundsatz, dass die Patienten rechtzeitig und umfassend über die beabsichtigte Verwendung und Weitergabe ihrer Daten informiert werden müssen. Da hier regelmäßig auch Gesundheitsdaten tangiert sind, muss insbesondere § 4a Abs. 3 BDSG Beachtung finden. Dieser sieht vor, dass im Einwilligungstext auch ausdrücklich die sensiblen Daten, die Gegenstand der Einwilligung sind, benannt werden müssen. Der Begriff Gesundheitsdaten ist mithin zu präzisieren. Die Weitergabe ist auf die erforderlichen Daten zu beschränken.

Inkassounternehmen benötigen zur außergerichtlichen Beitreibung von Forderungen keine kompletten Befund- oder Therapieberichte. Hier genügen in der Regel die personenbezogenen Daten des Patienten und die sich aus der Rechnung ergebenden Informationen zu den durchgeführten Behandlungsmaßnahmen.

Von dieser Konstellation zu unterscheiden ist der Fall, dass der Arzt weiterhin Forderungsinhaber bleibt und das Inkassobüro lediglich im Auftrag des Arztes tätig wird. Auch in diesem Fall werden keine genaueren Behandlungsdaten benötigt. Allerdings bedarf es hier auch keiner schriftlichen Einwilligung des Patienten zur Einschaltung des Inkassounternehmens, wenn der Arzt bereits in einem zweiten Mahnschreiben wiederholt die Einschaltung eines Inkassounternehmens zur Durchsetzung ankündigt. Da in diesem Fall letztlich kein Forderungserwerb eintritt, stehen dem Inkassounternehmen ohnehin keine weiteren Informationen aus der Patientenakte zu.

In mir vorliegenden Formularen ist auch häufig der Hinweis auf das mögliche Einholen einer Information einer Auskunftei zur Prüfung der Bonität anzutreffen. Mangels gesetzlicher Erlaubnisnormen hierzu ist auch dies nur mit der ausdrücklichen Einwilligung des Patienten möglich.

Fraglich ist in diesem Zusammenhang nur, ob die entsprechende Einwilligung gesondert eingeholt werden muss, anderenfalls könnte dies als Überraschungsklausel im Sinne des § 305c BGB aufzufassen sein. Diesbezüglich empfehle ich eine „Kästchenlösung“ mit gesonderter Ankreuzmöglichkeit. Sofern die Zusammenarbeit mit einer bestimmten Auskunftei erfolgt, ist diese auch mit Namen und Anschrift in die Einwilligungserklärung aufzunehmen. Anderenfalls genügt der Hinweis auf wechselnde Auskunfteien.

Der behandelnde Arzt sollte darauf achten, dass eine Bonitätsprüfung nur dann erfolgt, wenn auch tatsächlich mit erhöhten Kosten zu rechnen ist (konkreter Kostenvoranschlag). Für eine prophylaktische Abfrage, unabhängig von dem jeweiligen Behandlungsfall, sehe ich keine Erforderlichkeit, die mit den Grundsätzen des Datenschutzes vereinbar wäre.

Einen besonderen Blick habe ich auch auf die häufig anzutreffende Regelung gerichtet, welche Forderungen an die refinanzierende Bank abgetreten werden können.

Grundsätzlich halte ich es für bedenklich, wenn die Einwilligung auf die Finanziers der Verrechnungsstelle ausgedehnt wird. Die Bedenken beziehen sich hierbei im Wesentlichen auf die Weitergabe von Patientendaten an ein Kreditinstitut, die hiermit einem größeren Personenkreis zugänglich gemacht werden können.

Diese Bedenken haben mich dazu veranlasst, mir die in diesem Zusammenhang stattfindenden Prozesse von einer zahnärztlichen Verrechnungsstelle aus Baden-Württemberg näher erläutern zu lassen.

Hierzu wurde mir mitgeteilt, dass de facto in der Vergangenheit nie entsprechende Behandlungsdaten an die Bank übermittelt worden seien. Es bestehe jedoch eine theoretische Möglichkeit, weshalb eine entsprechende Klausel in die Verträge aufgenommen wurde. Mir wurde jedoch versichert, dass mit der Bank, die Vertragspartner ist, eine ausdrückliche vertragliche Vereinbarung zu diesem Bereich getroffen wurde. Diese Vereinbarung sehe vor, dass diese gemäß § 402 BGB auf ihr Einsichtsrecht in die der ärztlichen Schweigepflicht unterliegenden Patienteninformationen und Behandlungsdaten verzichte.

Auch wenn Gerichte entsprechende Klauseln – im Falle einer informierten Einwilligung des Patienten – für zulässig angesehen haben, halte ich dies für datenschutzrechtlich bedenklich. Unbestritten unterliegt die Arztpraxis Aspekten des wirtschaftlichen Arbeitens. Dennoch ist daran zu erinnern, dass sowohl Ärzte als auch Zahnärzte nach dem aus ihrer Berufsordnung hervorgehenden Selbstverständnis kein Gewerbe betreiben. Mit jeder – auch von einer Einwilligung abgedeckten – Weitergabe von Patientendaten an eine weitere Institution sind immer auch Risiken verbunden, mit denen das besondere Vertrauensverhältnis zwischen Arzt und Patient belastet wird.

Ich rate daher dazu, von derartigen Vereinbarungen mit dem Patienten abzusehen.

4.9.1.5
Verwendung von Smartphones bei Hausbesuchen

Moderne, mittlerweile weit verbreitete Kommunikationsmittel wie Smartphones oder Tablet-PCs – beispielsweise iPads – werden oft als Beitrag eingeschätzt, die Behandlungsqualität zu verbessern. Sofern dieses „Plus“ an Behandlungsqualität mit moderner Technik einhergeht, erfordert dies jedoch auch immer einen besonderen Blick für den Datenschutz.

Die Eingabe eines Verbandes beschäftigte sich folgerichtig mit der Frage, ob behandlungsbezogene Fotos auch auf dem Handy oder dem iPad gespeichert werden dürfen. Gerade bei Hausbesuchen kann dies eine Möglichkeit darstellen, komplexere Erkrankungen zwecks genauerer Abklärung zu dokumentieren.

Zu dieser Frage habe ich dem eingebenden Verband mitgeteilt, dass eine Speicherung von behandlungsbezogenen Fotos auf einem Handy oder iPad nur für kurze Zeit, und zwar bis zur Überspielung auf den Praxisrechner akzeptiert werden kann. Die Übertragung hat dabei per USB-Kabel oder Ende-zu-Ende-verschlüsselt mit nach dem Stand der Technik sicheren Verfahren stattzufinden.

Hinsichtlich der Verwendung von Smartphones oder Tablet-PCs im Alltag des Arztes werden sich künftig sicher noch mehr Fragen stellen. Hinzuweisen ist grundsätzlich auf die Handreichung auf meiner Homepage, die sich mit weiteren Punkten befasst, die bei der beruflichen Nutzung entsprechender Geräte zu beachten sind (www.datenschutz.hessen.de/tf015.htm).

4.9.1.6
Zulässigkeit der Mitnahme von Krankenhauspatientendaten in die neue eigene Praxis – Verwendung der Daten zur Information der Patienten über die neue Adresse

Aufgrund von zwei Eingaben aus dem letzten Jahr habe ich mich auch mit der Frage beschäftigt, inwiefern Ärzte/ Ärztinnen auch noch nach dem Wechsel ihres Arbeitsplatzes ihre ehemaligen Patienten kontaktieren dürfen. Die Eingebenden zeigten sich insoweit überrascht, als sie nach mehreren Jahren Post ihrer ehemaligen Behandler von einem neuen Tätigkeitsort aus erhielten.

In den mir vorgelegten Schreiben ging es im Wesentlichen darum, die Patienten über den neuen Wirkungsort und die dort angebotenen Therapien und Behandlungen zu informieren.

Es wurde nun bei mir angefragt, ob eine „Mitnahme“ der Patientendaten zulässig gewesen sei und ob diese Daten durch die besagten Schreiben nicht für eine unzulässige Werbung zweckentfremdet wurden.

Zur Beantwortung dieser Frage habe ich das Folgende mitgeteilt:
Soweit ein liquidationsberechtigter Arzt eines Krankenhauses im Rahmen eines sogenannten „gespaltenen Aufnahmevertrages“ die ärztlichen Leistungen erbringt, ist er auch für die anschließende Aufbewahrung der Patientenunterlagen verantwortlich. Bei dieser Konstellation schließt der (Privat-)Patient einen eigenen Behandlungsvertrag mit dem jeweiligen (Chef-)Arzt. Die ärztliche Versorgung gehört damit nicht zu den Leistungen des Krankenhauses. Diese beschränkt sich vielmehr auf Leistungen wie Unterbringung, Verpflegung, Bereitstellung der erforderlichen technisch-operativen Einrichtungen etc.

Nach den mir vorliegenden Informationen waren in beiden Fällen entsprechende Verträge geschlossen worden.

Dem behandelnden Arzt steht damit auch noch nach Beendigung der Tätigkeit im Krankenhaus ein entsprechender Zugriff auf die Patientendaten zu. Eine andere Bewertung ist lediglich dann vorzunehmen, wenn ein sogenannter „totaler Krankenhausaufnahmevertrag“ geschlossen wurde. Bei diesem gehört auch die ärztliche Versorgung zu den Leistungen des Krankenhauses. Dem Krankenhaus obliegen insoweit sämtliche Pflichten aus dem Behandlungsvertrag, u.a. auch die Aufbewahrung der Patientenunterlagen.

Diese Bewertung deckt sich auch mit einer Stellungnahme der Landesärztekammer Hessen zur Mitnahme von Patientendaten.

Auch die Schreiben selbst wurden von mir nicht beanstandet. Sie ließen sich aufgrund ihres lediglich informativen Charakters in den Kontext der früheren Behandlung einordnen. Letztlich dürfen Patientendaten in dem Umfang genutzt werden, wie dies dem Behandlungsvertrag zwischen Arzt und Patient dient. In beiden Konstellationen trug das Schreiben dazu bei, über die neue Wirkungsstätte des Arztes zu informieren, damit bei Bedarf eine Weiterbehandlung erfolgen kann. Zudem ging dem Patienten damit der Hinweis zu, wo er Informationen zu seinen vergangenen Behandlungen erhalten kann.

Bezüglich der geschilderten Praxis bestanden daher keine datenschutzrechtlichen Bedenken. Gleichwohl zeigt der Fall, dass Ärzte im Einzelfall prüfen müssen, ob sie aufgrund der vergangenen vertraglichen Situation zu einer Mitnahme von Patientendaten bei Beendigung ihres Arbeitsverhältnisses berechtigt sind.

4.9.1.7
Datenschutzgerechte Ausgestaltung des Empfangsbereichs

Aus datenschutzrechtlicher Sicht ist der Empfangsbereich ein besonders sensibler Bereich einer Arztpraxis. Dieser ist häufig Gegenstand von Diskussionen und Anfragen an meine Dienststelle. Der Patient hat hier in der Regel den ersten Kontakt mit dem Praxisteam und möchte Grundsätzliches zu seinem Besuch oder seiner Erkrankung mitteilen. Hierbei mag dem einen oder anderen schon die Frage in den Sinn gekommen sein, ob wartende Personen am Empfangstresen oder auch im Wartebereich einzelne Angaben mithören können.

Der Arzt muss seine Arztpraxis so organisieren, dass persönliche Angaben von Patienten von anderen Besuchern der Praxis nicht zur Kenntnis genommen werden können. Dieser Grundsatz ist insbesondere bei der räumlichen Gestaltung und bei der Arbeitsorganisation zu berücksichtigen.

Ganz allgemein sollte es vermieden werden, dass sich zu viele Patienten am Wartetresen aufhalten und fremde Anliegen mithören könnten. Dies kann in der Regel dadurch erreicht werden, dass eine Diskretionszone geschaffen wird, so dass jeweils nur ein Patient am Empfang vorsprechen kann. Die Umsetzung kann beispielsweise mittels eines gespannten Seils oder eines Hinweisschildes erfolgen. Wichtig ist lediglich, dass der abgetrennte Bereich als solcher erkennbar ist.

Unabhängig von den baulichen Gegebenheiten besteht grundsätzlich in jeder Praxis die Möglichkeit, eine entsprechende Diskretionszone einzurichten. Ebenso ist ein Augenmerk darauf zu richten, dass Empfangs- und der Wartebereich nicht ineinander übergehen, sondern voneinander abgetrennt sind.

Die Umsetzung datenschutzrechtlicher Gesichtspunkte in der Arztpraxis muss mithin nicht immer einen Kostenfaktor darstellen. Die datenschutzgerechte Ausgestaltung des Wartebereichs kann in der Regel mit relativ einfachen Mitteln umgesetzt werden.

4.9.2
Neues Merkblatt der Landespsychotherapeutenkammer für Hinterbliebene verstorbener Mitglieder

Im Falle einer fehlenden Nachfolgeregelung durch ein verstorbenes Kammermitglied haben die Erben die Aufbewahrungspflicht als vertragliche Nebenpflicht aus dem Behandlungsvertrag zu erfüllen. Gemäß § 203 Abs. 3 S. 2 StGB gilt die gesetzliche Schweigepflicht hierbei auch für die

Erben. Sofern sich digitale Daten im Nachlass befinden, sind bei der anschließenden Verwahrung einige Besonderheiten zu beachten.

4.9.2.1
Hintergrund

Auch im vergangenen Jahr war ich wieder häufig in beratender Funktion gegenüber einzelnen Kammern und Verbänden aus dem Gesundheitswesen tätig. Hierzu gehörte auch die Landespsychotherapeutenkammer Hessen. Gegenstand der Beratung war unter anderem das Merkblatt „Hinweis für Hinterbliebene verstorbener Mitglieder der hessischen Psychotherapeutenkammer zum Umgang mit Patientendaten“. Hier galt es unter anderem, das Merkblatt an zwischenzeitlich veränderte technische Gegebenheiten anzupassen.

4.9.2.2
Datenschutzrechtliche Vorgaben

Ein besonderes Anliegen war es mir zunächst, dass in dem Merkblatt noch einmal deutlich hervorgehoben wird, dass nach § 203 Abs. 3 S. 2 StGB auch der Erbe zur Beachtung des beruflichen Geheimnisses verpflichtet ist. Dies gilt mithin auch dann, wenn der Erbe selbst kein Arzt bzw. keine Ärztin ist. Der Gesetzgeber geht letztlich von einem Fortwirken der besonderen Vertrauensbeziehung zwischen Arzt und Patient aus. Auch nach dem Tode des Arztes muss diese durch dessen Erben gewährleistet werden.

Eine Einsicht in die Patientenakte durch den Erben ist damit nur mit der Einwilligung des jeweiligen Patienten möglich. Das gleiche gilt für die Herausgabe der Patientenakte an Dritte, sofern keine gesetzliche Grundlage hierfür existiert.

In der Regel werden die Erben darum bemüht sein, die Patientendokumentation in die Obhut von in der Region niedergelassenen Psychotherapeuten bzw. Psychotherapeutinnen zu geben. Der Aufgabenschwerpunkt liegt damit für die Erben regelmäßig in der ordnungsgemäßen Verwahrung der Patientenakten bis zu diesem Zeitpunkt.

Im Falle von Papierakten lässt sich dies relativ einfach durch die Aufbewahrung in einem verschlossenen Raum gewährleisten. Hier ist in erster Linie sicherzustellen, dass keine anderen Personen Zutritt zu diesen Räumlichkeiten haben.

Da allerdings auch in psychotherapeutischen Praxen zunehmend digitale Speichermedien Verwendung finden, stellt sich die Frage nach den hier zu beachtenden Besonderheiten bei der Verwahrung durch die Erben.

Auf die folgenden Punkte zum Umgang mit digitalen Dateien habe ich die Kammer hierbei aufmerksam gemacht:

– Die Daten von Patienten dürfen nicht „in der Cloud“ gespeichert werden.

– Ein Rechner, auf dem die Daten gespeichert sind, sollte nicht vernetzt sein und ebenso wie portable Speichermedien an einem sicheren Ort untergebracht werden.

– Die Daten selbst müssen verschlüsselt gespeichert werden. Hierzu ist ein etabliertes Verschlüsselungsprogramm mit einem anerkannt sicheren Algorithmus zu nutzen (z.B. AES oder 3DES).

– Der Schlüssel für die Verschlüsselung wird oft aus einem Passwort abgeleitet. In diesem Fall sollte das Passwort länger als elf Stellen sein und alle Zeichen (Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen) umfassen. Das Passwort selbst sollte nicht zusammen mit dem Speichermedium hinterlegt werden.

Selbstverständlich können durch ein entsprechendes Merkblatt nicht alle Fragen im Detail erörtert werden. Zu begrüßen ist es insoweit, dass die Landespsychotherapeutenkammer Hessen auf ihrem Merkblatt auch ausdrücklich anbietet, Erben eines Praxisinhabers bei einzelnen Fragen zu beraten.

4.9.2.3
Alternative Regelungsmöglichkeiten

Zum Teil werden Erben mit den hier dargelegten Aufgaben zunächst überfordert sein. An dieser Stelle soll deshalb noch auf ein alternatives Modell aufmerksam gemacht werden, das seitens der Psychotherapeutenkammer Niedersachsen Ende 2012 umgesetzt wurde (siehe hierzu die Mitteilungen der Psychotherapeutenkammer Niedersachsen, in: Psychotherapeutenjournal 1/2013). Das zugrundeliegende Konzept könnte sich auch für andere Heilberufskammern des Landes Hessen empfehlen.

Ein Hauptanliegen des Modells ist es, Familienangehörige und Erben von Psychologischen Psychotherapeuten und Kinder- und Jugendlichen-Psychotherapeuten vor dem Vorwurf einer Schweigepflichtverletzung bei plötzlicher Verhinderung oder Tod des Praxisinhabers berufsrechtlich und strafrechtlich zu schützen. Zudem sollen Patienten, Krankenkassen oder beispielsweise Rentenversicherungen möglichst schnell eine fachkundige Antwort auf ihre Anfragen erhalten können. Ergänzend wird angeführt, dass gerade in diesem Beruf die Begleitung eines Patienten bei der Akteneinsicht besondere Kenntnisse und Fähigkeiten erfordere.

Zu diesem Zweck wurde die Berufsordnung dahingehend geändert, dass alle Mitglieder verpflichtet werden, schon zu Lebzeiten einen approbierten Kollegen als Beauftragten und Ansprechpartner für den Verhinderungs-/Todesfall zu benennen. Durch diese „Meldepflicht“ kann insbesondere den Patienten ohne größeren Zeitverlust ein kompetenter Ansprechpartner benannt werden. Der benannte Kollege übernimmt damit faktisch die Funktion des Erben.

