18. Wahlperiode

Drucksache **18/7202**

HESSISCHER LANDTAG

04. 04. 2013

Einundvierzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2012
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 4. April 2013 · Ausgegeben am 9. April 2013
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 41. Tätigkeitsbericht 9
Register der Rechtsvorschriften zum 41. Tätigkeitsbericht 17
Kernpunkte 21

1. Einführung 25
1.1 Allgemeines 25
1.2 Abschied vom deutschen Datenschutz? 25
1.3 Stellung des Hessischen Datenschutzbeauftragten und Aufgabenzuwachs 33
1.4 Arbeitsschwerpunkte und Statistik 39
1.5 Rechtsentwicklung 43

2. Übergreifende Themen (öffentlicher und nicht öffentlicher Bereich) 47
2.1 Querschnittsthemen 47
2.1.1 Geplante EU-Verordnung über elektronische Identifizierung und Vertrauensdienste 47
2.1.2 Dauerbrenner: Anforderung von Personalausweiskopien . . . 54

2.2 Fachthemen 58
2.2.1 Hessisches Spielhallengesetz 58
2.2.2 Die elektronische Gesundheitskarte mit Lichtbild wird eingeführt 61
2.2.3 Telefondatenüberwachung von Personal- oder Betriebsratsmitgliedern 67
2.2.4 Auskunftsanspruch des Kunden eines Gasanbieters 69
2.2.5 Auskunftsanspruch des (Mit-)Eigentümers über zu seiner Wohnung aufgenommene Daten 70

2.3 Entwicklungen und Empfehlungen im Bereich der Technik 71
2.3.1 Nutzung von Smartphones für dienstliche bzw. berufliche Zwecke 71
2.3.2 Orientierungshilfen Smart-Metering, IPv6 und Mandantenfähigkeit 72

3. Datenschutz im öffentlichen Bereich 75
3.1 Europa 75
3.1.1 Gemeinsame Kontrollinstanz für das Schengener Informationssystem 75
3.1.2 Gemeinsame Kontrollinstanz für Europol 78

3.2 Bund 81
3.2.1 Bundesmeldegesetz 81

3.3 Hessen 84
3.3.1 Querschnitt 84
3.3.1.1 Ein Rahmen zur Nutzung von facebook durch hessische Behörden 84

3.3.2 Justiz und Polizei 89
3.3.2.1 Prüfung des Einsatzes der Quellen-TKÜ 89
3.3.2.2 Recherche der Polizei in sozialen Netzen 98

3.3.3 Schulen, Schulverwaltung, Hochschulen, Archive 101
3.3.3.1 Gesetz zur Neuregelung des Archivwesens und des Pflichtexemplarrechts 101
3.3.3.2 Hessisches BAföG/AFBG-Verfahren 106
3.3.3.3 Videoüberwachung in Schulen 116
3.3.3.4 Einverständniserklärung zur Veröffentlichung von Schülerdaten im Internet 118

3.3.4 Statistik 121
3.3.4.1 Zensus 2011 – Abschluss der Erhebung und Erfassung der Daten 121

3.3.5 Sozialwesen 126
3.3.5.1 Mitwirkungspflichten bei der Beantragung von Sozialleistungen 126
3.3.5.2 Datenübermittlung des Jobcenters an die Ausländerbehörde bei SGB II-Anträgen durch europäische Unionsbürgerinnen und -bürger 132
3.3.5.3 Zugriffsberechtigungen auf EDV-Programme des Jobcenters 140

3.3.5.4 Informations- und Datenaustausch zwischen Kindergarten und Schule 142
3.3.5.5 Archivierung von Akten des Jugendamtes 144

3.3.6 Personalwesen 147
3.3.6.1 Löschen von Daten im SAP R/3 HR-System 147

3.3.7 Kommunale Selbstverwaltungskörperschaften 150
3.3.7.1 Änderung der Hessischen Gemeindeordnung 150
3.3.7.2 Datenschutzverstoß durch den Magistrat der Stadt Bad Homburg 153
3.3.7.3 Stadtverordnete fragen den Magistrat nach der Parteimitgliedschaft städtischen Führungspersonals 155
3.3.7.4 Falsche Angaben gegenüber dem Betroffenen und dem Hessischen Datenschutzbeauftragten widersprechen dem Transparenzgrundsatz 156
3.3.7.5 Personenbezogene Information über das Ergebnis eines gerichtlichen Musterverfahrens an die übrigen Widerspruchsführer 157
3.3.7.6 Bauschildinformationen im Internet 159