Zum Zeitpunkt meiner Anfrage an die Psychotherapeutenkammer Niedersachsen Ende diesen Jahres konnte noch kein abschließendes Fazit zu dem neuen Verfahren gezogen werden. Ich werde jedoch im nächsten Jahr noch einmal um einen kurzen Erfahrungsbericht bitten.

5. Bilanz

5.1
Löschung im SAP R/3 HR-System (41. Tätigkeitsbericht, Ziff. 3.3.6.1)

5.1.1
Löschung von Abwesenheitsdaten (Urlaubs- und Krankheitsdaten)

In meinem 41. Tätigkeitsbericht, Ziff. 3.3.6.1 habe ich festgestellt, dass 2.968 löschbare Datensätze mit Urlaubs- und Krankheitsdaten nicht gelöscht waren. Dies war eine deutliche Verbesserung der feststellbaren Fälle, über die ich in meinem 40. Tätigkeitsbericht, Ziff. 3.10.3 berichtet hatte. Ursprünglich handelte es sich um 7.559 nicht gelöschte Datensätze.

Leider musste ich jetzt feststellen, dass trotz der detaillierten Darstellung der Problematik in meinem 41. Tätigkeitsbericht, die Löschung von Urlaubs- und Krankheitsdaten immer noch nicht konsequent durchgeführt wird: Eine Auswertung zum Stichtag 14.11.2013 hat ergeben, dass wiederum 2.834 löschbare Fälle nicht bearbeitet wurden.

Die Gründe hierfür kann ich nicht nachvollziehen. Eine Erklärung für das rechtswidrige Verhalten konnte mir auch von der zuständigen Mitarbeiterin, die im Hessischen Competence Center (HCC) für die technische Umsetzung des Löschlaufs Verantwortung trägt und die zuständigen Behörden betreut, nicht gegeben werden. Nur so viel: Die Personal führenden Stellen haben die Freigabe für die Löschung der Daten nicht erteilt, sind also nicht tätig geworden. Damit konnte also im HCC die Löschung nicht durchgeführt werden.

Ich werde die Stellen, bei denen die Löschungen permanent nicht durchgeführt werden, nach § 29 Abs. 1 HDSG „vor Ort“ überprüfen um festzustellen, ob es nachvollziehbare Hinderungsgründe gibt.

§ 29 Abs. 1 HDSG
Alle datenverarbeitenden Stellen und ihre Auftragnehmer sind verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

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

Sollte dies nicht der Fall sein, werde ich umgehend eine Beanstandung gem. § 27 HDSG aussprechen.

§ 27 HDSG

(1) Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,
2. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Hessische Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Mit der Beanstandung kann der Hessische Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Hessischen Datenschutzbeauftragten getroffen worden sind. Die in Abs. 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Hessischen Datenschutzbeauftragten zu.

Bei folgenden Buchungskreisen ist die Anzahl der nicht gelöschten Datensätze signifikant erhöht:

Vorsorgekasse (betrifft alle Ressorts)	1.110 Fälle
Schulbereich	869 Fälle
Bildungsverwaltung	167 Fälle
Immobilienmanagement	155 Fälle
Polizeipräsidien	107 Fälle

Ministerium HKM	85 Fälle
Justizvollzug	69 Fälle
Historisches Erbe	49 Fälle

5.1.2
Löschung ganzer Datensätze

Das Programm zum „Löschen ganzer Datensätze“ im SAP R/3 HR-System wurde im Frühjahr 2013 fertig gestellt und produktiv gesetzt.

Eine Auswertung, die mir nach Anforderung von dem für die technische Umsetzung der Löschung zuständigen Hessischen Competence Center (HCC) zur Verfügung gestellt wurde, hat erfreulicherweise ergeben, dass 7.849 Datensätze gem. § 107f HBG gelöscht wurden.

§ 107f HBG

(1) Personalakten sind nach ihrem Abschluss von der Personalakten führenden 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 An-

spruchs, sind die Akten dreißig Jahre aufzubewahren.

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

Bei 885 Datensätzen wurde durch die Personal führenden Dienststellen ein Sperrvermerk gesetzt, der dazu geführt hat, dass die Löschung programmtechnisch verhindert wurde. Ich gehe davon aus, dass die Gründe dafür rechtlich begründbar sind, und werde eine entsprechende Auswertung veranlassen, um zu prüfen, ob die Sperrung berechtigt vorgenommen wurde.

Bei diesem Löschverfahren kann ich feststellen, dass die Personal führenden Stellen die Löschung zeitnah und konsequent durchgeführt haben.

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

6.1
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13./14. März 2013

Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

– Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.

– Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen bzw. absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Abs. 3 BKRG festgelegt werden.

6.2
Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen

– Anlage zur Entschließung –

Mindestens folgende Anforderungen sind an die zukünftige Gestaltung und den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen zu stellen:

– Die kryptografischen Komponenten sind unter Berücksichtigung der Empfehlungen des BSI gemäß dem derzeitigen Stand der Technik zu wählen. Ihre Sicherheitseigenschaften sollen auf unabhängigen kryptografischen Annahmen beruhen. Beide Komponenten müssen sich durch geheim zu haltende Schlüssel parametrisieren lassen.

– Zur Wahrung der Verknüpfbarkeit des derzeitigen Datenbestandes mit zukünftigen Meldungen kann eine Überverschlüsselung der ersten Stufe der derzeitigen Kontrollnummern (dem Ergebnis der Anwendung einer Hashfunktion auf Bestandteile der Identitätsdaten) erfolgen.

– Eine flexible Ausgestaltung des Verfahrens soll vorausschauend berücksichtigen, dass auch in Zukunft mit der Notwendigkeit des Austauschs von kryptografischen Methoden zu rechnen ist.

– Die Sicherheit des verwendeten Schlüsselmaterials wie auch seiner Nutzung ist bei allen Beteiligten durch Maßnahmen der Systemsicherheit, den Einsatz von dem Stand der Technik entsprechenden Kryptomodulen und die Protokollierung von Einsatz und Administration auf einheitlichem Schutzniveau zu gewährleisten.

– Für jedes Register und jedes Abgleichverfahren sind zumindest in der zweiten Stufe der Kontrollnummernbildung spezifische Schlüssel einzusetzen.

– Bei einem Abgleich von Registerdaten ist zu gewährleisten, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind.

6.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13./14. März 2013

Europa muss den Datenschutz stärken

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

– Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.

– Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.

– Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.

– Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.

– Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.

– Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.

– Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.

– Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.

– Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.

– Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

6.4
Erläuterungen zur Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013

„Europa muss den Datenschutz stärken“

– **Jedes personenbeziehbare Datum muss geschützt werden**
Nach Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie z.B. IP-Adressen, Kenn-Nummern, Standortdaten ein.

– **Es darf keine grundrechtsfreien Räume geben**
Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

– **Einwilligungen müssen ausdrücklich erteilt werden**
Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss

für Bürgerrechte sowie der Forderungen des Europäischen Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es – auch mit Blick auf Art. 8 Abs. 2 der Grundrechtecharta – nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

– **Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern**
Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch – in Anlehnung an Art. 8 Abs. 2 der Grundrechtecharta – das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

– **Profilbildung muss beschränkt werden**
Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und es muss festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

– **Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte**
Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

– **Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können**
Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine

einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

– **Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission**
Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Art. 8 Abs. 3 der Grundrechtecharta und Art. 16 Abs. 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

– **Grundrechtsschutz braucht effektive Kontrollen**
Die Sanktionen müssen – wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat – abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

– **Hoher Datenschutzstandard für ganz Europa**
Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die über den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

6.5
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13./14. März 2013

Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

6.6
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13./14. März 2013

Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

6.7
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 2013

Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

Sozial- und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert.

Durch die zunehmende Digitalisierung auch im Sozial- und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von "gläsernen Patientinnen und Patienten oder Versicherten" weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

– Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.

– Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

– Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

6.8
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 2013

Forderungen für die neue Legislaturperiode:
Die Datenschutzgrundrechte stärken!

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit der Kommunikation und der Privatsphäre rückt - wie repräsentative Studien belegen - mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiter zu entwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

– Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz

der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.[1]

– Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.[2]

– Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z.B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.[3]

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

6.9
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 2013

Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlass- und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldege-

[1] Siehe dazu die Entschließungen „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ und „Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags“.

[2] Siehe dazu die heutige Entschließung "Stärkung des Datenschutzes im Sozial- und Gesundheitswesen".

[3] Siehe dazu die heutige Entschließung "Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“.

heimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung "Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen" verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU-Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizeien und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Datenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

6.10
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 2013

Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung „Sicherheit bei E-Government durch Nutzung des Standards OSCI“ Bund, Ländern und Kommunen empfohlen hat. Das so genannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI-Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikations-Endpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

7. Beschlüsse des Düsseldorfer Kreises

7.1
Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z.B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

7.2
Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Inte-

ressen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines “stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z.B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potenzielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall

eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit "Unfallkameras", wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

8. Materialien

8.1

Orientierungshilfe „Soziale Netzwerke“

(Stand: 13. März 2013)

Inhaltsverzeichnis

1 Einführung

1.1 Thematische Ausrichtung

Die vorliegende Orientierungshilfe reflektiert das gemeinsame Verständnis der Datenschutzbeauftragten und Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich über die Wahrung des Datenschutzes bei der Verwendung sozialer Medien, insbesondere sozialer Netzwerke, zur Erfüllung eigener Aufgaben oder Geschäftszwecke. Ziel ist es, neben der Konkretisierung der gesetzlichen Mindeststandards auch Best-Practice-Ansätze aufzuzeigen, soweit der gesetzliche Normierungsrahmen Lücken hinsichtlich eines ausreichenden Schutzes des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufweist. Die Darstellung zielt auf die datenschutzrechtliche Bewertung der verschiedenen „Schichten“ sozialer Netzwerke. Diese Schichten setzen sich aus den Inhaltsdaten, Bestandsdaten und Nutzungsdaten zusammen. Die Bewertung basiert auf den bestehenden gesetzlichen Grundlagen, den einschlägigen Beschlüssen und Entschließungen der nationalen und internationalen Gremien, insbesondere der Artikel-29-Datenschutzgruppe.

Auf eine Trennung zwischen der Darstellung „technischer“ und „rechtlicher“ Anforderungen wird in der Orientierungshilfe bewusst verzichtet. Vielmehr wurden als Leitlinie die Schutzziele der Datensicherheit und des Datenschutzes, Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit, Transparenz und Nichtverkettbarkeit (Zweckbindung) herangezogen. In diesen Schutzzielen lassen sich sämtliche Anforderungen am besten vereinen.

1.2 Zielgruppen

Die Orientierungshilfe richtet sich an Betreiber sozialer Netzwerke. Sie richtet sich auch an Behörden und Unternehmen, die mit sozialen Netzwerken ihre Aufgaben erfüllen (wollen) oder ihre Geschäftszwecke verfolgen. Außerhalb des Fokus liegen die privaten Nutzer sozialer Netzwerke. Die Orientierungshilfe ist insofern keine Anleitung für den datenschutzgerechten Gebrauch solcher Netzwerke. Hinweise und Anleitungen für Nutzer[1] derartiger Dienste werden von verschiedenen Datenschutzbehörden und anderen Einrichtungen zur Verfügung gestellt.

1.3 Schutzziele

Diese Orientierungshilfe verwendet neben den „klassischen" Schutzzielen Vertraulichkeit (Kapitel 0), Verfügbarkeit (Kapitel 0) und Integrität (Kapitel 0) als Maßstab auch die modernen Datenschutzziele Nichtverkettbarkeit (Kapitel 0), Transparenz (Kapitel 0) und Intervenierbarkeit (Kapitel 0)[2].

Diese ergänzenden Ziele sind teilweise bereits in Datenschutzgesetzen oder anderen Normen explizit verankert (so z.B. in § 10 Abs. 2 Nr. 6 DSG NRW), lassen sich aber auch aus den anderen Regelungen ableiten, die die Aufrechterhaltung des technisch-organisatorischen Datenschutzes zum Inhalt haben.

1.4 Begriffsdefinitionen

Die in dieser Orientierungshilfe verwendeten Begriffe von zentraler Bedeutung werden im Folgenden erläutert.

Soziales Netzwerk: Gesamtheit aus technischer und organisatorischer Infrastruktur mit Soft- und Hardware, Betreiber(n) und Nutzern dieser Infrastruktur sowie der darin vorhandenen Daten.

Betreiber oder Anbieter: Eine Organisation, in der Regel juristische Person, die die wesentlichen organisatorischen und technischen Bestandteile eines sozialen Netzwerks bereitstellt und den Dienst damit ermöglicht und darüber den Umfang und die Bedingungen der Nutzung festlegt.

Mitglied: In Bezug auf ein bestimmtes soziales Netzwerk bei diesem registrierte Person[3].

Nutzer: Person, die Dienste eines sozialen Netzwerks nutzt, sei es als registriertes Mitglied oder als nicht-registrierter Externer.

Dritter: Jede andere natürliche oder juristische Person, die nicht Betreiber oder Nutzer in Bezug auf ein bestimmtes soziales Netzwerk ist.

1.5 Allgemeine datenschutzrechtliche Anforderungen

---

[1] Mit der geschlechtsneutralen Form werden Frauen wie Männer gleichermaßen umfasst.
[2] Siehe z. B. Rost/Pfitzmann „Datenschutz-Schutzziele – revisited", in DuD 6/2009.
[3] Dies kann eine natürliche Person, d. h. ein privater Nutzer oder eine juristische Person als professioneller Nutzer sein.

Die Datenschutzbeauftragten des Bundes und der Länder und die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben sich mittlerweile mehrfach in Form von Beschlüssen und Entschließungen zum Datenschutz in sozialen Netzwerken geäußert. Sie haben bei den Betreibern die Beachtung verschiedener Anforderungen angemahnt.

- Information
  Es müssen leicht zugängliche und verständliche Informationen darüber existieren, welche Daten für welche Zwecke erhoben und verarbeitet werden. Nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung (siehe 0).
- Standard-Einstellungen
  Sämtliche Voreinstellungen für die Verwendung personenbezogener Daten des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, entspricht nicht den gesetzlichen Vorgaben (siehe 0). Voreinstellungen sind so zu wählen, dass Risiken für die Privatsphäre der Nutzer minimiert werden und dem Prinzip der Erforderlichkeit Rechnung getragen wird.
- Betroffenenrechte
  Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können (siehe 0).
- Biometrische Daten
  Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig (siehe 0 und 0).
- Pseudonyme Nutzung und Löschverpflichtungen
  Das Telemediengesetz (TMG) schreibt die Eröffnung pseudonymer Nutzungsmöglichkeiten in sozialen Netzwerken vor, soweit dies technisch möglich und zumutbar ist. Nutzer müssen die Möglichkeit haben, in dem sozialen Netzwerk unter Pseudonym oder mehreren Pseudonymen zu handeln. Dies dient der Wahrung des informationellen Grundrechts bei der Nutzung des Internet. Das TMG enthält im Hinblick auf Nutzungsdaten – soweit keine Einwilligung vorliegt – ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen (siehe 0).
- Social Plug-ins
  Das direkte Einbinden von Social Plug-ins in Websites deutscher Anbieter ist unzulässig, wenn dadurch eine Datenübertragung an den jeweiligen Anbieter des Social Plug-ins aus-

gelöst wird, ohne dass die Internetnutzer hinreichend informiert werden und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden (siehe 0).

- Datensicherheit
  Die großen Mengen an teils sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben (siehe 0).
- Minderjährigenschutz
  Daten von Minderjährigen sind besonders zu schützen. Insofern kommt datenschutzfreundlichen Standardeinstellungen eine wichtige Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und für diese leicht verständlich und beherrschbar sein.
- Kontaktpersonen
  Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

2 Technische Grundlagen – Datensicherheit

Aus einem informationstechnischen Blickwinkel bestehen soziale Netzwerke typischerweise aus folgenden Komponenten:

- Client (Internet-Browser oder Smartphone-App),
- Übertragungsnetz (Internet),
- Server-Infrastruktur,
- Datenhaltungs-Infrastruktur (sog. Content Delivery Networks).

Diese Komponenten haben jeweils ihre eigenen Datensicherheitsanforderungen, die unterschiedliche Sicherheitsmaßnahmen erforderlich machen. Die Maßnahmen dienen der Datensicherheit und damit grundsätzlich dem Datenschutz (etwa die Verschlüsselung). Mitunter existieren auch widerstreitende Interessen, z.B. wenn durch Beobachtung des Nutzerverhaltens Angriffe auf das Netzwerk verhindert werden sollen und dabei zusätzliche, das Recht auf informationelle Selbstbestimmung gefährdende Datenverarbeitung stattfindet.

In diesem Kapitel werden verschiedene Aspekte der Technik sozialer Netzwerke beleuchtet und im Hinblick auf ihre Datensicherheitsanforderungen diskutiert. Die getroffene Auswahl ist nicht abschließend, sondern stellt eine Fokussierung auf diejenigen Bereiche dar, die in der Datenschutzdiskussion von besonderer und aktueller Bedeutung sind.

2.1 Datenhaltung

Betreiber (zentralisierter) sozialer Netzwerke verwalten typischerweise große Datenmengen4. Die zum performanten Betrieb solcher Datenmengen genutzten Techniken und Architekturen sind vergleichsweise neu und entwickeln sich noch immer rasch weiter. Die wichtigsten Anforderungen an diese Systeme sind:

- Die Systeme sollten über ausreichende Sicherheitsoptionen wie Zugriffschutz und Authentisierung verfügen, da die entsprechenden Anforderungen nicht von Beginn an in die Entwicklung der Systeme eingegangen sind.
- Die Daten sollten auf logische und räumlich einheitliche Speicherorte verteilt werden, um die Löschung und Beauskunftung von Nutzerdaten nicht zu erschweren.
- Das Löschen von Daten sollte nicht über das Entfernen der Indexeinträge, die zum Auffinden der eigentlichen Daten genutzt werden, erfolgen. Vielmehr sind die Daten tatsächlich zu löschen.

2.2 Biometrische Techniken

Biometrie stellt zunächst keine typische Technik sozialer Netzwerke dar, da biometrische Merkmale wie Fingerabdrücke oder Gesichtsgeometrien nicht erhoben werden.

Allerdings hat die biometrische Erkennung von Gesichtern auf den Fotos der Nutzer mittlerweile Einzug in verschiedene Netzwerke gehalten. Dies ist offenbar auch auf Fotos geringerer Qualität mit einigem Erfolg möglich, zumindest wenn sich die Erkennung nur auf die relativ überschaubare Menge der Freunde eines Nutzers beschränkt. In der Regel handelt es sich dabei um lernende Systeme, die eine anfängliche und fortlaufende „Mitarbeit“ derjenigen Nutzer erfordern, die Personen auf Fotos manuell markieren.