4. Aufsichtsbehörde nach § 38 BDSG 161
4.1 Der Hessische Datenschutzbeauftragte als Bußgeldbehörde 161
4.2 Videoüberwachung 169
4.3 Keine Bestätigung eines in den Medien behaupteten Missbrauchs der Videoanlage in einem Discountermarkt in Südhessen 176
4.4 Immer wieder „bcc“-Fehler beim Versenden von Massen-E-Mails 178
4.5 Zuständigkeit des betrieblichen DSB 179
4.6 Interessenkonflikt beim betrieblichen Datenschutzbeauftragten – „Inkompatibilität“ 180
4.7 Das unabdingbare Recht auf Auskunft über die eigenen Daten nach § 13 Abs. 7 TMG und § 34 Abs. 1 BDSG 182
4.8 Dauerwirkung von Interneteinträgen 186
4.9 Impressumspflicht bei Telemedien 187
4.10 Informationsaustausch zwischen bürgender Bank und Bürgschaftsgläubiger 189

4.11 Auskunfteien 190
4.12 Datenschutzgerechte Ausgestaltung von Arztbewertungsportalen 198
4.13 Bestellung von Datenschutzbeauftragten für Arztpraxen . . . 204
4.14 Hinweis- und Informationssystem der Versicherungswirtschaft 206
4.15 Löschung von Gesundheitsdaten bei Versicherungen 209
4.16 Datenübermittlung zwischen Versicherungen 211
4.17 Telefonische Spendenwerbung 212
4.18 Internetgestütztes Kampfrichter-Administrationssystem . . . 214

5. Bilanz 217
5.1 Elektronische Aufenthaltsüberwachung ehemaliger Straftäter 217
5.2 Visawarndatei und Abgleich am Visumsverfahren beteiligter Personen mit der Antiterrordatei 217

6. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 219
6.1 Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke . . 219
6.2 Ein hohes Datenschutzniveau für ganz Europa! 220
6.3 Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln 223
6.4 Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz 223
6.5 Patientenrechte müssen umfassend gestärkt werden 225
6.6 Orientierungshilfe zum datenschutzgerechten Smart Metering 226
6.7 Melderecht datenschutzkonform gestalten! 227
6.8 Europäische Datenschutzreform konstruktiv und zügig voranbringen! 229
6.9 Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben 230
6.10 Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten 231

6.11 Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller 233

7. Beschlüsse des Düsseldorfer Kreises 235
7.1 Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft 235
7.2 Nearfield Communication (NFC) bei Geldkarten 247

8. Materialien 249
8.1 Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutz-Grundverordnung 249
8.2 Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur 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 274
8.3 Kurzfassung der Stellungnahme des Hessischen Datenschutzbeauftragten zum „Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“, COM (2012) 238 final 285
8.4 Stellungnahme des Hessischen Datenschutzbeauftragten zum „Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“, COM(2012) 238 final 287

Organisationsplan des Hessischen Datenschutzbeauftragten . . . 299
Sachwortverzeichnis zum 41. Tätigkeitsbericht 305

Abkürzungsverzeichnis zum 41. Tätigkeitsbericht

ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AES	Advanced encryption standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a. F.	alte Fassung
Art.	Artikel
AufenthG	Gesetz über den Aufenthalt, die Erwerbtätigkeit und die Integration von Ausländern im Bundesgebiet
AuslR	Ausländerrecht
Az.	Aktenzeichen
BAföG	Bundesgesetzes über individuelle Förderung der Ausbildung – Bundesausbildungsförderungsgesetz
Bcc	Blind carbon copy
bDSB	betrieblicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BRDrucks.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BTDrucks.	Bundestagsdrucksache
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
bzw.	beziehungsweise
ca.	zirka
cc	carbon copy

CD	Compact Disc
CDU	Christlich Demokratische Union Deutschlands
d. h.	das heißt
ders.	derselbe
DIJuF	Deutsche Institut für Jugendhilfe und Familienrecht e. V.
DMZ	demilitarisierte Zone
DÖV	Die öffentliche Verwaltung
Drucks.	Drucksache
DuD	Zeitschrift Datenschutz und Datensicherheit
DV	Datenverarbeitung
DVBl	Deutsches Verwaltungsblatt
EAW	engl.: European Arrest Warrant (europäischer Haftbefehl)
EC	engl.: electronic cash
EFA	Europäischen Fürsorgeabkommen
eGK	elektronische Gesundheitskarte
eID	elektronische Identifizierung
eID-System	elektronisches Identifizierungssystem
EMRK	Europäische Menschenrechtskonvention
Erg.Lfg.	Ergänzungslieferung
Erster GlüÄndStV	Erster Glückspieländerungsstaatsvertrag
eSignaturen	Elektronische Signaturen
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte-Zeitschrift
EUR	Euro
Eurodac	europäisches Fingerabdrucksystem
Europol	europäisches Polizeiamt
EUV	Vertrag über die Europäische Union
EUVO eIAS	Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
e. V.	eingetragener Verein
Fa.	Firma
FAZ	Frankfurter Allgemeine Zeitung

FDP	Freie Demokratische Partei Deutschlands
FES	Fortgeschrittene elektronische Signatur
ff.	fortfolgende/r/s
ForstG	Forstgesetz
FreizügG/EU	Gesetz über die allgemeine Freizügigkeit von Unionsbürgern/Freizügigkeitsgesetz/EU
FStrG	Bundesfernstraßengesetz
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e. V.
gem.	gemäß
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz für das Schengener Informationssystem
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GPS	Global Positioning System, globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung
GÜL	Gemeinsame Überwachungsstelle der Länder (für die elektronische Aufenthaltsüberwachung)
GVBl.	Gesetz- und Verordnungsblatt des Landes Hessen
GVE	Entwurf der EU-Kommission für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr – Datenschutz-Grundverordnung
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz)
HBG	Hessisches Beamtengesetz
HBO	Hessische Bauordnung
HDSG	Hessisches Datenschutzgesetz
HeBaV	Hessisches BAFöG/AFBG-Verfahren
Hess. Verf.	Hessische Verfassung
HessVGH	Hessischer Verwaltungsgerichtshof
HGB	Handelsgesetzbuch
HGO	Hessische Gemeindeordnung

HArchivG	Hessisches Archivgesetz
HIS	Hinweis- und Informationssystem
HLT	Hessischer Landtag
HMDIS	Hessisches Ministerium des Innern und für Sport
HMG	Hessisches Meldegesetz
HMUELV	Hessisches Ministerium für Umwelt, Energie, Landwirtschaft und Verbraucherschutz
HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HPVG	Hessisches Personalvertretungsgesetz
Hrsg.	Herausgeber
HSchG	Hessisches Schulgesetz
HSL	Hessisches Statistisches Landesamt
HSM	Hessisches Sozialministerium
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HUIG	Hessisches Umweltinformationsgesetz
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. d. F.	in der Fassung
i-frames	inlineframes
IP	Internet Protokoll, Netzwerkprotokoll im Internet (engl. Internet protocol)
IPsec	Internet Protokoll security
IPv6	Internet Protokoll Version 6
i. S. v.	im Sinne von
IT	Informationstechnik
i. V. m.	in Verbindung mit
KOM	Europäische Kommission
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
lit.	Buchstabe
LKA	Landeskriminalamt
LTDrucks.	Landtagsdrucksache
MittRA	Mitteilung des Rechtsausschusses des Europäischen Parlaments an die Mitglieder
MMR	Zeitschrift „MultiMedia und Recht“

NGOs	non governmental organisations
NJW	Neue Juristische Wochenschrift
nPA	neuer Personalausweis
Nr.	Nummer
Nrn.	Nummern
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht – Rechtsprechungsreport
NZA	Neue Zeitschrift für Arbeitsrecht
o. Ä.	oder Ähnliche/r/s
o. g.	oben genannte/r/s
OLG	Oberlandesgericht
OSCI	Online Services Computer Interface
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PC	Personalcomputer
PDA	Personal Digital Assistant
PIN	engl.: personal identification number (persönliche Geheimzahl)
PlPr	Plenarprotokoll
PrOVG	Preußisches Oberverwaltungsgericht
QES	Qualifizierte elektronische Signatur
Rdnr.	Randnummer
RGBl.	Reichsgesetzblatt
RiStBV	Richtlinien für das Strafverfahren und Bußgeldverfahren
RL 95/46/EG	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Okt. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
RLE	Entwurf der EU Kommission 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