Der Umstand, dass hierbei – aus Sicht des Betreibers eines sozialen Netzwerkes – ohne aufwändige zusätzliche Erhebungen eine massentaugliche biometrische Datenbasis geschaffen wird, birgt datenschutzrechtliche Risiken. Details hierzu werden in Abschnitt 0 erörtert.

2.3 Tracking

Obwohl kein exklusives Thema sozialer Netzwerke, ist das Tracking von Nutzern ein wichtiges Element in der Gesamtfunktionalität vieler Netzwerke. Als Instrument zur Steuerung und Analyse

[4] Die von großen Anbietern wie Facebook oder Google betriebenen Datenbanken gehören zu den größten der Welt. Facebook hatte Mitte 2010 ein Datenvolumen von 15 Petabytes (PB, dies sind 15.000.000 Gigabytes) bei einem Anstieg von 60 TB pro Tag; siehe Thusoo et al.: „Data warehousing and analytics infrastructure at facebook“, in Proceedings of the 2010 international conference on Management of data, http://borthakur.com/ftp/sigmodwarehouse2010.pdf. Aktuell werden mehr als 100 PB angegeben, http://www.facebook.com/notes/facebook-engineering/under-the-hood-hadoop-distributed-filesystem-reliability-with-namenode-and-avata/10150888759153920.

von Werbeeinblendungen trägt das Tracking entscheidend dazu bei, die Einnahmen der unentgeltlich angebotenen Netzwerke zu sichern. Dabei haben soziale Netzwerke gegenüber anderen Angeboten im Internet einen entscheidenden Vorteil: Sie kennen ihre Nutzer5. Es ist ihnen daher immer möglich, die Aktivitäten nutzerspezifisch zu verfolgen. Der Nutzer kann sich dem nicht durch Browsereinstellungen o.Ä. entziehen, ohne seinen Anmeldestatus zu verlieren.

In technischer Hinsicht stehen sozialen Netzwerken die typischen Methoden für das Tracking zur Verfügung: Cookies, Flash-Cookies bzw. LSO (Local Shared Objects) oder HTML5 Client-Side Storage. Meist wird eine Kombination dieser Techniken eingesetzt (mehr zum Nutzertracking und zur Reichweitenanalyse in 0).

2.4 Werbung

Insbesondere für diejenigen sozialen Netzwerke, die ihre Mitgliedschaft kostenlos anbieten, bilden Werbeeinnahmen die bei weitem größte Einnahmequelle. Entsprechend wird auf die Möglichkeiten Wert gelegt, die Werbung möglichst zielgenau und damit erfolgversprechend und gewinnbringend platzieren zu können.

Den sozialen Netzwerken ist es oft möglich, sowohl die Angaben soziographischer Natur ihrer Nutzer (Alter, Geschlecht, Wohnort etc.) als auch deren aktuelle Aktivitäten bei der Werbeeinblendung zu berücksichtigen. Besonders interessant ist dies, wenn sich die Beobachtung der Nutzer über die Grenzen des eigenen Netzwerks hinaus auf das gesamte Web erstreckt. Dies ist mit Hilfe sog. Social Plug-ins möglich, die Webseitenanbieter in ihre Seiten integrieren.

Statt bzw. ergänzend zu der Finanzierung durch Werbung bestehen andere Möglichkeiten der Kostendeckung, etwa Nutzungsentgelte.

2.5 Technische und organisatorische Maßnahmen zur Datensicherheit

Soziale Netzwerke sind verpflichtet, Maßnahmen zur Gewährleistung der Datensicherheit zu ergreifen. Sie verwalten die persönlichen Daten, Beziehungen, Fotos, Meinungen, Interessen und Gewohnheiten von Millionen, nicht selten minderjährigen Menschen.

2.5.1 Verhinderung systematischer Massendownloads von Profildaten aus dem sozialen Netzwerk

[5] Jedenfalls soweit es sich um ihre Mitglieder handelt und die Anmeldung nicht unter Pseudonym erfolgt ist. Nichtmitglieder können Soziale Netzwerke zwar auch aufrufen, sind in ihren Möglichkeiten in der Regel aber sehr beschränkt.

Anbieter sozialer Netzwerke müssen sicherstellen, dass die Nutzer ihrer Angebote die Profildaten und Kommunikationsinhalte anderer Nutzer nicht ohne ausdrückliche Einwilligung der Betroffenen automatisiert von Dritten ausgelesen werden können.

Folgende Maßnahmen gegen den automatisierten und systematischen Abruf (z.B. durch crawler) von Profildaten und Kommunikationsinhalten sollten getroffen werden:

- Der Zugriff von Suchmaschinen oder anderen Indexierern auf die Profile der Nutzer sollte von diesen im Rahmen der Datenschutzeinstellungen festgelegt werden können und in den Standardeinstellungen deaktiviert sein.
- Betreiber von sozialen Netzwerken sollten Maßnahmen ergreifen, die eine Massenkopie von Daten aus dem Netzwerk verhindern. Zu solchen Maßnahmen zählen z.B. die Beobachtung von auffälligen Aktivitäten im Netzwerk (Unterscheidung zwischen manuellen und maschinellen Zugriffen) oder die externe Auditierung der eigenen Infrastruktur.

2.5.2 Angriffe auf den sozialen Graphen

Vereinfacht lassen sich soziale Netzwerke als Graphen betrachten, die Knoten (Nutzerprofile) und Kanten (Freundschaftsbeziehungen) verbinden. Ziel vieler Betreiber von Netzwerken ist es, diesen Graphen möglichst groß und engmaschig zu machen. Insbesondere soll er nicht in voneinander unabhängige Bereiche zerfallen. Diese aus Netzwerksicht wünschenswerte Eigenschaft macht soziale Netzwerke (und auch andere zusammenhängende Netzwerke) anfällig für sich von Knoten zu Knoten fortpflanzende Missbräuche.

Eine einmal gefundene Schwachstelle (z.B. zum Auslesen oder Verändern von Daten) kann ausgehend von einem Nutzer (z.B. dem Account eines Angreifers) rasch in dem gesamten Netzwerk ausgenutzt werden und damit die Infrastruktur in ihrer Gesamtheit gefährden. Einige aktuellere Beispiele hierfür sind Koobface[6], Ramnit[7] oder LilyJade[8]; das Problem reicht bis in die Anfangszeiten sozialer Netzwerke zurück (z.B. 2005 der Spacehero-Wurm auf MySpace[9]).

Betreiber sozialer Netzwerke müssen sämtliche nach dem Stand der Technik als erforderlich anzusehenden Maßnahmen ergreifen, damit solche Angriffe unterbunden werden oder zumindest so rechtzeitig erkannt werden, dass Gegenmaßnahmen getroffen werden können. Hierzu sollten u. a. folgende Vorkehrungen getroffen werden:

---

[6] http://en.wikipedia.org/wiki/Koobface
[7] http://www.spiegel.de/netzwelt/web/zehntausende-opfer-mehrzweck-wurm-kapert-facebook-konten-a-807521.html
[8] http://www.securelist.com/en/blog/706/Worm_2_0_or_LilyJade_in_action
[9] http://namb.la/popular/

- Einführung von CAPTCHAs[10], um Programme (sog. Social Bots) zu behindern,
- Plausibilitätsprüfungen von Nutzeraccounts, um insbesondere automatisiert betriebene Accounts zu erkennen,
- Beobachtung der Aktivitäten im Netzwerk auf Auffälligkeiten (z.B. besonders hohe Zugriffszahlen) und entsprechende Gegenmaßnahmen (z.B. zeitliche oder zahlenmäßige Begrenzung abfragbarer oder herunterladbarer Profile),
- Meldungen anderer Nutzer.

Diese Vorkehrungen[11] können systematische Massendownloads von Profildaten erschweren, sind jedoch nicht lückenlos[12] und erfordern ein permanentes Nachsteuern. Datensicherheit ist als Prozess zu begreifen, der zyklisch immer wieder durchlaufen werden muss. Die Betreiber sozialer Netzwerke müssen die Nutzer über bestehende Restrisiken informieren.

3 Verantwortlichkeit

Nach Art. 2 d) der RL 95/46/EG (EG-Datenschutzrichtlinie[13]) ist für die Verarbeitung Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hiervon zu unterscheiden ist der Auftragsdatenverarbeiter im Sinne von Art. 2 e) der RL 95/46/EG als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Bei der Beurteilung wird auf die konkrete Funktion bei der Durchführung der Datenverarbeitung abgestellt. Die jeweilige Stelle kann für gewisse Datenverarbeitungen als verantwortliche Stelle, für andere Verarbeitungen auch als Auftragsdatenverarbeiter tätig werden. Je nach eingenommener Rolle können sich somit unterschiedliche Funktionen für Anbieter und Betreiber, aber auch die Nutzer eines sozialen Netzwerks ergeben.

3.1 Verantwortungsverteilung bei sozialen Netzwerken

3.1.1 Betreiber von sozialen Netzwerken

Betreiber von sozialen Netzwerken, die Online-Kommunikationsplattformen zur Nutzung bereitstellen, sind regelmäßig als verantwortliche Stelle nach Art. 2 d) der RL 95/46/EG bzw. § 3 Abs. 7

---

[10] Completely Automated Public Turing test to tell Computers and Humans Apart, siehe http://de.wikipedia.org/wiki/CAPTCHA.

[11] Z.B. Facebook Immune System, http://allfacebook.de/wp-content/uploads/2011/10/FacebookImmuneSystem.pdf, oder Everything you ever wanted to know about Facebook Security, http://www.scribd.com/doc/70451272/Facebook-Security-Infographic.

[12] Z.B. The Socialbot Network: When Bots Socialize for Fame and Money, http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1.

[13] 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 S. 31).

BDSG anzusehen.[14] Sie bestimmen über die Zwecke und Mittel der Datenverarbeitung. Die Fähigkeit, die Verarbeitungszwecke zu bestimmen, ist bereits feststellbar, wenn mit den im Rahmen der Nutzung der Dienste erhobenen Daten zum Beispiel Werbe- oder Marketingzwecke verfolgt werden. Hierbei werden Nutzungsdaten (z.B. IP-Adresse, Browsertyp, Cookies) und Inhaltsdaten (eingestellte Fotos, eingestellte Beiträge) verarbeitet. Eine entsprechende Zwecksetzung ergibt sich nicht selten aus den Allgemeinen Geschäftsbedingungen des Betreibers des sozialen Netzwerks. Die Entscheidung über die Mittel der Datenverarbeitung, d. h. die zum Einsatz kommende Soft- und Hardware, wie auch die Entscheidung über die Verarbeitung selbst, z.B. über die Speicherdauer, liegt im Regelfall ebenfalls bei den Betreibern von sozialen Netzwerken. Die Bezeichnung als „verantwortliche Stelle“ oder als „Auftragsdatenverarbeiter“ (auch in schriftlichen Vereinbarungen oder Verträgen) ist nicht maßgebend für die Bewertung. Es kommt auf die tatsächliche Aufgabenverteilung an, also welcher Stelle die jeweilige Funktion bzw. Rolle bei der Datenverarbeitung zukommt.

3.1.2 Professionelle Nutzer

Denkbar ist, dass mehrere verantwortliche Stellen gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Dies führt dazu, dass alle Stellen die Adressaten für die Einhaltung der Datenschutzvorschriften und insbesondere für die Erfüllung der Betroffenenrechte (Auskunft, Löschung, Sperrung, Berichtigung etc.) sind. Die Artikel-29-Datenschutzgruppe hat festgestellt, dass bezüglich der Akteure in einem sozialen Netzwerk sowohl die Konstellation denkbar ist, dass zwei oder mehrere Verantwortliche gemeinsam die vollständige Kontrolle über die Zwecke und Mittel ausüben, als auch der Fall, dass zwei oder mehrere Verantwortliche nur bezüglich eines Teils der Datenverarbeitung gemeinsam eine solche Kontrollfunktion besitzen.[15] Die Verfolgung gleicher Ziele und der Einsatz gleicher Mittel können auf verschiedene gemeinsam für die Datenverarbeitung Verantwortliche verteilt sein. Bei komplexen Verarbeitungsformen macht dies eine klare Zuweisung von Verantwortlichkeiten notwendig.[16] Unklarheiten dürfen sich nicht zu Lasten der Nutzer des sozialen Netzwerks auswirken. Diese müssen ihre Rechte auf Benachrichtigung, Löschung, Sperrung, Berichtigung und Widerspruch richtig adressieren können.

Webseitenbetreiber sind für die Datenverarbeitung Verantwortliche, wenn sie mittels Einbindung von Inhalten und von Diensten sozialer Netzwerkebetreiber (z.B. Social Plug-ins) zur Ausgestal-

[14] Art. 29-Datenschutzgruppe, WP 163 vom 12.07.2009, S. 6.
[15] Art. 29-Datenschutzgruppe, WP 169 vom 16.02.2010, S. 26.
[16] Vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Wer ist datenschutzrechtlich verantwortlich für Facebook-Fanpages und Social-Plugins?, www.datenschutzzentrum.de/facebook/facebook-verantwortlichkeit.html.

tung ihres eigenen Dienstes die Datenverarbeitung der Anbieter des sozialen Netzwerks technisch ermöglichen.17

Die Verantwortlichkeit der Verwender der Dienste sozialer Netzwerke wird vor allem dann begründet, wenn diese zur Ausgestaltung ihres eigenen Angebotes die Dienste der Netzwerkanbieter nutzen und dabei eigene Geschäftszwecke verfolgen, z.B. durch die Inanspruchnahme von vom Betreiber zur Verfügung gestellten Statistiken. Derartige Nutzungsstatistiken werden auf der Grundlage von personenbezogenen Nutzerdaten der Nutzer erstellt.

3.2 Nutzer als verantwortliche Stelle

Nutzer von sozialen Netzwerken sind im Regelfall als Betroffene im Sinne von Art. 2 a) der RL 95/46/EG, § 3 Abs. 1 BDSG und nicht als für die Datenverarbeitung Verantwortliche. Allerdings ist nicht ausgeschlossen, dass sie selbst über die Zwecke und Mittel der Datenverarbeitung entscheiden bzw. mitentscheiden. Im Zusammenhang mit dem Freunde-Finder-Verfahren sozialer Netzwerke wurde etwa angenommen, dass die Nutzer und der Betreiber des sozialen Netzwerks bewusst und gewollt zusammenwirken, indem die Nutzer die erforderlichen Adressdaten bereitstellen und der Netzwerkbetreiber die Erstellung von Einladungs-E-Mails und deren Versand übernimmt.18

Nutzer sind datenschutzrechtlich für die Verarbeitung personenbezogener Daten anderer Personen verantwortlich, wenn sie diese in ihren Nutzerprofilen oder auf den Plattformen in sozialen Netzwerken veröffentlichen. Nur wenn der Nutzer in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten tätig wird, kommen die Datenschutzvorschriften nicht zur Anwendung (vgl. Art. 3 Abs. 2 der EG-Datenschutzrichtlinie, § 1 Abs. 2 Nr. 3 BDSG).19 Die Annahme einer ausschließlich persönlichen oder familiären Datenverarbeitung ist bei der Verwendung fremder personenbezogener Daten jedoch zumeist nicht gegeben; dies gilt insbesondere, wenn die personenbezogenen Informationen für jedermann sichtbar sind. Selbst wenn die Sichtbarkeit auf bestimmte Kreise bzw. Listen beschränkt ist, wird der persönliche und familiäre Bereich verlassen, wenn sich Netzwerkbetreiber eigene Nutzungs- und Verarbeitungsrechte an den eingestellten Informationen einräumen. Ausgeschlossen ist eine familiäre und persönliche Nutzung sozialer Netzwerke außerdem, wenn der Nutzer das Profil ganz oder teilweise zu beruflichen oder geschäftlichen Zwecken verwendet.

Von einer rein familiären und persönlichen Nutzung eines sozialen Netzwerkes kann ausgegangen werden, wenn die Zugriffsmöglichkeiten auf Informationen anderer Betroffener in dem Profil des

---

[17] Ernst, Social Plugins: Der „Like-Button“ als datenschutzrechtliches Problem, NJOZ 2010, 1917, 1918.
[18] LG Berlin, Urteil vom 06.03.2012, 16 O 551/10 (nicht rechtskräftig).
[19] Vgl. Art. 3 Abs. 2 der EG-Datenschutzrichtlinie, § 1 Abs. 2 Nr. 3 BDSG, sowie Art. 29-Datenschutzgruppe, WP 163 vom 12.07.2009, S. 6.

jeweiligen Nutzers auf die von ihm selbst ausgewählte Kontakte beschränkt ist und eine Nutzung dieser Daten durch den Netzwerkbetreiber ausgeschlossen wird, d. h. die verwendeten Informationen ausschließlich zur privaten Kommunikation und Interaktion verwendet werden.

4 Rechtliche Grundlagen – Zulässigkeit

Die europäische und deutsche Rechtsordnung verpflichten Betreiber sozialer Netzwerke, beim Erheben, Verarbeiten und Nutzen personenbezogener Daten die datenschutzrechtlichen Vorgaben einzuhalten, Art. 7 RL 95/46/EG und § 4 Abs. 1 BDSG.

4.1 Anwendbares Recht

Für die Bestimmung, welche Rechtsordnung Anwendung findet, ist der Sitz des Dienstanbieters maßgeblich. Das für soziale Netzwerke einschlägige Telemedienrecht verweist zur Bestimmung des anzuwendenden Rechts auf die allgemeinen Regeln des BDSG, § 3 Abs. 3 Nr. 4 TMG. Anwendbar sind somit die Regelung des § 1 Abs. 5 BDSG bzw. zu dessen europarechtskonformen Auslegung Art. 4 RL 95/46/EG.
Danach ist die Anwendung deutschen Datenschutzrechts ausgeschlossen, wenn der Betreiber des Netzwerkes seinen Sitz in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat. In diesen Fällen kommt das jeweilige nationalstaatliche Recht des Sitzlandes zur Anwendung.

Deutsches Datenschutzrecht findet bei Betreibern sozialer Netzwerke Anwendung, die ihren Sitz **nicht** in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum innehaben und im Inland Daten erheben, verarbeiten oder nutzen. Dies ist der Fall, wenn der Betreiber zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind. Die Artikel-29-Datenschutzgruppe legt den Begriff „Mittel“ weit aus. Unter diesen Begriff fallen demnach auch Anlagen von Auftragsdatenverarbeitern20, die im Auftrag der Betreiber Daten im Inland erheben oder verarbeiten. Ein Bezug zum Inland wird auch dann hergestellt, wenn Cookies oder Javascript auf den Endgeräten der Nutzer zur Durchführung der Datenverarbeitung durch den Betreiber gespeichert oder ausgeführt werden.21

Dieser stark technisch orientierte Ansatz wird durch einen normativen Ansatz ergänzt. Zweck der Regelung des Art. 4 RL 95/46/EG ist es, das datenschutzrechtliche Schutzniveau nicht dadurch zu

---

[20] A. A. VG Schleswig, Beschl. v. 14.02.2013; https://www.datenschutzzentrum.de/presse/20130215-verwaltungsgericht-facebook.htm.
[21] Art.-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht v. 16. Dezember 2010, WP 179 0836-02/10/DE, S. 25f.

gefährden, dass außereuropäische Anbieter in den Markt drängen, ohne sich den auf diesem Markt geltenden Regeln unterwerfen zu müssen. Zugleich sollen zu heterogene Regelungsanforderungen an die Betreiber vermieden werden.

Die stark auf die objektiven Merkmale abstellende Bestimmung der Erhebung, Verarbeitung und Nutzung von Daten im Inland wird durch die Zweckbestimmung des Betreibers ergänzt. Unter das Datenschutzrecht des jeweiligen Ziellandes fallen Betreiber nur, wenn auch der Wille zur Datenverarbeitung von personenbezogenen Daten im jeweiligen Land zum Ausdruck kommt. Die durch das Internet hervorgerufene Vernetzung erlaubt aus technischer Sicht, jeden Dienst von jedem Ort der Welt aus abzurufen. Daher soll nationales Datenschutzrecht für Angebote gelten, die sich explizit oder implizit an die Betroffenen in dem jeweiligen Land richten. Indizien für eine derartige Ausrichtung des Angebotes könnten die Spracheinstellungen, Domainendungen oder die direkte inhaltliche Ansprache sein.

Deutsches Datenschutzrecht findet daher auf Betreiber mit Sitz im außereuropäischen Ausland Anwendung, die im Inland Daten erheben, verarbeiten und nutzen und deren Angebot sich an in Deutschland lebende Personen richtet.

Wenn der nichteuropäische Betreiber eine Niederlassung in einem Mitgliedstaat der Europäischen Union betreibt, findet das jeweilige Landesrecht des europäischen Sitzstaates Anwendung. Voraussetzung ist jedoch, dass es sich bei der Niederlassung um eine datenschutzrechtlich relevante Niederlassung handelt. Die Niederlassung muss für das jeweils in Frage stehende Verfahren die datenschutzrechtliche Verantwortung, d. h. die tatsächliche Entscheidungsbefugnis über Art und Umfang der Datenverarbeitung innehaben.

Öffentliche Stellen des Bundes und der Länder als Betreiber sozialer Netzwerke unterliegen den nationalen datenschutzrechtlichen Anforderungen aus dem BDSG bzw. den jeweiligen Landesdatenschutzgesetzen bzw. dem Bundesdatenschutzgesetz und dem Telemedienrecht. Die Anwendung des datenschutzrechtlichen Teils des Telemediengesetzes gilt gemäß § 11 Abs. 1 TMG nicht für soziale Netzwerke, soweit die Bereitstellung solcher Dienste im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von oder zwischen nicht-öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von internen Arbeits- oder Geschäftsprozessen erfolgt.

4.2 Gesetzliche Grundlagen im Bundesdatenschutz- und Telemediengesetz

Das deutsche Datenschutzrecht legt für Betreiber sozialer Netzwerke Anforderungen fest. Maßgeblich ist der Zweck der Erhebung und der Verarbeitung und die technische Natur des Datums.

Somit kann ein „technisches Datum“ unterschiedlichen rechtlichen Regelungsregimen unterfallen. Der Name eines Betroffenen kann insoweit ein Bestands-, Nutzungs-, Abrechnungs- und Inhaltsdatum sein; dessen Verarbeitung kann im TMG oder im BDSG bzw. LDSG geregelt sein.

4.2.1 Inhaltsdaten

Zu den Inhaltsdaten zählen Informationen der Betroffenen, die Gegenstand der Leistungserbringung durch den Betreiber des sozialen Netzwerkes sind und den „Inhalt“ des Dienstes ausmachen. Dazu gehören die Profilinformationen eines persönlichen Profils und die Inhalte der Kommunikation. Derartige Informationen unterfallen entweder bereichsspezifischen Gesetzen oder den allgemeinen Regeln des BDSG oder LDSG.

4.2.2 Bestandsdaten

Bestandsdaten unterliegen den Regeln des § 14 Abs. 1 TMG. Bestandsdaten sind Angaben, die für die Begründung, Durchführung und Beendigung eines Nutzungsverhältnisses notwendig sind. Welche konkreten Daten das sind, wird durch den jeweiligen Nutzungsvertrag bestimmt. Dazu zählen identifizierende Nutzerangaben (Name, Anschrift, E-Mail), Zugangsdaten (Nutzername, ID, Kennwort) oder weitere vertragsrelevante Informationen (Tarife, Nutzungszeiten etc.).

4.2.3 Nutzungsdaten

In den Anwendungsbereich des TMG fallen auch sämtliche Daten, die erforderlich sind, um die Inanspruchnahme des sozialen Netzwerkes zu ermöglichen und abzurechnen. Die Erhebung, Verarbeitung und Nutzung derartiger Nutzungsdaten ist in § 15 TMG umfassend geregelt. Zu den Nutzungsdaten zählen Merkmale zur Identifikation des Nutzers (IP-Adresse, Cookies, Nutzerkennung), Angaben über Beginn und Ende der Nutzung und Angaben über die in Anspruch genommenen Dienste. Soweit die Nutzungsdaten für die Abrechnung kostenpflichtiger Angebote des sozialen Netzwerkbetreibers verwendet werden, handelt es sich um Abrechnungsdaten, deren Verwendung durch § 15 Abs. 4 TMG geregelt wird.

4.3 Rechtsnatur der Mitgliedschaft in einem sozialen Netzwerk

Soziale Netzwerke sind ein relativ neues Phänomen der Entwicklung des Internets, deren rechtliche Einordnung, die entscheidend für die datenschutzrechtliche Bewertung ist, nicht einfach ist. Eine einheitliche, allgemein anerkannte Auffassung zu ihrer Rechtsnatur hat sich daher bislang noch nicht herausgebildet.

4.3.1 Vertragliche Ausgestaltung

Der Vorteil einer vertraglichen Ausgestaltung ist es für Betreiber sozialer Netzwerke, dass in Deutschland der Abschluss von Nutzungsverträgen grundsätzlich formfrei möglich ist. Es gilt der

Grundsatz der Privatautonomie: Jeder kann mit jedem einen Vertrag über einen individuell gewünschten Inhalt abschließen. Dabei darf nicht außer Acht gelassen werden, dass über verbraucherschützende Vorschriften wie die §§ 305 ff. BGB zivilrechtlich eine Inhaltskontrolle möglich ist.

Datenschutzrechtlich gilt, dass Datenerhebungen und –verwendungen, die für den Vertragszweck erforderlich sind, grundsätzlich auf gesetzlicher Grundlage nach § 28 Abs. 1 S. 1 Nr. 1 BDSG bzw. § 14 Abs. 1 TMG zulässig sind. Ähnlich wie bei der Mitgliedschaft in einem Verein sind jedoch Regelungen, die mit dem Hauptzweck der Mitgliedschaft nichts zu tun haben, aber von hoher datenschutzrechtlicher Relevanz sind, kritisch zu hinterfragen: Ebenso wenig wie ein Sportverein über eine Satzungsregelung, nach der die Mitgliederdaten an Sportartikelhersteller verkauft werden dürfen, diese Datenübermittlung legitimieren kann, kann sich ein Betreiber eines sozialen Netzwerks über seine Nutzungsrichtlinien ausbedingen, die Mitgliederdaten zu einem Zweck zu verwenden, der mit der vereinbarten Nutzung des sozialen Netzwerks unmittelbar nichts zu tun hat. Dies gilt z.B. für die oben erwähnte Werbung, es sei denn, der Vertrag ist so deutlich ausgestaltet, dass der Nutzer sich darüber im Klaren ist, dass er auch einen Vertrag über die werbliche Nutzung seiner Daten schließt.

Wenn der Betreiber des sozialen Netzwerks die Nutzungsbedingungen ändert, braucht er jedenfalls bei wesentlichen Änderungen die Zustimmung des Nutzers; ansonsten gelten für diesen die alten Bedingungen fort. Ein kollektives Einverständnis der Nutzer in Form eines fehlenden Widerspruchs durch ein betreiberseitig definiertes Quorum genügt nicht. Anders als beim Verein, bei dem von Gesetzes wegen Satzungsänderungen nur unter der Beteiligung der Mitglieder möglich sind (vgl. § 33 BGB), werden die Nutzungsbedingungen bei sozialen Netzwerken einseitig durch den jeweiligen Betreiber gesetzt. Hieran ändern auch betreiberseitig initiierte Abstimmungen über geplante Änderungen nichts. Es handelt sich letztlich um eine Änderung des Nutzungsvertrags, mit der das einzelne Mitglied einverstanden sein muss.

Allerdings ist es im vertraglichen Bereich denkbar, dass das Mitglied seine Zustimmung durch konkludentes Handeln äußert. Dies kann sogar in einem Unterlassen bestehen, wie sich im Umkehrschluss aus § 308 Nr. 5 BGB ergibt. Voraussetzung ist, dass dies entsprechend vorher vertraglich vereinbart wird und dem Mitglied eine angemessene Frist zur Abgabe einer ausdrücklichen Erklärung eingeräumt wird sowie bei Fristbeginn ein Hinweis auf die vorgesehene Bedeutung seines Verhaltens erfolgt.

Liegt ein wirksamer Vertrag vor, muss der Betreiber eines sozialen Netzwerks im Rahmen seiner Informationspflichten nach § 13 Abs. 1 TMG und § 4 Abs. 3 S. 1 BDSG den Nutzer über die konkreten Datenflüsse unterrichten (sofern sich diese nicht bereits direkt aus der vertraglichen Rege-

lung ergeben). Im Fall von pseudonymer Nutzerdatenanalyse ist der Nutzer ebenfalls darüber zu unterrichten und auf sein Widerspruchsrecht hinzuweisen, § 15 Abs. 3 TMG.

4.3.2 Einholen einer datenschutzrechtlichen Einwilligung

Das Rechtsinstitut der Einwilligung kommt in denjenigen Konstellationen zum Tragen, in denen die beabsichtigte Datenerhebung und -verwendung nicht mehr von dem (vertraglich vereinbarten) Zweck des Nutzungsverhältnisses gedeckt ist. Dies ist insbesondere dann der Fall, wenn der Zweck in keinem Zusammenhang mit der Nutzung des sozialen Netzwerkes steht. Auch der Umgang mit personenbezogenen Daten zum Zweck der individualisierten Werbung bedarf der Einwilligung. Denn für die unmittelbare Inanspruchnahme des Dienstes ist die Datenverarbeitung zum Zweck der Werbung nicht erforderlich.

In diesen Fällen muss der Nutzer informiert einwilligen, d.h. er muss über Zweck und Umfang der Datenverarbeitung aufgeklärt werden und sein Einverständnis aktiv – beispielsweise durch das Setzen eines Häkchens – bekunden. Wichtig ist – parallel zu den Ausführungen zur vertraglichen Ausgestaltung – dass beim Nutzer ein entsprechender Rechtsbindungswillen vorhanden ist und auch nachgewiesen werden kann. Im Einzelnen sieht das Gesetz in § 13 Abs. 2 und 3 TMG vor, dass der Dienstanbieter bei einer elektronischen Einwilligung sicherstellen muss, dass

- der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann,
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann und
- er auf dieses Widerrufsrecht hingewiesen wird.

Die Einwilligung ist das Mittel der Wahl für Datenerhebungen und -verwendungen, die über den im Rahmen der Mitgliedschaft vereinbarten Vertragszweck hinausgehen.

Aufgrund der Gestaltungsmacht des Netzwerkbetreibers ist dieser in der Lage, den Umfang der geschuldeten vertraglichen Leistung zu bestimmen. Eine einseitige nachträgliche Erweiterung der Pflichten des Nutzers durch das Abverlangen einer Einwilligung unter der Bedingung, nur bei der Erteilung der Einwilligung das Nutzungsverhältnis fortzusetzen, stellt die Freiwilligkeit der Erteilung der Einwilligung in Frage. Soziale Netzwerke sind auf die Pflege der Kommunikationsbeziehungen, die Teil der menschlichen Identität sind, ausgerichtet. Wird die Fortnutzung des Dienstes von der Erteilung der Einwilligung abhängig gemacht, hat der Nutzer nur die Wahl, seine Kommunikationsbeziehung abzubrechen oder den Eingriff in seine Persönlichkeitsrechte zu legitimieren. Auch die Nutzung von personenbezogenen Daten Betroffener, die nicht Nutzer des jeweiligen Netzwerkes sind bzw. nicht mit den Betreibern direkt in Kontakt stehen, ist in der Regel nur auf der Grundlage einer entsprechenden Einwilligung der Betroffenen möglich. Nicht auszuschließen sind Fälle, in

denen Betreiber ein berechtigtes Interesse darlegen können, personenbezogene Daten zu verarbeiten und auch Personen, die nicht Nutzer des Netzwerkes sind, diesen Eingriff dulden müssen, z.B. Maßnahmen der Datensicherheit gegen Angriffe von außen. Eine derartige Befugnis ist jedoch im jeweiligen Einzelfall plausibel zu begründen und muss die Ausnahme bleiben. Den schutzwürdigen Interessen dieser Betroffenen, die womöglich eine bewusste Entscheidung getroffen haben, einen bestimmten Dienst nicht zu nutzen, sollte Rechnung getragen werden.

4.4 Zweckbindung und Nichtverkettbarkeit

Einige Datenschutzgesetze haben inzwischen die Nichtverkettbarkeit als Schutzziel bzw. als allgemeine Maßnahme zur Datensicherheit aufgenommen. Ziel der Nichtverkettbarkeit ist, dass personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. So fordern §§ 12 Abs.2 TMG, 28 Abs. 1 S. 2 BDSG, Art. 6 Abs. 1 lit. b) RL 95/46/EG, dass bei der Datenverarbeitung gewährleistet sein muss, dass personenbezogene Daten nur dann zu einem anderen Zweck verarbeitet und genutzt werden dürfen, soweit dafür eine gesetzliche Rechtfertigung existiert oder die Betroffenen in die Zweckänderung eingewilligt haben.

Im Rahmen von sozialen Netzwerken geht es somit zum einen um die Frage, welche Inhalts-, Nutzungs- und Bestandsdaten in das Profil eines Nutzers einfließen, aber auch, inwieweit unterschiedliche Profile innerhalb des Netzwerkes, aber auch mit Profilen oder weiteren Inhalts-, Nutzungs- und Bestandsdaten des Nutzers außerhalb des Netzwerkes durch den Anbieter oder Dritte verbunden werden können. Im Sinne der informationellen Selbstbestimmung muss das Netzwerk dem Nutzer die Möglichkeit bieten, zu entscheiden, wer was wann über ihn weiß und dies auch jederzeit feststellen zu können. Die folgenden Grundsätze sollten zur Förderung der Kontrolle beachtet werden[22]:

- Den Nutzern sollten Möglichkeiten zur Verfügung stehen, mit denen sie Verkettungen bzw. Zweckänderungen ihrer Daten und deren Ausmaß erkennen können.
- Die Nutzer sollten in der Lage sein, die Verkettung ihrer Daten über ein geeignetes Identitätsmanagement zu kontrollieren. Dazu gehört auch die Möglichkeit, in dem sozialen Netzwerk unter verschiedenen Pseudonymen (z.B. zur Trennung beruflicher und privater Nutzung) zu agieren (vgl. dazu unten 4.5).
- Verkettungen müssen rückgängig gemacht werden können, indem z.B. Verknüpfungen von Profilen mit einer App oder einem Profil in einem anderen Netzwerk gelöscht werden können.

[22] Vgl. Studie „Verkettung digitaler Identitäten“ ULD / TU Dresden, https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

- Die Vertrauenswürdigkeit in die Verarbeitung sollte durch geeignete Nachweise gefördert werden (IT-Grundschutz, Audits, Zertifizierung).

4.5 Anonyme und pseudonyme Nutzung

Das TMG fordert in § 13 Abs. 6 von Betreibern sozialer Netzwerke, die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzende ist über diese Möglichkeit zu informieren. Den Nutzenden muss jedenfalls ermöglicht werden, in dem Sozialen Netzwerk unter Pseudonym zu agieren. Eine Offenlegung der tatsächlichen Identität des Nutzers gegenüber dem Betreiber des Sozialen Netzwerks kann dagegen zur Erschwerung von Missbrauch insbesondere dann hingenommen werden, wenn die Nutzer das Netzwerk nicht nur passiv (Herunterladen von Informationen), sondern auch aktiv (Einstellen von Informationen) nutzen können. Betreiber sozialer Netzwerke für Privatnutzung sollten die Nutzung von Pseudonymen aktiv fördern.

Bei Netzwerken, die im beruflichen Kontext genutzt werden, ist es in der dortigen Zielgruppe zwar eher unüblich, anonym bzw. unter Pseudonym aufzutreten. Trotzdem gilt die Verpflichtung aus § 13 Abs. 6 TMG zur Eröffnung einer optionalen Möglichkeit, in dem Netzwerk unter Pseudonym zu handeln, auch für solche Netzwerke. Bei entsprechenden Vorgaben zur Gestaltung der Pseudonyme muss die Qualität des Netzwerkes nicht leiden, so dass eine Unzumutbarkeit für den Anbieter nicht anzunehmen ist.

4.6 Zweckbindung

Zentrale Intention der Nichtverkettbarkeit ist die Sicherung der Zweckbindung. Das bedeutet, dass personenbezogene Daten nur für den Zweck verarbeitet werden dürfen, den die gesetzliche Vorgabe erlaubt bzw. der im Rahmen der Einwilligung durch den Betreiber des sozialen Netzwerkes vorgegeben worden ist. Nach § 13 Abs. 1 TMG hat der Dienstanbieter den Nutzer vor der Erhebung über den Zweck zu informieren. Soll der Zweck geändert werden, so ist dies nur möglich, wenn entweder hierfür eine gesetzliche Grundlage besteht oder die Einwilligung beim Betroffenen eingeholt wird (vgl. auch § 12 Abs. 2 TMG). Der Zweck muss im Rahmen der Einwilligung so umrissen werden, dass es dem Betroffenen möglich ist einzuschätzen, welche Verkettungsmöglichkeiten sich hieraus ergeben. Pauschale Zweckbestimmungen wie „zur Erbringung des Dienstes“ sind nicht ausreichend.