RSA	Asymmetrisches kryptographisches Verschlüsselungsverfahren – Rivest, Shamir, Adlemann –
RStV	Rundfunkstaatsvertrag
RZ	Rechenzentrum
S.	Seite
s.	siehe
SAP R/3 HR	in der Hessischen Landesverwaltung eingesetztes DV-System zur Personaldatenverarbeitung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SIM	subscriber identity module für „Teilnehmer-Identitätsmodul“
SIRENE	Supplementary Information Request at the National Entry (Kontrollstelle beim Bundeskriminalamt für das Schengener Informationssystem)
SIS II	Schengener Informationssystem der zweiten Generation
sog.	sogenannte
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SWIFT	Society for Worldwide Interbank Financial Telecommunication (Internationale Genossenschaft der Geldinstitute)
SZ	Süddeutsche Zeitung
TCP/IP	Transmission Control Protocol (aufgesetzt auf dem) Internet Protokoll
TFTP	Terrorist Finance Tracking Program (Programm zum Aufspüren von Terrorfinanzierungen)
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
u. a.	unter anderem
u. Ä.	und Ähnliche/r/s
u. U.	unter Umständen

USB	Universal Serial Bus
VerwArch	Verwaltungsarchiv
VG	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung
VPN	virtuale private network
VVG	Versicherungsvertragsgesetz
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
VwVG	Verwaltungsvollstreckungsgesetz
WEG	Gesetz über das Wohnungseigentum und das Dauerwohnrecht
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
Ziff.	Ziffer
ZUM-RD	Zeitschrift für Urheber- und Medienrecht – Rechtsprechungsdienst

Register der Rechtsvorschriften

AEUV	Vertrag über die Arbeitsweise der Europäischen Union i. d. F. vom 9. Mai 2008 (ABl. EU C 115 S. 47)
AO	Abgabenordnung i. d. F. vom 1. Okt. 2002 (BGBl. I S. 3866, 2003 S. 61), zuletzt geändert durch Gesetz vom 21. Juli 2012 (BGBl. I S. 1566)
AufenthG	Aufenthaltsgesetz i d. F. vom 25. Febr. 2008 (BGBl. I S. 162), zuletzt geändert durch Gesetz vom 15. Feb. 2013 (BGBl. I S. 254)
BAföG	Bundesausbildungsförderungsgesetz vom 7. Dez. 2010 (BGBl. I S. 1952), zuletzt geändert durch Gesetz vom 20. Dez. 2011 (BGBl. I S. 2854)
BArchG	Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz) vom 6. Jan. 1988 (BGBl. I S. 62), zuletzt geändert durch Gesetzes vom 5. Sept. 2005 (BGBl. I S. 2722)
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)
BetrVG	Betriebsverfassungsgesetz i. d. F. vom 25. Sept. 2001 (BGBl. I S. 2518), zuletzt geändert durch Gesetz vom 29. Juli 2009 (BGBl. I S. 2424)
BGB	Bürgerliches Gesetzbuch i. d. F. der Bekanntmachung vom 2. Jan. 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Gesetz vom 20. Dez. 2012 (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)
Erster GlüÄndStV	Erster Glücksspieländerungsstaatsvertrag vom 15. Dez. 2011 (GVBl. 2012 S. 190)
EStG	Einkommenssteuergesetz i. d. F. vom 8. Okt. 2009 (BGBl. I S. 3366, 3862), zuletzt geändert durch Gesetz vom 8. Mai 2012 (BGBl. I S. 1030)
EU-Signaturrichtlinie	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dez. 1999 (ABl. EG S. 12–20)
Europol-Beschluss	Beschluss des Rates Nr. 2009/371 vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (ABl. EU Nr. L 121/37)
EUV	Vertrag über die Europäische Union i. d. F. des Vertrages von Lissabon vom 13. Dez. 2007 (ABl. EU Nr. C 306 S. 1, ber. ABl. 2008 Nr. C 111 S. 56 und ABl. 2009 Nr. C 290 S. 1)
ForstG	Hessisches Forstgesetz i. d. F. vom 10. Sept. 2002 (GVBl. I S. 582)

GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Gesetz vom 11. Juli 2012 (BGBl. I S. 1478)
GKV-Modernisierungsgesetz	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung vom 14. Nov. 2003 (BGBl. I S. 2190), zuletzt geändert durch Gesetz vom 15. Dez. 2004 (BGBl. I S. 3445)
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) i. d. F. vom 13. Aug. 2008 (BGBl. I S. 1690), zuletzt geändert durch Gesetz vom 22. Dez. 2012 (BGBl. I S. 2959)
HArchivG	Hessisches Archivgesetz vom 18. Okt. 1989 (GVBl. I S. 270), zuletzt geändert durch Gesetz vom 26. Nov. 2012 (GVBl. I S. 458)
HBG	Hessisches Beamtengesetz i. d. F. vom 11. Jan. 1989 (GVBl. I S. 26), zuletzt geändert durch Gesetz vom 13. Dez. 2012 (GVBl. I S. 622)
HBO	Hessische Bauordnung i. d. F. vom 15. Jan. 2011 (GVBl. I S. 46), zuletzt geändert durch Gesetz vom 13. Dez. 2012 (GVBl. I S. 622)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 7. Jan. 1999 (GVBl. I S. 98)
HGB	Handelsgesetzbuch vom 10. Mai 1897 (RGBl. S. 219), zuletzt geändert durch Gesetz vom 20. Dez. 2012 (BGBl. I S. 2751)
HGO	Hessische Gemeindeordnung i. d. F. vom 7. März 2005 (GVBl. I S. 142), zuletzt geändert durch Gesetz vom 16. Dez. 2011 (GVBl. I S. 786)
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)
HPresseG	Hessisches Gesetz über Freiheit und Recht der Presse i. d. F. vom 12. Dez. 2003 (GVBl. 2004 I S. 2), zuletzt geändert durch Gesetz vom 13. Dez. 2012 (GVBl. I S. 622)
HPVG	Hessisches Personalvertretungsgesetz vom 24. März 1988, zuletzt geändert durch Gesetz vom 13. Dez. 2012 (GVBl. I S. 622)
Hessisches Spielhallengesetz	vom 28. Juni 2012 (GVBl. I S. 213)
HSchG	Hessisches Schulgesetz i. d. F. vom 14. Juni 2005 (GVBl. I S. 441), zuletzt geändert durch Gesetz vom 18. Dez. 2012 (GVBl. I S. 645)
HUIG	Hessisches Umweltinformationsgesetz vom 14. Dez. 2006 (GVBl. I S. 659), zuletzt geändert durch Gesetz vom 13. Dez. 2012 (GVBl. I S. 622)

HVwVfG	Hessisches Verwaltungsverfahrensgesetz i. d. F. vom 15. Jan. 2010 (GVBl. I S. 623)
KVRvaÄndG	Gesetz zur Änderung krankenversicherungsrechtlicher und anderer Vorschriften vom 24. Juli 2010 (BGBl. I S. 983)
OwiG	Gesetz über Ordnungswidrigkeiten i. d. F. vom 19. Feb. 1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 29. Juli 2009 (BGBl. I S. 2353)
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) i. d. F. vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 2959)
RStV	Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag) i. d. F. des 15. Rundfunkänderungsstaatsvertrags, in Kraft getreten am 1. Jan. 2013 (Art. 1 Gesetz zu dem Fünfzehnten Rundfunkänderungsstaatsvertrag vom 23. Aug. 2011 (GVBl. I S. 382))
SDÜ	Schengener Durchführungsübereinkommen vom 14. Juni 1985 (BGBl. 1993 II S. 1010), zuletzt geändert durch Verordnung Nr. 265/2010 (ABl. EU Nr. L 85 S. 1)
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – i. d. F. vom 11. Dez. 1975 (BGBl. I S. 3015), zuletzt geändert durch Gesetz vom 12. Apr. 2012 (BGBl. I S. 579)
SGB II	Zweites Buch Sozialgesetzbuch – Grundsicherung für Arbeitssuchende – i. d. F. vom 13. Mai 2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Gesetz vom 20. Dez. 2012 (BGBl. I S. 2781)
SGB V	Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – i. d. F. vom 20. Dez. 1988 (BGBl. I S. 2477), zuletzt geändert durch Gesetz vom 20. Feb. 2013 (BGBl. I S. 277)
SGB VIII	Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe – i. d. F. vom 14. Dez. 2006 (BGBl. I S. 3134), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 2975)
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – i. d. F. vom 18. Jan. 2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 21. Juli 2012 (BGBl. I S. 1566)
SGB XII	Zwölftes Buch Sozialgesetzbuch – Sozialhilfe – i. d. F. vom 27. Dez. 2003 (BGBl. I S. 3022), zuletzt geändert durch Gesetz vom 20. Dez. 2012 (BGBl. I S. 2789)
StPO	Strafprozessordnung i. d. F. vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 21. Jan. 2013 (BGBl. I S. 89)