4.7 Trennungsprinzip

Um die Nichtverkettbarkeit auch technisch zu unterstützen, gilt im Datenschutzrecht das Trennungsprinzip. Nach § 13 Abs. 4 Nr. 4 TMG hat der Dienstanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass die personenbezogenen Daten über die Nutzung

verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können. Außerdem muss sichergestellt sein, dass Nutzungsprofile i. S. d. § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können (§ 13 Abs. 4 Nr. 5 TMG). Für soziale Netzwerke bedeutet das, dass Nutzungsprofile, die zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des sozialen Netzwerks erstellt werden, getrennt von den Nutzerprofilen verarbeitet werden müssen, die aus den Inhaltsdaten eines Nutzers bestehen. Für Nutzungsprofile sind Pseudonyme zu verwenden. Fallen noch bei weiteren Telemedien (z.B. Chat-Dienste, Spiele etc.) personenbezogene Daten an, so sind auch diese Daten und Profilinformationen von den übrigen Daten so weit wie möglich zu trennen.

5 Transparenz und Kontrolle

5.1 Transparenz

Nach § 13 Abs. 1 TMG hat der Dienstanbieter die Nutzer vor der Datenverarbeitung über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der RL 95/46/EG in allgemein verständlicher Form zu unterrichten. Nach § 4 Abs. 3 BDSG sind den Betroffenen von der verantwortlichen Stelle deren Identität, der Zweck der Datenverarbeitung und die Kategorien von Empfängern mitzuteilen. Letzteres gilt jedoch nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

Diese Anforderungen gelten sowohl für die Erhebung von Nutzungs- und Bestandsdaten nach dem TMG als auch für Inhaltsdaten nach dem BDSG. Die Einwilligung nach § 13 TMG bzw. § 4a BDSG ist nur wirksam, solange sie in Kenntnis des vorgesehenen Zwecks der Erhebung, Verarbeitung oder Nutzung erteilt wurde.

Neben der Information über Art, Umfang und Zwecke der Erhebung und Verwendung sind Nutzer über ihre Rechte zu informieren, z.B. über das Recht, der Einwilligung zur Verarbeitung zu widersprechen (§ 13 Abs. 3 TMG) und über die Möglichkeit, das Angebot anonym oder pseudonym zu nutzen (§ 13 Abs. 6 TMG). Zusätzlich muss der Betreiber des sozialen Netzwerks kommerzielle Inhalte sowie die dahinterstehende natürliche oder juristische Person klar als solche kennzeichnen (§ 6 TMG).

Informationen und Nutzungsbedingungen, die Rechte und Pflichten der Nutzer und des Betreibers des sozialen Netzwerks regeln, müssen in einer verständlichen und übersichtlichen, deutschsprachigen, barrierefreien Erklärung, die im gesamten Angebot leicht zugänglich ist, bereitgestellt werden (Datenschutzerklärung und Nutzungsbestimmungen). Die Informationen müssen umfassend sein, also z.B. auch Informationen zu personenbezogenen Daten enthalten, die mit Hilfe von Cookies erhoben werden. Die Verwendung der Daten ist strukturiert und klar anzugeben, insbesondere

die Weitergabe und der Zugriff durch berechtigte Dritte ist eindeutig festzulegen. Die Informationen sind stets zu aktualisieren, insbesondere bei neuen und geänderten Funktionen, und allen Nutzern vor der Einführung zur bestätigenden Kenntnis zu geben.

Nutzer sollten über mögliche Konsequenzen ihres Handelns auch während der Nutzung des Dienstes (z.B. bei der Veränderung von Datenschutz-Einstellungen einer Bildersammlung) informiert werden, z.B. durch eingebaute, kontext-sensitive Funktionen, die angemessene Informationen auf der Basis der jeweiligen Handlungen der Nutzer liefern.

Die Information der Nutzer sollte sich auch auf den Umgang mit Daten von Personen, die nicht Nutzer des Netzwerkes sind, beziehen: Betreiber sozialer Netzwerke sollten auch über Ge- und Verbote im Hinblick darauf informieren, wie die Nutzer diese Daten behandeln dürfen, die in ihren Profilen enthalten sind (z. B. wann die Einwilligung eines Betroffenen vor der Veröffentlichung eingeholt werden muss oder über mögliche Konsequenzen von Regelverstößen). Insbesondere spielen Fotos in Nutzerprofilen, auf denen Personen abgebildet sind, die bei dem Netzwerk nicht angemeldet sind oder von der Veröffentlichung keine Kenntnis haben (in vielen Fällen sogar versehen mit Hinweisen auf den Namen und/oder das Nutzerprofil), in diesem Kontext eine Rolle. Die derzeit weit verbreiteten Praktiken stehen in vielen Fällen nicht in Einklang mit den bestehenden Regelungen des Schutzes des Rechts am eigenen Bild gemäß dem Kunsturhebergesetz.

Die verantwortliche Stelle ist mit einfach zugänglicher Kontaktmöglichkeit anzugeben; bei ausländischen Anbietern sollte auch eine Kontaktmöglichkeit in dem Land, auf dessen Markt das Angebot ausgerichtet ist, angegeben sein. Ferner ist zu empfehlen, die Nutzer über den Regulierungsrahmen zu informieren, dem der Betreiber des sozialen Netzwerks unterliegt. Für den Fall der Insolvenz oder des Verkaufs sind Nutzer darüber zu informieren, wie mit ihren personenbezogenen Daten umgegangen wird.

Gibt es verschiedene Nutzergruppen, sind sowohl die Datenschutzbestimmungen als auch die Nutzungsbedingungen nach Nutzergruppen zu untergliedern, sodass – falls Regelungen nur bestimmte Nutzergruppen betreffen sollten – jeder Nutzer eindeutig erkennen kann, welche Bestimmungen für ihn gelten. Dies kann der Fall sein, wenn das soziale Netzwerk neben den Nutzern mit persönlichem Profil z.B. auch professionelle Nutzer oder Drittanbieter und Entwickler im Netzwerk zulässt.

Insbesondere über den Zugriff und die Verarbeitung durch Dritte (z.B. Anbieter von Anwendungen innerhalb des Netzwerks, Kooperations- und Werbepartner oder auch Sicherheitsbehörden) sind die Nutzer zu informieren. Dies gilt auch, wenn z. B. für die Anzeige von Werbeeinblendungen in

dem Browser-Fenster eines Nutzers die IP-Adresse dieses Nutzers an einen anderen Dienstanbieter weitergegeben wird, der den Inhalt der Werbung liefert.

Bietet das soziale Netzwerk Schnittstellen für Drittanbieter an, sind der Umfang und die Weiterverwendung der Daten genau zu definieren und zu benennen.

Informationen sollten auch über verbleibende Sicherheitsrisiken gegeben werden und über andere mögliche Konsequenzen der Veröffentlichung personenbezogener Daten in einem Profil, wie auch über mögliche Zugriffe durch Dritte (einschließlich Strafverfolgungsbehörden und Geheimdiensten).

5.2 Kontrolle durch den Nutzer

Das Recht auf informationelle Selbstbestimmung setzt Kontrollbefugnisse für den Nutzer voraus. Der Anspruch, selbst zu bestimmen, wer wann was über die eigene Person weiß, soll dem Nutzer sowohl gegenüber dem Betreiber des sozialen Netzwerks als auch gegenüber anderen Nutzern und Drittanbietern eingeräumt werden. Dies schließt nicht nur die selbstgenerierten Daten (z.B. Informationen über die eigene Person), sondern auch fremdgenerierte Daten (z.B. Markierungen auf Fotos durch Dritte) mit ein. Die Kennzeichnung von Fotos (d. h. das Hinzufügen von Links auf existierende Nutzerprofile oder des Namens der abgebildeten Person/en) sollte an die vorherige Einwilligung der Betroffenen gebunden sein.

Die Konfigurations- und Einstellungsmöglichkeiten sollten also zulassen, dass Informationen gruppen- oder personenbezogen sichtbar sind. Eine Weitergabe an Dritte (Nutzer des Netzwerks, Entwickler, Werbepartner) ohne explizite Einwilligung des Betroffenen ist unzulässig. Verständliche und übersichtliche Hilfestellungen zu den Einstellungsmöglichkeiten inklusive klarer Angaben über die möglichen Auswirkungen, ggf. ergänzt durch FAQs, sowie die höchstmögliche Schutzeinstellung zum Zeitpunkt der Registrierung (datenschutzfreundliche Standardeinstellungen, die der Nutzer auf eigenen Wunsch verändern kann) erlauben dem Nutzer, selbstbestimmt mit seinen Informationen umzugehen. Informationen, die auf Grund schwacher Schutzeinstellungen (möglicherweise sogar ohne das Wissen der Nutzer) offen für Dritte innerhalb und außerhalb des Netzwerks abrufbar sind und ggf. durch Suchmaschinen erfasst werden, unterliegen nicht mehr der Kontrolle der Nutzer und widersprechen dem Grundsatz der informationellen Selbstbestimmung. Die Kontrolle des Nutzers über die eigenen Daten muss auch gewährleistet werden, wenn er diese bewusst an Dritte weitergibt. Eine Weitergabe der Daten durch diese Dritten ohne Einwilligung des Betroffenen ist grundsätzlich nicht zulässig.

Werden Daten durch den Nutzer gelöscht, sollten Anbieter sicherstellen, dass die Löschung auch für etwaige Kopien, die Dritten zur Verfügung gestellt wurden, umgesetzt wird, es sei denn, der Nutzer hat in die weitere Nutzung eingewilligt.

Um kontrollieren zu können, welche Daten der Betreiber über die betroffene Person gespeichert hat, muss die Umsetzung des Auskunftsanspruchs nach § 34 Abs. 1 BDSG durch den Betreiber des sozialen Netzwerks gesichert sein. Dies kann über ein Online-Abrufverfahren erfolgen, muss aber alle vom Betreiber gespeicherten Daten (Inhalts-, Bestands- und Nutzungsdaten) beinhalten. Es bedarf in diesem Fall eines bestmöglichen Schutzes vor Missbrauch.

Bei international ausgerichteten Netzwerken ist darauf zu achten, dass die Nutzerkontrolle nicht durch Sprachbarrieren gefährdet ist.

5.3 Interne Kontrolle

Die Einhaltung der Datenschutzbestimmungen muss in internen Datenschutzrichtlinien und Konzepten festgelegt sowie ggf. durch einen internen Datenschutzbeauftragten kontrolliert werden.[23] Hierbei muss sichergestellt sein, dass dieser in seiner Funktion weisungsfrei, der Unternehmensleitung direkt unterstellt, ausreichend geschult und qualifiziert ist. Dieser muss hinreichend unterstützt und rechtzeitig über datenschutzrelevante Änderungen informiert werden. Neue oder geänderte Funktionen sind in der Regel durch eine Vorabkontrolle auf Datenschutzverstöße zu kontrollieren (insbesondere bei Risiken für die Rechte und Freiheiten der Betroffenen wie z.B. bei der Verarbeitung besonderer Datenkategorien wie politische Meinung, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben).[24]

Datenschutzkonzepte (inklusive Rechte- und Rollenkonzepte) und technische Dokumentationen sind vor dem Produktivbetrieb zu erstellen und legen – neben der Dokumentation der Systeme und ihrer Funktionen – insbesondere den Umgang und die Verwendung (Zweckbindung) der zu verarbeitenden Daten, den Schutzbedarf der Daten sowie die technischen und organisatorischen Maßnahmen fest, die vom Betreiber des sozialen Netzwerks zu ergreifen sind. Die Datenschutzkonzepte sind zu aktualisieren, sobald Änderungen oder Neuerungen entwickelt werden.

Technische und organisatorische Maßnahmen sind insbesondere zu ergreifen, um zu gewährleisten, dass die Vertraulichkeit und Integrität der Daten gesichert ist. Die Verknüpfung verschiedener Daten bzw. die Zweckentfremdung der Daten ist zu verhindern. Hierfür ist eine revisionssichere Protokollierung zu installieren, die die Zugriffe auf die Anwendung und auf das System protokolliert

[23] Vgl. § 4f BDSG.
[24] Vgl. § 4d Abs. 5 BDSG.

(„wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?“ und „wer hatte von wann bis wann welche Zugriffsrechte?“). Zusätzlich kontrolliert ein Monitoring die Verfügbarkeit der Systeme und informiert rechtzeitig über Unregelmäßigkeiten. Die Informationen der Systeme sind über festgelegte Mitarbeiter bei Bedarf auszuwerten und ggf. in geeignete Maßnahmen zu überführen.

5.4 Externe Kontrolle

Die externe Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen obliegt den Aufsichtsbehörden für den Datenschutz, die entsprechend der gesetzlichen Vorgaben deutsches Datenschutzrecht (vgl. 0) oder das Datenschutzrecht des jeweiligen Sitzstaates anzuwenden haben. Die Zuständigkeit der deutschen Aufsichtsbehörden ergibt sich aus § 38 Abs. 1 S. 1 BDSG.

Die sachliche Zuständigkeit der Aufsichtsbehörde ergibt sich aus dem jeweiligen Landesdatenschutzgesetz bzw. dem Bundesdatenschutzgesetz. Die örtliche Zuständigkeit knüpft an den (deutschen) Sitz der verantwortlichen Stelle an.

Um die ergriffenen technisch-organisatorischen Maßnahmen zu verbessern, können verantwortliche Stellen ihre Verfahren und Anwendungen auch durch einen unabhängigen Auditor prüfen und bewerten lassen.

6 Integrität und Authentizität

Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[25] Dieses Recht schließt die Gewährleistung der Unversehrtheit und der korrekten Funktionsweise von Systemen mit ein. Die Integrität der Daten ist gegeben, wenn die Daten vollständig und unverändert sind.[26]

Nutzer müssen sich also darauf verlassen können, dass die Informationen – ihre eigenen, aber auch die der anderen Nutzer – vollständig und richtig, d. h. nicht durch Dritte verändert, sind, es sei denn, dies ist eindeutig erkennbar. Nach der Anlage zu § 9 Satz 1 BDSG ist durch technische und organisatorische Maßnahmen sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht verändert werden können. Zusätzlich muss durch die verantwortliche Stelle sichergestellt sein, dass die Systeme und Anwendungen korrekt funktionieren. Werden Sicherheitslücken oder bereits eingetretene Scha-

[25] 1 BvR 370/07, 1 BvR 595/07 http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.
[26] https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

densfälle entdeckt, sind sofort Gegenmaßnahmen zu ergreifen und betroffene Nutzer umgehend darüber und über die ergriffenen Maßnahmen zu informieren. Der Umfang an personenbezogenen Daten in sozialen Netzwerken und deren teilweise hoher Schutzbedarf erfordern hohe Standards bei der IT-Sicherheit, um die Daten vor Missbrauch wie z.B. Identitätsdiebstahl zu schützen.

Eng verbunden mit dem Begriff der Integrität ist die Authentizität der Nutzer sowie der technischen Systeme. Personen oder Organisationen, die in die eigene Kontaktliste aufgenommen werden, haben oft einen weiter reichenden Zugriff auf die persönlichen Informationen. Ein Nutzer muss also erkennen können, wer hinter dem Profil steht. Private Nutzer haben das Recht, Telemedien anonym oder pseudonym zu nutzen, jedoch muss das Vortäuschen einer falschen Identität (Identitätsdiebstahl) ausgeschlossen werden. Hierfür muss die verantwortliche Stelle Maßnahmen ergreifen, um so gut wie möglich sicherzustellen, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Dies beinhaltet einerseits Sicherheitsmaßnahmen, um den Zugriff auf die Konten der Nutzer zu schützen (z.B. Zugriff nur über gesicherte Verbindungen, Passwortmindestanforderungen), aber auch Überwachungssysteme, um z.B. Missbrauch durch virtuelle Profile (sog. Social bots27) schnell zu erkennen und zu verhindern.

Lässt ein soziales Netzwerk zu, dass Organisationen, öffentliche Stellen oder Unternehmen Seiten im Netzwerk betreiben, sollte dies nur vertretungsberechtigten Personen erlaubt sein. Gibt ein Nutzer vor, im Namen von Organisationen, öffentlichen Stellen oder Unternehmen zu handeln, kann so das Vertrauen der Nutzer erschlichen werden, die der Organisation, der öffentlichen Stelle oder dem Unternehmen ggf. weiter reichenden Zugriff auf Informationen geben.

7 Vertraulichkeit

Soziale Netzwerke werden zu unterschiedlichen Zwecken von öffentlichen Stellen, insbesondere von Sicherheitsbehörden, genutzt. Informationen aus sozialen Netzwerken können für öffentliche Stellen etwa erforderlich sein, um Straftaten aufzuklären oder um Gefahren für die öffentliche Sicherheit zu erkennen und abzuwehren. Inwieweit ein Zugriff auf die Daten in sozialen Netzwerken zulässig ist, müssen die öffentlichen Stellen nach den für sie geltenden Rechtsvorschriften in eigener Verantwortung bewerten.

Betreiber sozialer Netzwerke sind nach deutschem Recht z.B. verpflichtet, beschlagnahmte Unterlagen nach § 98 StPO an Strafverfolgungsbehörden herauszugeben oder, soweit sie Telekommunikationsdienste anbieten, nach § 100g StPO Auskunft über Verkehrsdaten zu erteilen.

[27] http://www.heise.de/security/meldung/Studie-Viele-Facebook-Nutzer-sind-sorglos-1370431.html

Behörden erlangen Informationen nicht nur über Auskunftsersuchen an die Betreiber, sondern häufig durch eigene Recherchen in sozialen Netzwerken.

Es bestehen erhebliche datenschutzrechtliche Bedenken gegen eine Anwendung der Ermittlungsgeneralklauseln als Rechtsgrundlage für verdeckte Recherchen in nicht öffentlich zugänglichen Bereichen sozialer Netzwerke.

8 Verfügbarkeit

Die verantwortliche Stelle hat sicherzustellen, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Dies bedeutet für Betreiber sozialer Netzwerke zunächst, dass die Daten gegen zufällige oder absichtliche Zerstörung und Verlust durch das Ergreifen von technischen und organisatorischen Maßnahmen geschützt werden müssen.28 Weiter muss sichergestellt sein, dass Nutzer nicht nur jederzeit auf ihre personenbezogenen Daten zugreifen können, sondern auch die Verfügungsgewalt hierüber haben. Eine dritte Ebene betrifft die öffentliche Verfügbarkeit der Daten.

Zur Sicherstellung der technischen Verfügbarkeit muss die Infrastruktur durch den Betreiber so abgesichert sein, dass z.B. externe Einflüsse wie Feuer oder Wasser bestmöglich abgewehrt werden können, eine dauerhafte Stromversorgung gewährleistet ist und die Daten durch Backup-Konzepte vor Verlust geschützt sind.

Die Verfügbarkeit der Daten für Nutzer beinhaltet zunächst den Zugriff auf ihre personenbezogenen Daten in dem sozialen Netzwerk. Dies steht in direktem Zusammenhang mit der o. g. technischen Verfügbarkeit sowie mit den Zugriffsrechten auf die eigenen Daten. Inhaltsdaten müssen unter der direkten Kontrolle der Nutzer stehen, d. h. die Daten sind zur Bearbeitung und Löschung durch den Nutzer selbst verfügbar zu halten. Kündigt ein Nutzer sein Konto in dem sozialen Netzwerk, sollte die Möglichkeit bestehen, die dort gespeicherten (Inhalts-) Daten vor der Löschung zu exportieren (diese Möglichkeit kann auch ohne das Löschbegehren zu jedem Zeitpunkt zur Verfügung gestellt werden). Dies schließt neben Texten auch die Fotos und weitere Medien ein. Die exportierten Daten sollten in gängigen, wiederverwendbaren Formaten zur Verfügung gestellt werden.29

---

[28] Vgl. BDSG, Anlage zu § 9 Satz 1: Es sind „(…) sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, (…) zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)."

[29] Geeignet wären etwa PDF oder XML.

Die öffentliche Verfügbarkeit von Profilen, d. h. die Sichtbarkeit von personenbezogenen Daten wie Profilname, Foto oder Geschlecht, erleichtert zwar das Auffinden der Person in dem sozialen Netzwerk, darf aber nicht außerhalb der Verfügungsgewalt der betroffenen Person stehen. Öffentlich zugängliche Daten – sowohl innerhalb des Netzwerks für registrierte Nutzer als auch außerhalb des Netzwerks, z.B. durch die Indexierung durch Suchmaschinen – erhöhen das Risiko eines Identitätsdiebstahls, so dass Nutzer zur Ausübung ihres Rechts auf informationelle Selbstbestimmung die Möglichkeit haben müssen, die Verfügbarkeit ihrer Daten gegenüber Dritten einzuschränken. Dabei ist angezeigt, dass die jeweils datenschutzfreundlichste Variante bereits seitens des Anbieters voreingestellt ist.

9 Intervenierbarkeit (Betroffenenrechte)

9.1 Änderungen des Funktionsumfangs sozialer Netzwerke

Soziale Netzwerke sind komplexe Gebilde, welche einer stetigen Änderung unterworfen sind. Durch die Einführung neuer Funktionen können – möglicherweise unbeabsichtigt – Änderungen erfolgen, die sich enorm auf die Rechtevergabe auswirken.

Die Einhaltung der Prinzipien „Privacy by Design“ und davon abgeleitet „Privacy by Default“ wird daher von Daten- wie auch Verbraucherschützern beständig gefordert. „Privacy by Design“ setzt eine auf Datenschutzbelange Rücksicht nehmende Entwicklung von Produkten voraus. „Privacy by Default“ bedeutet in der Anwendung auf soziale Netzwerke, dass neue Nutzer beim Beitritt und bestehende Nutzer bei der Einführung neuer Funktionen eine selbstbestimmte Entscheidung treffen können, für wen welche Daten sichtbar oder gesperrt sind. Dies sollte zunächst nur der Nutzer selbst sein, welcher dann schrittweise sein Profil für weitere Personen oder Gruppen öffnen kann. Die dabei geltenden Regeln und Abläufe müssen transparent sein und sollten auf evtl. unbeabsichtigte Änderungen verständlich hinweisen. Die Nutzergruppen, welche Zugriff auf die Daten des Netzwerkes haben können, müssen klar benannt werden (z.B. Freunde, Freunde von Freunden, Nicht-Mitglieder, Suchmaschinen), um dem Nutzer einfache Entscheidungen zu ermöglichen. Werden die Nutzungsregeln für ein soziales Netzwerk geändert, muss dies transparent erfolgen und muss mit einer angemessenen Übergangsfrist bekanntgegeben werden. Weiterhin ist Nutzern die Möglichkeit einzuräumen, Änderungen abzulehnen (siehe hierzu auch Kapitel 0).

Neue Funktionen dürfen niemals ohne aktive Änderungen der Einstelllungen durch den Nutzer zu einer Ausweitung des Umfangs der veröffentlichten Daten oder deren Sichtbarkeit innerhalb und außerhalb des Netzwerks führen.

9.2 Löschen

9.2.1 Löschen von Inhalten der Nutzer

Betreiber sozialer Netzwerke sind grundsätzlich verpflichtet, Löschungsbegehren der Nutzer in Bezug auf deren eigene personenbezogene Daten unverzüglich umzusetzen.

Das Löschen als technischer Prozess ist bei digitalen Verfahren ein mehrstufiger Prozess, der in der Regel für den Nutzer intransparent bleibt. Verteilte Dateisysteme führen teilweise zu Problemen, erteilte Löschbefehle physisch auszuführen, da die Daten an mehreren Orten physisch vorgehalten werden und einzelne Objekte mehrfach vorhanden sein können. Zudem können sich logische und rechtliche Grenzen bei solchen Daten ergeben, die zum Bestandteil der Profile anderer Nutzer geworden sind (z.B. durch Zitieren, Verweisen, „Liken“).

Zwar kann es im Interesse der Nutzer sein, die Daten für eine Wiederherstellung versehentlich gelöschter Daten noch kurzfristig vorzuhalten (vergleichbar mit einem Papierkorb); die sich daran anschließende Löschung muss jedoch sicher und endgültig erfolgen. Insbesondere muss ein Netzwerkbetreiber zuverlässige und überprüfbare Aussagen darüber treffen, wann zur Löschung vorgesehene Daten endgültig vernichtet sind.

Netzwerkbetreiber sollten außerdem die Möglichkeit vorsehen, personenbezogene Daten, die zum Gegenstand der Profile anderer Nutzer geworden sind, zu entfernen. Betreiber können jedoch die Löschung begrenzen, wenn dadurch die Wahrnehmung berechtigter und gesetzlich anerkannter Interessen, z.B. die Wahrnehmung der Meinungsfreiheit, der jeweiligen Profilinhaber beeinträchtigt werden. Die Grenzen der Löschung sind gegenüber den Nutzern transparent zu machen.

9.2.2 Verfallsdaten von Inhalten der Nutzer

Bereits längere Zeit wird über das „Gedächtnis des Internets“ und die Wiederauffindbarkeit von Informationen, die zum Teil schon lange zurückliegen, diskutiert. Die derzeitige Generation der Nutzer sozialer Netzwerke wird im Alter ein mehr oder weniger vollständiges digitales Abbild ihrer selbst im Netz vorfinden.30 Vor dem Hintergrund der stetig voranschreitenden technischen und analytischen Möglichkeiten ruft dies nachvollziehbare Ängste hervor.

Die Frage nach Verfallsdaten, automatischen Löschroutinen und Sperrungen stellt sich insbesondere im Kontext der sozialen Netzwerke. Es gibt erste technische Ansätze zur automatisierten Lö-

[30] Vgl. BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Studie Soziale Netzwerke – zweite, erweiterte Studie, http://www.bitkom.org/files/documents/BITKOM_Publikation_Soziale_Netzwerke_zweite_Befragung.pdf.

schung von Daten31, die sich jedoch bisher auch noch nicht genug praxistauglich erwiesen haben.32

In erster Linie sind die Betreiber gefordert, entsprechende Funktionen einzuführen und nutzerfreundlich zu gestalten. Hierbei sind verschiedene Modelle denkbar, angefangen von Standardfragen bei der Veröffentlichung von Beiträgen nach deren vorgesehener Gültigkeitsdauer bis hin zu einfach zu bedienenden Löschroutinen. Denkbar ist auch, die öffentliche Zugänglichkeit von Profildaten zeitlich zu begrenzen.

Weiterhin ist angesichts neuerer technischer Entwicklungen, z.B. auf Basis von HTML533 oder IPv634, zu prüfen, inwieweit damit mehr Selbstkontrolle über Nutzerdaten bzw. eine Aufweichung der bestehenden Kunden-Contentprovider-Strukturen möglich ist.

9.2.3 Abmeldung von einem sozialen Netzwerk

Die Abmeldung aus einem sozialen Netzwerk muss einfach und endgültig möglich sein. Die von einzelnen Netzwerken geübte Praxis, Profile in einen „Ruhezustand“ zu versetzen, um dem Nutzer eine spätere Rückkehr zu ermöglichen, ist unzureichend. Der Nutzer muss eine vollständige Kontrolle über seine Daten erlangen und selbst bestimmen können, wie mit seinen Daten verfahren wird. Dabei kann grob zwischen endgültiger Abmeldung (und damit einhergehender Löschung), Ruhezustand (und Nichtsichtbarkeit für Dritte) und einer Mitnahme der Daten (mit anschließender Löschung beim Betreiber) unterschieden werden. In diesen Fällen sind folgende Anforderungen zu erfüllen:

- Der Nutzer sollte eine explizite Löschbestätigung anfordern können, indem der Betreiber eine Löschung in Textform zusichert.
- Die Effektivität der Löschroutinen oder anlassbezogenen Löschungen sollten durch den Betreiber mittels entsprechender allgemein zugänglicher Dokumentation nachgewiesen werden.
- Die Betreiber haben transparent über die Aufbewahrungsfristen für inaktive Accounts zu informieren.

---

[31] Vgl. Saarland University - Information Security and Cryptography Group - Prof. Dr. Michael Backes, X-pire! - Wie man dem Internet das "Vergessen" beibringt, http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/.
[32] Vgl. Universität Regensburg, Lehrstuhl Wirtschaftsinformatik 4 - Management der Informationssicherheit, Fakultät für Wirtschaftswissenschaften, Prof. Dr. Hannes Federrath, Digitaler Radiergummi und seine Folgen, http://www-sec.uni-regensburg.de/research/streusand/.
[33] Vgl. Konrad Lischka, Hier liest Facebook nicht mit, SPIEGEL ONLINE, http://www.spiegel.de/netzwelt/web/0,1518,825950,00.html.
[34] Vgl. Lutz Donnerhacke, Kommentar: IPv6 und der Datenschutz, heise online, http://www.heise.de/netze/artikel/Kommentar-IPv6-und-der-Datenschutz-1375692.html.

9.3 Auskunft an Betroffene

Betreiber sozialer Netzwerke sind zur (vollständigen) Auskunft nach § 34 BDSG bzw. § 13 Abs. 7 TMG verpflichtet.

Für Auskunftsersuchen hat der Betreiber eine einfach zu erreichende Kontaktmöglichkeit innerhalb des Netzwerks einzurichten. Um Missbrauch zu verhindern, müssen Auskunftsersuchen angemessen sicher autorisiert werden, z.B. durch eine Bestätigungsmail an die für das Nutzerprofil registrierte E-Mail-Adresse. Der Nutzer muss die Form der Auskunft (in Textform/elektronisch) wählen können.

Eine Auskunft muss Inhalts-, Bestands- und Nutzungsdaten vollständig umfassen. Inhalts- und Bestandsdaten sind dabei die im Netzwerk hinterlegten persönlichen Daten, Kommunikationen, Bilder und Videos. Nutzungsdaten umfassen das Logging des Nutzers, also welche Seiten des sozialen Netzwerks oder externer Quellen, die über Social Plug-ins mit dem Netzwerk verbunden sind, er besucht hat, wann und wie er sich ein- oder ausgeloggt hat oder welche Anfragen ihn innerhalb des Netzwerks erreicht haben. Ebenfalls vom Auskunftsrecht umfasst sind Nutzungsdaten, durch die der Nutzer auch nach dem Ausloggen für das Netzwerk identifizierbar bleibt, z.B. über ein Cookie oder das Browserprofil. Weiterhin sollten einfache Möglichkeiten des Downloads von eigenen Profilen etabliert werden. Der Entwurf der neuen EU-Datenschutzgrundverordnung sieht ein solches Prinzip der Datenportabilität als Recht der informationellen Selbstbestimmung der Nutzer vor.

Auch Nicht-Nutzern ist ein Recht auf Auskunft zu den über sie gespeicherten personenbezogenen Daten einzuräumen. Dafür müssen Betreiber sozialer Netzwerke transparent darstellen, in welcher Weise Daten von Nicht-Nutzern erhoben und verarbeitet werden, z.B. durch den Abgleich von Adressbüchern von Mitgliedern, welche auch Daten von Nicht-Mitgliedern enthalten können.

10 Einzelthemen

10.1 Zugriff auf Adressen

Häufig werden von den Betreibern Funktionen angeboten, die es dem Nutzer ermöglichen, ein auf dem Gerät (PC, Smartphone) gespeichertes oder bei einem E-Mail-Provider geführtes Adressbuch dem sozialen Netzwerk vollständig zur Verfügung zu stellen (sog. Friend-Finding).

Hierbei ist neben der expliziten Einwilligung des Nutzers eine Möglichkeit zur Vorabprüfung der Adressen und zur Sperrung von Einzeladressen durch den Nutzer vor der Übertragung notwendig. Eine automatische Übertragung aller Adressen eines Nutzers an ein soziales Netzwerk ist nicht zulässig. Der Nutzer hat die Verantwortung für die Daten der betroffenen Dritten. Er muss erkennen können, welche Adressen übertragen wurden und muss diese bei Bedarf löschen können.

Besondere Risiken bestehen beim Hochladen beruflich erlangter Kontaktdaten in ein Profil eines Sozialen Netzwerks, z.B. wenn Ärzte oder Psychotherapeuten Kontaktdaten ihrer Patienten bzw. Klienten dafür freigeben und diese dann auf einmal z.B. Freundschaftsanfragen an ihre dortigen Profile übermittelt bekommen. Auf diese Risiken sollten Betreiber Sozialer Netzwerke hinweisen.

Eine Nutzung der Adressdaten durch den Betreiber eines Sozialen Netzwerks für eigene Zwecke im Rahmen der Werbung für den Beitritt zum eigenen Netzwerk (Friend-Finding) ist nur mit Einwilligung der Betroffenen zulässig.

10.2 Biometrie

Der Einsatz biometrischer Verfahren im Rahmen sozialer Netzwerke erfordert besondere Rahmenbedingungen. Von praktischer Bedeutung ist dabei vor allem das Verfahren der Gesichtserkennung, welches die automatische Markierung von Personen auf in das soziale Netzwerk hochgeladenen Bildern erlaubt.

Die Erstellung, Speicherung und weitere Verwendung biometrischer Daten erfordert die vorherige, explizite Einwilligung der Betroffenen. Diese Einwilligung kann nur auf der Basis einer umfassenden Information der Betroffenen über die Art und Weise der Verwendung der entsprechenden persönlichen Daten in diesem Zusammenhang erfolgen (informierte Einwilligung).

Betreiber eines sozialen Netzwerks dürfen lediglich die Daten registrierter Nutzer, deren entsprechende Einwilligung vorliegt, verarbeiten. „No matches“, also personenbeziehbare biometrische Daten, die keinem Nutzer des sozialen Netzwerkes zuzuordnen sind, müssen unverzüglich und irreversibel gelöscht werden. Neue, nachträgliche Erkennungs- bzw. Zuordnungsvorgänge („Matchingläufe“), etwa über den Bestand nicht identifizierter Personen, sind nicht zulässig. Ein biometrischer Abgleich eines neuen Mitglieds (oder nach der Einwilligung eines Mitglieds) mit dem bisherigen, kompletten Datenbestand des sozialen Netzwerkes darf nicht erfolgen.

Nur unter den soeben genannten Bedingungen ist die Einholung einer Einwilligung zur Erstellung temporärer biometrischer Daten entbehrlich. Nach Erstellung des temporären Templates muss durch den Betreiber geprüft werden, ob eine Einwilligung in die dauerhafte Speicherung des Templates vorliegt. Ist dies nicht der Fall, muss nach den beschriebenen Bedingungen eine Löschung vorgenommen werden. Die Erfüllung dieser Anforderung ist durch eine entsprechende Dokumentation nachzuweisen.

Die Möglichkeit zur jederzeitigen Rücknahme der Einwilligung ist sicherzustellen; die sich daraus ergebenen Konsequenzen müssen technisch umgesetzt werden. Das Referenztemplate muss

gelöscht und dessen Verknüpfung bzw. Zuordnung über den gesamten Datenbestand des sozialen Netzwerkes aufgelöst werden.

Für die Übermittlung biometrischer Daten durch den Betreiber des sozialen Netzwerkes an Dritte oder die Nutzung für andere Dienste ist eine entsprechende weitergehende Einwilligung beim Betroffenen erforderlich (informierte Einwilligung).

Es ist technisch und organisatorisch sicherzustellen, dass die biometrischen Daten ausschließlich für die Zwecke genutzt werden, für die sie auch erhoben wurden und denen die Betroffenen im Rahmen ihrer Einwilligung zugestimmt haben.

Bei der Aufnahme und der Übertragung der Bilder (Upload) sind verschlüsselte Kommunikationswege zu nutzen. Dies gilt insbesondere dann, wenn die biometrischen Algorithmen im Endgerät der Nutzer ablaufen und die Ergebnisse dieser Verfahren mit zentralen Datenbanken abgeglichen werden.[35]

10.3 Werbung

Im Hinblick auf Bestandsdaten (zum Begriff siehe 0) sieht das einschlägige TMG keine andere gesetzliche Grundlage für eine Verwendung zum Zweck der Werbung als die Einwilligung der Nutzenden vor. Gleiches gilt für die Nutzungsdaten (zum Begriff siehe 0), jedenfalls wenn diese nicht lediglich unter einem Pseudonym zusammengeführt werden (siehe unten 10.4 Reichweitenanalyse). Im Hinblick auf die nach dem BDSG zu beurteilenden Inhaltsdaten ist insbesondere für Werbung auf der Basis von Profildaten nach § 3 Abs. 9 BDSG – dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben – eine informierte Einwilligung der Betroffenen erforderlich.

10.4 Reichweitenanalyse

Betreiber sozialer Netzwerke, vor allem diejenigen, die eine Finanzierung des Angebotes über Werbeeinnahmen durchführen, betreiben Reichweitenanalysen, mittels derer die Art und Weise der Nutzung des Dienstes sowie die Interessen und Vorlieben der Nutzer festgestellt, analysiert und ausgewertet werden können.

---

[35] Vgl. auch Working Paper 192 der Art. 29-Gruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, vom 22. März 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf.