SWIFT-Abkommen	Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP-Abkommen, ABl L 195 vom 27. Juli 2010, S. 3)
TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 3. Mai 2012 (BGBl. I S. 958)
TMG	Telemediengesetz vom 26. Feb. 2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 31. Mai 2010 (BGBl. I S. 692)
TPGEntLÄndG)	Gesetz zur Regelung der Entscheidungslösung im Transplantationsgesetz vom 12. Juli 2012 (BGBl. I S. 1504)
UWG	Gesetz gegen den unlauteren Wettbewerb vom 3. Juli 2004 (BGBl. I S. 1414) i. d. F. der Bekanntmachung vom 3. März 2010 (BGBl. I S. 254)
VVG	Gesetz über den Versicherungsvertrag (Versicherungsvertragsgesetz) vom 23. Nov. 2007 (BGBl. I S. 2631), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 3044)
VwGO	Verwaltungsgerichtsordnung i. d. F. vom 19. März 1991 (BGBl. I S. 686), zuletzt geändert durch Gesetz vom 21. Juli 2012 (BGBl. I S. 1577)
WEG	Gesetz über das Wohnungseigentum und das Dauerwohnrecht vom 15. März 1951 (BGBl. I S. 175), zuletzt geändert durch Gesetz vom 10. Mai 2012 (BGBl. I S. 1084)

Kernpunkte

1. Mit Rücksicht auf die Globalisierung des automatisierten Informationsaustauschs muss das Datenschutzrecht der EU modernisiert werden. Der Ansatz des 2012 vorgelegten Reformpakets der Kommission, das Datenschutzniveau auf gesamteuropäischer Ebene anzuheben, ist auch durchaus begrüßenswert. Nicht akzeptabel sind die mit dem Vorhaben verbundenen Kompetenzüberschreitungen, die mit den gewachsenen Strukturen des Deutschen Datenschutzes unvereinbar sind und deren systemimmanente Fortentwicklung unmöglich machen (Ziff. 1.2).

2. Die Zusammenlegung des privaten und öffentlichen Bereichs beim Hessischen Datenschutzbeauftragten macht diesen definitiv zu einer obersten Landesbehörde im organisatorischen und funktionellen Sinn. Dies erforderte eine neue Organisationsstruktur, die ab Januar 2012 zur Verfügung stand (Ziff. 1.3).

3. Im IT-Bereich habe ich mich mit den Stärken und Schwächen der geplanten EU-Verordnung über elektronische Identifizierung und Vertrauensdienste auseinandergesetzt und Verbesserungsvorschläge unterbreitet (Ziff. 2.1.1). Außerdem habe ich mich an der Erarbeitung einiger neuer Orientierungshilfen zu den Themen IPv6, Smart-Metering und Mandantenfähigkeit beteiligt (Ziff. 2.3.2).

4. In verschiedenen Zusammenhängen wird zur Identitätsfeststellung nicht nur die Vorlage des Personalausweises verlangt, sondern dieser auch kopiert. Sofern dies nicht spezialgesetzlich vorgeschrieben ist, bestehen dagegen sicherheits- und datenschutzrechtliche Bedenken. Deshalb hat das Bundesministerium des Innern Rahmenbedingungen formuliert, die hinsichtlich solcher Ausweiskopien zu prüfen und einzuhalten sind. In meinem Tätigkeitsbericht habe ich Grundlagen und Einzelfälle erläutert (Ziff. 2.1.2).

5. Das Hessische Spielhallengesetz berücksichtigt nur einen Teil der Einwände, die ich im Gesetzgebungsverfahren geäußert habe. Insbesondere im System der Spielersperren sind Nachbesserungen erforderlich, die wenigstens in der noch ausstehenden Rechtsverordnung zum Spielhallengesetz erfolgen müssen (Ziff. 2.2.1).

6. Immer wieder sind mangelhafte Auskünfte Grund für Bürgerbeschwerden. Das Auskunftsrecht gehört zu den unabdingbaren Rechten der Betroffenen und Transparenz ist ein tragender Gesichtspunkt des Datenschutzrechts, aber auch anderer Regelungen wie der Impressumspflicht (Ziff. 2.2.4, 2.2.5, 3.3.7.4, 4.7 und 4.9).

7. Soziale Netzwerke werfen vielerlei datenschutzrechtliche Fragestellungen auf, sind aus der modernen Welt aber nicht mehr wegzudenken. In meinem Tätigkeitsbericht habe ich eine Möglichkeit vorgestellt, wie die öffentliche Verwaltung in Hessen nur in facebook aktive Bürger erreichen kann, ohne gegen Datenschutzprinzipien zu verstoßen (Ziff. 3.3.1.1). Eine andere Facette beleuchtet die Grenzen der Zulässigkeit der polizeilichen Recherche in sozialen Netzen (Ziff. 3.3.2.2).

8. Mit Befremden habe ich feststellen müssen, dass der Hessische Landtag in letzter Minute einer aufgrund meiner Beratung entstandene datenschutzrechtlich ausgewogene Regelung durch Weglassen einer Passage den Boden entzogen hat. Nach dem neuen Archivgesetz sollen nunmehr auch rechtswidrig erhobene Daten archiviert werden (Ziff. 3.3.3.1).

9. Die zunehmende Videoüberwachung ist häufig Grund für Beratungsanfragen und Bürgerbeschwerden. Mein Bericht greift Fälle aus dem öffentlichen wie dem nicht öffentlichen Bereich auf (Ziff. 3.3.3.3 und 4.2).

10. Im Fokus von Eltern steht häufig die datenschutzrechtliche Zulässigkeit der Erhebung und Verarbeitung von Daten in Betreuungs- und Bildungseinrichtungen. Über die zulässigen Übermittlungen, aber auch die Frage der Notwendigkeit einer Einwilligung der Erziehungsberechtigten beim Informations- und Datenaustausch zwischen Kindergarten und Schule berichte ich in einem Beitrag (Ziff. 3.3.5.2). Ein anderer Beitrag geht der Frage der datenschutzrechtlichen Rahmenbedingungen für die Veröffentlichung von Schülerdaten im Internet nach (Ziff. 3.3.3.4).

11. Das inzwischen zur Verfügung gestellte Programm zur Löschung von urlaubs- und krankheitsbedingten Abwesenheiten bei der in der Landesverwaltung einheitlich eingesetzten Software SAP R/3 HR wird immer noch von vielen Behörden nicht oder nicht zeitnah eingesetzt. Eine Begründung für die Nichtlöschung der Daten wurde mir gegenüber nicht abgegeben (Ziff. 3.3.6.1).

12. Der Magistrat der Stadt Bad Homburg hat in einer Pressemitteilung über den Ausgang einer Dienstaufsichtsbeschwerde berichtet und dabei den vollen Namen des Beschwerdeführers genannt. Er berief sich darauf, dass der Betroffene eine Person des öffentlichen Lebens sei, weil er früher kommunalpolitisch tätig war. Eine kurze kommunalpolitische Tätigkeit entfaltet aber keine derartige Wirkung für die Zukunft, dass sie noch nach 14 Jahren die Annahme begründen könnte, der Bürger sei eine Person der Zeitgeschichte (Ziff. 3.3.7.2).

13. Zu den Arztbewertungsportalen gehört auch das in meine Zuständigkeit fallende Portal www.sanego.de. Mit den für andere Arztbewertungsportale zuständigen Aufsichtsbehörden habe ich mich auf eine gemeinsame Vorgehensweise zur Klärung und Bewertung der von den Portalen getroffenen Maßnahmen zur Gewährleistung des Persönlichkeitsschutzes von Ärzten verständigt (Ziff. 4.12).

1. Einführung

1.1
Allgemeines

Der Datenschutz befindet sich mehr denn je im Umbruch. War der 40. Tätigkeitsbericht von der Zusammenlegung von privatem und öffentlichem Bereich geprägt, so deutet sich nunmehr eine weitreichende Europäisierung des Datenschutzrechts an. Es soll gar nicht in Abrede gestellt werden, dass die deutschen Datenschutzbeauftragten ihre völlige Unabhängigkeit auch im privaten Bereich den europäischen Instanzen verdanken. Aber das kann nicht bedeuten, dass diese Unabhängigkeit unionsrechtlich wieder abgeschafft wird. Dies ist jedoch die Konsequenz des Reformpakets der Kommission, über das einleitend im vorliegenden 41. Tätigkeitsbericht informiert werden soll (Ziff. 1.2). Die Zusammenlegung von privatem und öffentlichem Bereich beim Hessischen Datenschutzbeauftragten war im Übrigen nicht die Erfüllung eines fachimperialistischen Wunschtraums, sondern die Auferlegung einer – wenn auch gerne übernommenen – Verpflichtung und Last, die an die Dienststelle vor allem in der Übergangsphase hohe Anforderungen stellte. Auch hierüber wird im Einleitungsteil näher berichtet (Ziff. 1.4). Das Ausmaß des Umbruchs wird freilich erst deutlich, wenn Klarheit über die Aufgabenstellung und Befugnisse des Hessischen Datenschutzbeauftragten besteht. Hierzu finden sich für den Berichtszeitraum erläuternde Anmerkungen (Ziff. 1.3). Dabei kann es sich nur um eine Momentaufnahme handeln. Die Dynamik des Datenschutzrechts wird an ausgewählten Beispielen aus der Rechtsprechung und dem Schrifttum aufgezeigt (Ziff. 1.5).