Durch eine derartige Reichweitenanalyse werden umfangreiche und sehr detaillierte Aussagen über die Nutzerinnen und Nutzer durch die Betreiber erhoben, die umfangreiche und sehr detaillierte Aussagen über die Nutzer erlauben, die über die willentlich und bewusst angegebenen Informationen hinausgehen. Die Nutzer sollten grundsätzlich selbst in die Lage versetzt werden, die Datenverarbeitung in ihren Geräten zu steuern. Letzteres ist z.B. durch den Einsatz von Browser-Plug-ins realisierbar. Dadurch kann z.B. das Speichern von Cookies oder Ausführen von Java-Script-Programmen unterbunden werden.

Der Umfang und die Art der Daten der Reichweitenanalyse kann von der Verarbeitung rein technischer Angaben, wie z.B. des genutzten Betriebssystems bis hin zu einer detaillierten Erfassung der Mouse-Aktivitäten eines einzelnen Nutzers reichen. Auch der Fokus der Analyse kann unterschiedlich sein. Einige Anbieter können durch den Einsatz von Social Plug-ins nicht nur die Nutzung des eigenen Dienstes analysieren. Auch die Nutzung anderer Angebote des Internets durch die in dem jeweiligen Netzwerk angemeldeten Nutzer wird analysiert.

Unabhängig von der technischen Art und Weise der eingesetzten Reichweitenanalyse ist diese nur zulässig, wenn sie auf einer entsprechenden rechtlichen Grundlage beruht. Als gesetzliche Rechtsgrundlage kommt § 15 Abs. 3 TMG zur Anwendung. Danach ist die Analyse der Nutzung des angebotenen Dienstes oder darüber hinaus zur

- Werbung,
- Marktforschung oder
- bedarfsgerechten Gestaltung des eigenen Dienstes

zulässig. Die Wahrung dieser Voraussetzung ist durch den Betreiber des Netzwerkes nachzuweisen. Dies gilt insbesondere in den Fällen, in denen die Analyse des Nutzungsverhaltens über das eigene Angebot hinausreicht. Eine anbieterübergreifende Reichweitenanalyse kann nicht auf § 15 Abs. 3 TMG gestützt werden und bedarf regelmäßig der Einwilligung der Nutzenden.

Die Reichweitenanalyse muss den Nutzern kenntlich gemacht werden. Ihnen ist außerdem gemäß § 15 Abs. 3 TMG die Möglichkeit einzuräumen, der Erhebung, Verarbeitung und Nutzung der Informationen über die Nutzung des Dienstes oder anderer Angebote des Internets widersprechen zu können. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen.

Die Erstellung der Nutzungsprofile ist nur bei Verwendung von Pseudonymen zulässig. Die IP-Adresse ist kein Pseudonym i. S. d. § 15 Abs. 3 TMG.36 Betreiber haben daher sicherzustellen, dass die Pseudonyme nicht aus leicht reidentifzierbaren Daten bestehen.

Gemäß Art. 5 Abs. 3 der E-Privacy-Richtlinie muss der Nutzer bei Cookies, die nicht zur Erbringung eines Dienstes erforderlich sind, vor deren Speicherung seine Einwilligung erteilt haben. Diese Regel ist bei Cookies, die zur Reichweitenanalyse genutzt werden, anwendbar.

Betreiber sozialer Netzwerke sind, anders als andere Anbieter von anmeldefreien Internetdiensten, zumeist sehr einfach in der Lage, die unter Pseudonym erstellten Nutzungsprofile einzelnen Nutzern zuzuordnen. Eine derartige Verknüpfung zwischen den von den Nutzern erstellten Profilen und den durch den Betreiber erstellten Nutzungsprofilen ist nur zulässig, wenn die Betroffenen vorher eingewilligt haben. Die Einwilligung muss den Anforderungen des § 4a BDSG bzw. § 13 Abs. 2 TMG entsprechen.

Eine Zusammenführung dieser Angaben ohne die Einwilligung der Nutzer ist unzulässig und stellt einen Bußgeldtatbestand dar.

Für Themennetzwerke, die für besondere Nutzergruppen eingerichtet wurden, können Beschränkungen hinsichtlich der grundsätzlichen Zulässigkeit der Nutzungsanalyse bestehen. So unterliegen aufgrund des hohen Schutzbedarfes besonderer personenbezogener Daten (§ 3 Abs. 9 BDSG) soziale Netzwerke zu den Themen Gesundheit, sexuelle Orientierung, politische oder religiöse Anschauungen etc., gesonderten und besonderen Rechtfertigungsanforderungen hinsichtlich der Durchführung der Reichweitenanalyse. Die Erforschung und Auswertung des Nutzerverhaltens ist nur auf der Grundlage einer Einwilligung zulässig. Gleiches gilt für soziale Netzwerke ohne unmittelbaren thematischen Bezug zu besonderen personenbezogenen Daten, bei denen derartige Daten zum Zweck der Reichweitenanalyse genutzt werden. Auch hier ist eine gesonderte Einwilligung erforderlich.

10.5 Nutzung auf mobilen Endgeräten

Die Verwendung eines sozialen Netzwerks auf einem mobilen Gerät unterscheidet sich in einigen Punkten wesentlich von der Verwendung mit einem Webbrowser, wenn spezielle Apps oder eine Integration von (mehreren) sozialen Netzwerken in das Betriebssystem des mobilen Gerätes zum Einsatz kommen. Die grundsätzlichen Funktionalitäten wie Kontakte knüpfen und pflegen, Nachrichten austauschen und Bilder und Fotos teilen, sind auf mobilen Geräten wie Smartphones oder

[36] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 in Stralsund, http://www.informationsfreiheit-mv.de/dschutz/beschlue/Analyse.pdf.

Tablets ebenfalls vorhanden. Darüber hinaus sind Lokalisierungsdaten über den eigenen Aufenthaltsort sowie ggf. die Standorte anderer Teilnehmer des sozialen Netzwerks verfügbar.

10.5.1 Umgang mit Lokalisierungsdaten

Mobile Endgeräte verfügen üblicherweise über Ortungsdienste, welche mit GPS sowie durch Informationen aus WLAN-Hotspots und Mobilfunkmasten realisiert werden. Sollen diese standortbezogenen Daten an ein soziales Netzwerk übertragen werden, wird eine Einwilligung des Nutzers benötigt, soweit dies nicht für die Erbringung der jeweiligen Dienstleistung erforderlich ist. Die Voreinstellung dieser Datenübertragung sollte derart sein, dass keine Daten übertragen werden. Sollen die Standortdaten allen Personen eines sozialen Netzwerks zugänglich gemacht werden, dann ist eine eindrückliche Warnung an den Nutzer erforderlich. Alle Einstellungen zur Lokalisierung sollten über einen leicht auffindbaren Menüpunkt klar erkennbar und jederzeit änderbar sein. Eine Deaktivierung Nutzung und Löschung der Standortdaten muss jederzeit leicht möglich sein; eine Deaktivierung aller Ortungsdienste des Gerätes ist hierfür nicht ausreichend.

Die fortlaufende Speicherung von Aufenthaltsinformationen im Sinne einer Historie ist nur gestattet, solange und soweit dies für die Erbringung einer Dienstleistung erforderlich ist. Nutzer sind über evtl. existierende Datenbestände historischer Aufenthaltsinformationen im Rahmen der Information nach § 13 Abs. 1 TMG zu unterrichten. Sie sollten darüber hinaus jederzeit die Möglichkeit haben, Aufenthaltshistorien zu löschen.

10.5.2 Übertragung

Personenbezogene Daten dürfen nur an den Betreiber des sozialen Netzwerks übertragen werden. Eine Übermittlung dieser Daten an andere Empfänger (wie den Hersteller der App-Software) ist im Allgemeinen nicht erforderlich und damit auch nicht zulässig. Sollten doch Diagnose- oder Trackingdaten zusätzlich erfasst werden, so muss hierzu die explizite Einwilligung des Nutzers eingeholt oder sämtliche personenbezogenen Daten vor der Übertragung i. S. d. § 3 Abs. 6 BDSG anonymisiert werden.

Eine Übertragung der Daten muss über eine ausreichend verschlüsselte Verbindung (SSL/TLS) erfolgen und gegen unberechtigte Zugriffe (Man-In-The-Middle-Angriffe) geschützt sein.

Literatur

[1] Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282012%294&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864#RelatedDocuments

[2] Selbstbedienungsladen Smartphone: Apps greifen ungeniert persönliche Daten ab, http://www.heise.de/ct/artikel/Selbstbedienungsladen-Smartphone-1464717.html

[3] Data Protection Commissioner of Ireland: Facebook Ireland Ltd Report of Audit, http://dataprotection.ie/documents/Facebook%20Report/Facebookauditreport1.pdf

[4] Data Protection Commissioner of Ireland: Facebook Technical Analysis Report, http://dataprotection.ie/documents/Facebook%20Report/report.pdf/appendices.pdf

[5] Data Protection Commissioner of Ireland: Facebook Ireland Ltd Report of Re-Audit, http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

[6] Tao Stein et al.: Facebook Immune System, http://allfacebook.de/wp-content/uploads/2011/10/FacebookImmuneSystem.pdf

[7] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 08. Dezember 2011): Datenschutz in sozialen Netzwerke, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf?__blob=publicationFile

[8] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden: Datenschutzkonforme Gestaltung sozialer Netzwerke, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/170408DatenschutzkonformeGestaltungSozNetzwerke.pdf?__blob=publicationFile

[9] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke (WP 163), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf

[10] International Working Group on Data Protection in Telecommunications: Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum" - 43. Sitzung, 3.-4. März 2008, http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf

[11] Berliner Beauftragter für Datenschutz und Informationsfreiheit: ICH SUCHE DICH. Wer bist du? Soziale Netzwerke & Datenschutz, Juli 2012, http://www.datenschutz-berlin.de/attachments/894/2012-Broschuere-Soziale-Netzwerke.pdf

[12] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: selbst & bewusst. Tipps für den persönlichen Datenschutz bei Facebook, Januar 2013, http://www.datenschutz-hamburg.de/uploads/media/selbst_bewusst-Datenschutz_bei_Facebook_01.pdf

[13] Datenschutzbeauftragter des Kantons Zürich: Checkliste Privacy Facebook, November 2012, https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/veroeffentlichungen/leitfaede

n_und_checklisten/_jcr_content/contentPar/publication_1/publicationitems/titel_wird_aus_dam_e/download.spooler.download.1355402195455.pdf/Checkliste+Privacy+Facebook.pdf

Abkürzungen

AGB	Allgemeine Geschäftsbedingungen
API	Application Programming Interface
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
FAQ	Frequently Asked Questions
GG	Grundgesetz
GPS	Global Positioning System
HDFS	Hadoop Distributed File System
HTML	Hyptertext Markup Language
IP	Internet Protocol
KUG	Kunsturhebergesetz
LDSG	Landesdatenschutzgesetz
LSO	Local Shared Object
RL	Richtlinie
SSL	Secure Sockets Layer
StPO	Strafprozessordnung
TLS	Transport Layer Security
TMG	Telemediengesetz
WLAN	Wireless Local Area Network

8.2

Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke

(Stand: Dezember 2013)

Inhaltsverzeichnis

1. Allgemeines

1.1 BDSG und UWG mit Regelungen für Werbung

§ 28 Abs. 3 BDSG enthält die datenschutzrechtlichen Regelungen für die Verarbeitung oder Nutzung personenbezogener Daten durch nicht-öffentliche Stellen für Zwecke der Werbung.

Zu den konkreten Werbeformen und dem Kontaktweg zu den betroffenen Personen (Ansprache per Postbrief, Telefonanruf, E-Mail, Fax etc.) regelt § 7 UWG, in welchen Fällen wettbewerbsrechtlich von einer unzumutbaren Belästigung der Beworbenen auszugehen und eine Werbung dieser Art unzulässig ist.

Weil § 28 Abs. 3 Satz 6 BDSG eine Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung nach den sonstigen Erlaubnisvorschriften dieses Absatzes nur für zulässig erklärt, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen, sind auch bei der datenschutzrechtlichen Beurteilung einer werblichen Verarbeitung oder Nutzung personenbezogener Daten die Wertungen von § 7 UWG für die jeweilige Werbeform mit zu berücksichtigen.

1.2 Unterrichtung bei der Datenerhebung

Werden personenbezogene Daten bei den Betroffenen erhoben, z. B. für Kaufverträge, Prospektanforderungen oder Gewinnspiele, sind die Betroffenen nach § 4 Abs. 3 BDSG u. a. über die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung der Daten zu unterrichten. Eine schon geplante oder in Betracht kommende Verarbeitung oder Nutzung der Daten für werbliche Zwecke ist daher den Betroffenen von Anfang an transparent darzulegen.

1.3 Datenerhebung einerseits – Datenerhebung und -nutzung anderseits

Für die Erhebung von personenbezogenen Daten für Zwecke der Werbung kommen als datenschutzrechtliche Grundlage die Einwilligung der betroffenen Personen sowie die gesetzlichen Erlaubnisse aus § 28 Abs. 1 Satz 1 Nrn. 1 bis 3 BDSG in Betracht.

Liegt für die **Verarbeitung oder Nutzung** personenbezogener Daten für Zwecke der Werbung keine Einwilligung vor, ist § 28 Abs. 3 BDSG die vorrangige Spezialregelung gegenüber § 28 Abs. 1 und Abs. 2 BDSG für eine solche Verarbeitung oder Nutzung.

2 Einwilligung in die Verarbeitung oder Nutzung personenbezogener Daten für Werbung

2.1 Gestaltung der Einwilligung

Nach § 4a Abs. 1 Satz 2 BDSG, der dazu ergangenen Rechtsprechung (siehe z. B. Urteil des BGH vom 25. Oktober 2012, Az. I ZR 169/10, Beschluss des KG vom 29. Oktober 2012, Az. 5 W 107/12) und den Empfehlungen der Art. 29-Datenschutzgruppe im WP 187 sind Einwilligungen nur wirksam, wenn sie in Kenntnis der Sachlage und für den konkreten Fall erklärt werden. Die Gestaltung der Einwilligungen muss also verständlich und konkret sein.

Einwilligungen für eine Verarbeitung oder Nutzung personenbezogener Daten für Werbung müssen danach auch die Art der beabsichtigten Werbung (Brief, E-Mail/SMS, Telefon, Fax), die Produkte oder Dienstleistungen, für die geworben werden soll, und die werbenden Unternehmen bezeichnen.

Dafür ist ein gesonderter Text oder Textabschnitt ohne anderen Inhalt zu verwenden.

Die Einwilligung bedarf grundsätzlich der Schriftform (Unterschrift), § 4a Abs. 1 Satz 3 BDSG. Zu Ausnahmen von der Schriftform in besonderen Fällen siehe unter Nr. 4 dieser Hinweise.

2.2 „Verfall“ der Einwilligung, Hinweis auf die UWG-Rechtsprechung

Die Zivilgerichte sehen bei erteilten Einwilligungen nach dem UWG zur werblichen Kontaktaufnahme teilweise keine unbegrenzte Gültigkeit. So hat das LG München I mit Urteil vom 8. April 2010, Az. 17 HK O 138/10, entschieden, dass eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert“ und deshalb keine rechtliche Grundlage mehr ist.

3 Hinweise zu § 28 Abs. 3 BDSG

3.1 Nur ein Gruppenmerkmal bei den Listendaten

Die in § 28 Abs. 3 Satz 2 BDSG beschriebenen Listendaten dürfen nur ein (einziges) Gruppenmerkmal enthalten (vgl. dazu auch den veröffentlichten Beschluss des Düsseldorfer Kreises vom 27. November 2009, im Internet unter
http://www.bfdi.bund.de/DE/Entschliessungen/Duessel

dorferKreis/DKreis_node.html).

3.2 Telefonnummer und E-Mail-Adresse kein Listendatum

Telefonnummer und E-Mail-Adresse zählen nach dem Wortlaut des Gesetzes in § 28 Abs. 3 Satz 2 BDSG nicht zum Listendatensatz.

3.3 Rufnummernverzeichnisse

Telekommunikationsdienste-Anbieter müssen sich an der spezialgesetzlichen Regelung in § 104 TKG orientieren, wonach es für die Zulässigkeit der Veröffentlichung von Telefonnummern und Anschlussinhabern darauf ankommt, was die betroffene Person bei ihrem Telekommunikationsdienste-Anbieter beantragt (keinerlei Veröffentlichung, Veröffentlichung nur in gedruckten oder auch in elektronischen Verzeichnissen). Andere Verzeichnisanbieter, die nicht dem TKG unterliegen, müssen dies gemäß § 29 Abs. 3 BDSG berücksichtigen.

3.4 Rechtsgeschäftliche und rechtsgeschäftsähnliche Schuldverhältnisse

Wegen der weiten Fassung der Definition von rechtsgeschäftlichen und rechtsgeschäftsähnlichen Schuldverhältnissen in § 311 BGB ist eine Anwendung von § 28 Abs. 3 Satz 2 Nr. 1 BDSG für eine werbliche Verarbeitung oder Nutzung von Adressdaten auch bei Preisausschreiben, Gewinnspielen, Katalog- und Prospektanforderungen möglich, wenn dabei die Adressdaten vom Betroffenen selbst für eine Kontaktaufnahme genannt werden; eine Einwilligung der Betroffenen ist bei solchen Sachverhalten nicht erforderlich.

3.5 Allgemein zugängliche Verzeichnisse

Weil in § 28 Abs. 3 Satz 2 Nr. 1 BDSG nur allgemein zugängliche Verzeichnisse (Adress-, Rufnummern-, Branchenverzeichnisse etc.) genannt sind, kommen für eine zulässige Datenerhebung für werbliche Zwecke auch nur solche Verzeichnisse in Betracht. Eine sonstige allgemeine Zugänglichkeit der Anschriftendaten (Zeitungsanzeigen, Anbieterkennzeichnungen im Internet usw.) genügt nach dem Wortlaut des Gesetzes nicht.

3.6 Nutzungsdauer von Listendaten aus rechtsgeschäftlichen und rechtsgeschäftsähnlichen Schuldverhältnissen

Bei § 28 Abs. 3 Satz 2 Nr. 1 BDSG stellt sich die Frage, wie lange Adressdaten mit weiteren Daten (Merkmal zur Personengruppe, evtl. hinzugespeicherte Daten) nach dem letzten aktiven Geschäftskontakt zu einem Betroffenen für die werblichen Zwecke der Reaktivierung, Rückgewinnung etc., noch genutzt werden dürfen, bzw. ab wann nach § 28 Abs. 3 Satz 6 BDSG schutzwürdige Interessen der Betroffenen einer länger währenden werblichen Nutzung entgegen stehen.

Eine konkrete Frist hat der Gesetzgeber in § 28 Abs. 3 Satz 2 Nr. 1 BDSG nicht vorgesehen. § 34 Abs. 1a BDSG sieht zwar bei der transparenten Übermittlung von Werbedaten eine Dokumentationspflicht von Herkunft und Empfänger der Daten für zwei Jahre vor. Die-

se Frist kann bei § 28 Abs. 3 Satz 2 Nr. 1 BDSG aber lediglich ein erster Anhaltspunkt sein und nicht ohne Prüfung des Einzelfalles unkritisch übernommen werden, da – je nach individuellem Sachverhalt – auch kürzere (z.B. bei reinen Interessentenanfragen) oder längere Nutzungsfristen rechtmäßig sein können.

Entscheidend ist, ob noch eine Erforderlichkeit für die weitere werbliche Nutzung der Daten von der verantwortlichen Stelle nachvollziehbar dargelegt werden kann. Als Kriterium für die Entscheidung über die Erforderlichkeit kann auf den Regelungsinhalt der Löschungsvorschrift bei einer nicht mehr erforderlichen Datenspeicherung in § 35 Abs. 2 Nr. 3 BDSG zurückgegriffen werden. Weiterhin dürfen keine schutzwürdigen Interessen der Betroffenen einer werblichen Nutzung entgegenstehen. So kann z. B. die Konditionenabfrage bei einem Bestattungsunternehmen keine längerfristige Datennutzung für werbliche Zwecke rechtfertigen.

3.7 Berufliche Werbung an die berufliche Anschrift (B2B), Spendenwerbung

Bei Nr. 2 und Nr. 3 des § 28 Abs. 3 Satz 2 BDSG wird – im Gegensatz zu Nr. 1 – nichts zur Datenerhebung ausgesagt. Damit gilt bei beruflicher Werbung an die berufliche Anschrift (Business to Business – B2B) die allgemeine Regelung aus § 28 Abs. 1 Nr. 3 BDSG, dass auch eine Datenerhebung für die berufliche Werbung und die Spendenwerbung aus allen allgemein zugänglichen Quellen möglich ist. Die weitere Verarbeitung und Nutzung der Daten für Werbung richtet sich dann nach § 28 Abs. 3 Satz 2 BDSG (Listendaten).

3.8 B2B-Werbung, Hinzuspeicherung von Daten

Die B2B-Werbung ist in § 28 Abs. 3 Satz 2 Nr. 2 BDSG speziell angesprochen. § 28 Abs. 3 Satz 3 BDSG sieht aber die Möglichkeit des Hinzuspeicherns weiterer Daten für Zwecke der (Eigen-) Werbung, also bei eigenen Kunden, dem Wortlaut nach nur bei § 28 Abs. 3 Satz 2 Nr. 1 BDSG vor.

B2B-(Eigen-)Werbung bei Bestandskunden kann jedoch auch auf § 28 Abs. 3 Satz 2 Nr. 1 BDSG gestützt werden, mit der Möglichkeit des Hinzuspeicherns weiterer Daten, wenn die dort genannten sonstigen Voraussetzungen erfüllt sind.

3.9 Hinzuspeichern und Nutzen von E-Mail-Adressen

E-Mail-Adressen, die unmittelbar von den betroffenen Personen im Rahmen einer Geschäftsbeziehung (Bestandskunden) erhoben wurden, können nach § 28 Abs. 3 Satz 3 BDSG hinzugespeichert und für E-Mail-Werbung genutzt werden. Entgegenstehende schutzwürdige Interessen des Betroffenen nach § 28 Abs. 3 Satz 6 BDSG sind u. a. dann gegeben, wenn die in § 7 Abs. 3 UWG enthaltenen gesetzlichen Vorgaben für elektronische Werbung nicht eingehalten werden.

3.10 Hinzuspeichern und Nutzen von Telefonnummern

Für Werbeanrufe bei **Verbrauchern** sieht das UWG keine Ausnahme vom Einwilligungser-

fordernis vor, so dass ein Hinzuspeichern und Nutzen von Telefonnummern wegen der besonderen Auswirkungen dieser Werbeform (stärkere Belästigung/Störung) datenschutzrechtlich an den entgegenstehenden schutzwürdigen Interessen der Betroffenen gemäß § 28 Abs. 3 Satz 6 BDSG scheitert.

Bei Werbung mit einem Telefonanruf gegenüber einem **sonstigen Marktteilnehmer** (B2B) kommt es für die wettbewerbsrechtliche Zulässigkeit nach § 7 Abs. 2 Nr. 2 UWG darauf an, dass von dessen zumindest mutmaßlicher Einwilligung ausgegangen werden kann. Im B2B-Bereich stehen deshalb bei einem Hinzuspeichern und Nutzen von Telefonnummern für Werbeanrufe nach § 28 Abs. 3 Satz 3 BDSG i. V. m. § 28 Abs. 3 Satz 2 Nr. 1 BDSG (Eigenwerbung bei Bestandskunden oder Eigenwerbung bei Firmenkontakten aus allgemein zugänglichen Verzeichnissen) datenschutzrechtlich nicht von vorne herein die schutzwürdigen Interessen der telefonisch anzusprechenden Gewerbetreibenden nach § 28 Abs. 3 Satz 6 BDSG entgegen.

Siehe dazu ergänzend auch BGH, Urteil vom 16. November 2006, Az. I ZR 191/03, und BGH, Urteil vom 20. September 2007, Az. I ZR 88/05.

3.11 Transparenzregelungen nach § 28 Abs. 3 Satz 4 BDSG auch bei B2B- und Spendenwerbung

§ 28 Abs. 3 Satz 4 BDSG fordert bei der Übermittlung von Adressdaten für Werbezwecke uneingeschränkt Transparenz über die Herkunft der Daten, so dass auch bei B2B- und Spendenwerbung aus der Werbung die Stelle hervorgehen muss, die die Adressdaten erstmalig erhoben hat.
Nach § 28 Abs. 4 Satz 2 BDSG ist bei der Ansprache zum Zweck der Werbung über die (für die Daten) verantwortliche Stelle zu unterrichten.

Des Weiteren muss die (unmittelbare) Herkunft der Daten auch beim Werbenden (als Empfänger der Daten) nach § 34 Abs. 1a Satz 2 BDSG für zwei Jahre gespeichert und bei Nachfrage des Betroffenen beauskunftet werden.

3.12 Bezeichnung der Stelle, die die Daten erstmalig erhoben hat (§ 28 Abs. 3 Satz 4 BDSG) bzw. die für die Nutzung der Daten verantwortlich ist (§ 28 Abs. 3 Satz 5 BDSG)

Die verantwortliche Stelle ist als konkrete juristische Person bzw. Firma mit ladungsfähiger Anschrift zu nennen. Kurzbezeichnungen (wie XY-Group) oder Postfachanschriften genügen dem Gesetzeszweck nicht. Die Stelle muss aus der Werbung eindeutig hervorgehen bzw. die für die Nutzung der Daten verantwortliche Stelle muss eindeutig erkennbar sein.

3.13 Begrenzung auf die Listendaten auch bei § 28 Abs. 3 Satz 5 BDSG

Nach den Materialien zu den Gesetzesberatungen für die sog. BDSG-Novelle 2 aus dem Jahr 2009 (BTDrucks. 16/13657) ist eine sinngemäße und dem (mutmaßlichen) Willen des Gesetzgebers entsprechende Auslegung der Vorschrift in der Weise vorzunehmen, dass

auch bei § 28 Abs. 3 Satz 5 BDSG die Eingrenzung auf die Listendaten gilt.

3.14 Vertragliche Informationen, die gleichzeitig auch werbliche Informationen enthalten („Beipack-Werbung“)

Wenn Vertragspartnern vertragliche Informationen und damit verbunden auch eigene oder fremde werbliche Informationen per Brief zugesandt werden, ist dies in den Grenzen von § 28 Abs. 3 Satz 2, Satz 5 und Satz 6 BDSG möglich.

Bei E-Mail-Werbung sind über § 28 Abs. 3 Satz 6 BDSG die Wertungen in § 7 Abs. 3 UWG zu beachten, wonach für Fremdwerbung keine Erleichterungen gelten.

3.15 Gesetzestext von § 28 Abs. 3 Satz 6 BDSG

Hier liegt nach allgemeiner Meinung bei der Einbeziehung (nur) der Sätze 2 bis 4 von § 28 Abs. 3 BDSG ein Redaktionsversehen vor. Dieses beruht offensichtlich darauf, das kurz vor Abschluss des Gesetzgebungsverfahrens Anfang Juli 2009 in § 28 Abs. 3 BDSG ein weiterer Satz eingeschoben und dies bei der Bezugnahmeformulierung in Satz 6 nicht mehr berücksichtigt wurde. Richtig müsste es also in § 28 Abs. 3 Satz 6 BDSG lauten "nach den Sätzen 2 bis 5". In dieser Weise ist das Gesetz anzuwenden.

3.16 Werbung anhand von Dritten erlangten Adressdaten („Freundschaftswerbung“)

Für die teilweise noch in der Abonnentenwerbung sowie in der Finanzberatungs- und Versicherungsvertreterbranche anzutreffende Praxis, weitere Werbeadressdaten bei Kunden- und Interessentenbesuchen durch Befragen Dritter zu erheben und für Werbeansprachen zu speichern und zu nutzen, sehen die Aufsichtsbehörden im Anwendungsbereich des § 28 Abs. 1 bis Abs. 3 BDSG keine Rechtsgrundlage, denn § 28 Abs. 3 Satz 2 Nr. 1 BDSG erlaubt die Speicherung und Nutzung von Adressdaten zur Werbung für eigene Angebote nur bei einer Datenerhebung beim Betroffenen selbst oder aus allgemein zugänglichen Verzeichnissen. Darüber hinaus steht der in § 4 Abs. 2 Satz 1 BDSG normierte Direkterhebungsgrundsatz solchen Datenerhebungen bei Dritten entgegen.

4 Hinweise zu § 28 Abs. 3a BDSG

4.1 Andere Form der Einwilligung für Werbung

§ 28 Abs. 3a BDSG bezieht sich wegen der Zuordnung zu § 28 Abs. 3 BDSG nur auf Einwilligungen für einen werblichen Umgang mit personenbezogenen Daten und betrifft im ersten Teil von Satz 1 mündlich und fernmündlich erklärte Einwilligungen.

Visitenkarten, die auf Messen oder sonstigen Veranstaltungen ausdrücklich zur Informationszusendung und weiteren geschäftlichen Kontaktaufnahme hinterlassen werden, kön-

nen eine solche anderweitig erteilte Einwilligung darstellen.

4.2 Schriftliche Bestätigung der Einwilligung

Die Textform gemäß § 126b BGB (E-Mail, PDF-Dokument) kann als ausreichend im Sinne des Schutzzwecks von § 28 Abs. 3a Satz 1 BDSG für die schriftliche Bestätigung einer anderweitig erteilten Einwilligung angesehen werden. Die Schriftform mit eigenhändiger Unterschrift nach § 126 BGB ist nach dem Bestätigungs- bzw. Informationszweck der Vorschrift nicht geboten.

4.3 Zeitpunkt der schriftlichen Bestätigung der Einwilligung

Eine unverzügliche oder separate Bestätigung der nicht schriftlich erteilten Einwilligung fordert das Gesetz nicht. Die Bestätigung muss im unmittelbaren zeitlichen Zusammenhang zur Einwilligung erfolgen, wobei ein Zeitraum von bis zu drei Monaten noch als vertretbar angesehen wird.
Dabei ist auch die schriftliche Bestätigung der Einwilligung in Verbindung mit der ersten Werbezusendung möglich, wenn beide Bestandteile (Bestätigung der Einwilligung und Werbetext) klar getrennt sind und die Bestätigung der Einwilligung entsprechend deutlich herausgestellt wird.

4.4 Double-Opt-In-Verfahren für elektronische Einwilligungen

Für das elektronische Erklären einer Einwilligung ist – zur Verifizierung der Willenserklärung des Betroffenen – das Double-Opt-In-Verfahren geboten (je nach konkreter Art des Kontaktes: E-Mail oder SMS), wobei die Nachweis-Anforderungen des BGH (Urteil vom 10. Februar 2011, I ZR 164/09) bei der Protokollierung zu berücksichtigen sind. Das bloße Abspeichern der IP-Adressen von Anschlussinhabern und die Behauptung, dass von diesen eine Einwilligung vorliege, genügt dem BGH nicht. Der Nachweis der Einwilligung erfordert mehr, z. B. den Ausdruck einer E-Mail des Betroffenen mit der entsprechenden Willenserklärung.

Ein solcher Nachweis reicht jedoch nicht im Fall der vorgesehenen Nutzung von über Website-Eintragungen erlangten Telefonnummern für Werbeanrufe aus. Mit der Übersendung einer Bestätigungs-E-Mail kann nämlich der Nachweis der Identität zwischen dem die Einwilligung mittels E-Mail Erklärenden und dem Anschlussinhaber der Telefonnummer nicht geführt werden.

4.5 § 28 Abs. 3a Satz 2 BDSG, zusammengefasste Einwilligungen

Wegen der strengen Anforderungen von § 7 Abs. 2 UWG (vorherige ausdrückliche Einwilligung für Telefon-, Fax- und elektronische Werbung), die werbende Unternehmen bei ihren Werbeansprachen von Verbrauchern berücksichtigen müssen, schafft § 28 Abs. 3a Satz 2 BDSG faktisch nur für die Verwendung von Adressdaten zur Briefwerbung an Verbraucher die Möglichkeit des Zusammenfassens von datenschutzrechtlicher Einwilligung (mit besonderer Hervorhebung) und anderen Vertragserklärungen mit einer Unterschrift.

5 Hinweise zu § 28 Abs. 4 BDSG

5.1 Werbewiderspruch und Wunsch nach Datenlöschung

Für die Umsetzung der Betroffenenrechte ist im Zweifelsfall vom Betroffenen klarzustellen bzw. bei ihm zu klären, was er mit seiner Willenserklärung bewirken möchte. Möchte er vorrangig von einer werblichen Ansprache durch das Unternehmen verschont bleiben, ist dafür die Aufnahme seiner Kontaktdaten in die Werbesperrdatei bei diesem Unternehmen das richtige Mittel zur Berücksichtigung seines Willens. Bei der Nutzung von Fremddaten kann dann durch Abgleich mit der Werbesperrdatei sichergestellt werden, dass die Kontaktdaten dieses Betroffenen nicht verwendet werden. Solche Werbesperrdateien sind damit aufgrund von § 28 Abs. 1 Satz 1 Nr. 2 BDSG – zur Berücksichtigung der Werbewidersprüche von Betroffenen nach § 28 Abs. 4 BDSG – zulässig.

Betroffene rechnen häufig nicht damit, dass ihre Daten beim Werbetreibenden in eine Sperrdatei aufgenommen werden und sind nicht selten bereits aus prinzipiellen Erwägungen gegen jegliche weitere Datenspeicherung bei der verantwortlichen Stelle. Werden die Daten ohne ein ausdrückliches Einverständnis von den Betroffenen einzuholen auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG beim Werbetreibenden in eine Sperrdatei aufgenommen, müssen Betroffene hierüber unterrichtet werden, damit sie ggf. ein entgegenstehendes Interesse geltend machen können.

Zweckmäßiger Weise sollten die Betroffenen im Zusammenhang mit der Unterrichtung über die Beachtung ihres Werbewiderspruchs auch über den Sinn und Zweck der Aufnahme ihrer Daten in eine Sperrdatei unterrichtet werden.

Der Werbewiderspruch eines Betroffenen kann sich, je nach seiner Willenserklärung, datenschutzrechtlich gegen den Dateneigner als verantwortliche Stelle nach dem BDSG wie auch wettbewerbsrechtlich gegen den Werbenden (bei der Nutzung von Fremddaten) als für diese geschäftliche Handlung nach dem UWG Verantwortlichen richten (§ 7 Abs. 1 UWG). Beide müssen ggf. diesen Werbewiderspruch künftig berücksichtigen (durch Aufnahme in eine Werbesperrdatei).

Wünscht ein Betroffener ausdrücklich und allein eine Löschung aller Daten, sollte er darauf hingewiesen werden, dass er bei einem künftigen – rechtlich zulässigen – Einsatz von Fremddaten eventuell wieder Werbung erhalten kann.

Ergänzend kann ein Hinweis für die Betroffenen auf die sog. Robinsonlisten der Werbewirtschaft hilfreich sein, siehe z. B. unter www.ichhabediewahl.de oder www.robinsonliste.de.

5.2 Umsetzungsfrist des Widerspruchs nach § 28 Abs. 4 Satz 1 BDSG

Die Umsetzung des Widerspruchs gegen die künftige Verarbeitung oder Nutzung der Kontaktdaten eines Betroffenen für Werbung muss in dem betreffenden Unternehmen grundsätzlich unverzüglich erfolgen.

Wenn konkrete Werbeaktionen angelaufen sind und sich die Kontaktdaten des Betroffenen schon in der technischen Verarbeitung befinden, kann es im Einzelfall für das Unternehmen unzumutbar sein, einen zwischenzeitlich eingegangenen Werbewiderspruch noch mit erheblichem Aufwand umzusetzen, z. B. einen bestimmten bereits adressierten Brief aus einer großen Menge heraus zu sortieren.

Auch hier ist Betroffenen überwiegend nicht bewusst, dass bereits "angelaufene" Werbeaktionen regelmäßig nicht mehr gestoppt werden können. Zur Vermeidung von unnötigen Beschwerden sollten die Werbetreibenden die Betroffenen in einem individuellen Antwortschreiben erstens auf die Beachtung des Werbewiderspruchs und zweitens die Tatsache, dass sie über einen möglichst genau zu benennenden Zeitraum noch Werbung erhalten können, unterrichten.

5.3 Unterrichtung über das Widerspruchsrecht nach § 28 Abs. 4 Satz 2 BDSG

Es ist nur dann von einer wirksamen Unterrichtung im Sinne des Gesetzes auszugehen, wenn ein durchschnittlicher Verbraucher beim üblichen Umgang mit Werbung oder Vertragsinformationen von der Unterrichtung Kenntnis erlangt. Das "Verstecken" der Unterrichtung in langen AGBs oder in umfangreichen Werbematerialien stellt keine Unterrichtung im Sinne des Gesetzes dar.

Mit der Unterrichtung über die verantwortliche Stelle ist die für die Verwendung der Werbedaten verantwortliche Stelle (Dateneigner) gemeint.

Bei mehreren Werbeansprachen muss die Unterrichtung über das bestehende Werbewiderspruchsrecht in jedem Werbeschreiben erfolgen.