1.2
Abschied vom deutschen Datenschutz?

1.2.1
Europäisierung des Datenschutzrechts

Der automatisierte Informationsaustausch erfolgt zunehmend global. Geboten ist daher ein transnationaler, jedenfalls europäischer Datenschutz. Der Datenschutz ist in erster Linie eine Aufgabe der rechtlichen Ordnung. Das europäische Datenschutzrecht ist jüngeren Datums und konnte sich auf deutsche Vorbilder stützen. Auf Unionsebene ließ die RL 95/46 EG genügend Spielräume für die mitgliedstaatlichen Gesetzgeber, so dass sich vor allem in Deutschland ein zeitgemäßes Datenschutzrecht weiterentwickeln konnte. Das Datenschutzrecht der EU muss gleichwohl modernisiert werden. Auf Ersuchen des Rats ergriff die Kommission die Initiative zu einer

grundlegenden Novellierung des Datenschutzrechts. Seit 2009 fanden öffentliche Anhörungen zum Datenschutz statt. Am 4. November 2010 veröffentlichte die Kommission die Mitteilung über ein Gesamtkonzept für den Datenschutz in der EU (KOM[2010]609). Es folgte eine intensive Diskussion, bei der die Frage der Vereinbarkeit der vorgesehenen Regelungen mit dem Europäischen Vertragsrecht und dem Verfassungsrecht der Mitgliedstaaten weitgehend ausgeblendet blieb. So kam es zu den Vorschlägen vom 25. Januar 2012 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]11 endg.; hier abgekürzt: RLE). Die Gesamtkonzeption ist erläutert in der Mitteilung „Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert" (KOM[2012]9 endg.). Das Reformpaket findet seine Legitimation in dem Anliegen, das Datenschutzrecht zu modernisieren. Für den „zukunftsfesten" Datenschutz werden fünf Eckpunkte vorgebracht: Das Recht auf Vergessenwerden, Transparenz, Datenschutz durch Gestaltung, Verantwortung für den Umgang mit personenbezogenen Daten und eine unabhängige Datenschutzkontrolle (vgl. Viviane Reding, Herausforderungen an den Datenschutz bis 2020: Eine europäische Perspektive, ZD 2011, 1 ff.). Das Reformpaket stieß auf Zustimmung und Kritik (vgl. Masing, SZ 9.1.2012, S. 10; ders., Herausforderungen des Datenschutzes, NJW 2012, 2305 ff.; Hirsch, SZ 8. Februar 2012; Bauer/von Steinrück, FAZ 27/1. Februar 2012, S. 19; Anger, Handelsblatt 24. Januar 2012; Opinion of the European Data Protection Supervisor on the data protection reformpackage, 7. März 2012; Stellungnahme des BvD vom 13. Dezember 2011, in BVD-News 1/2012, S. 12 ff.; Stellungnahme der Deutschen Gesellschaft für Recht und Informatik e. V. (DGRI) vom 21. Dezember 2011; Presseerklärung Bundesverband Verbraucherzentrale vom 25. Januar 2012; BITKOM, Stellungnahme vom 18. Mai 2012; Stellungnahme der deutschen Kreditwirtschaft vom 18. Mai 2012; Abel, Europäische Datenschutz-Verordnung – ein „Super-BDSG" für den Kontinent?, Datenschutz-Berater 1/2012, 8; Jan-Philipp Albrecht, Datenschutz mit Biss, AnwBl 2012, 348; Hanschmann, Das Verschwinden des Grundrechts auf Datenschutz, EuGRZ 2011, 219 ff.; Kotzur, Datenschutz in der europäischen Grundrechtsgemeinschaft, EuGRZ 2011, 105 ff.; Hornung, Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25. Januar 2012, ZD 2012, 99 ff.;

Hülsmann, Der betriebliche und behördliche Datenschutzbeauftragte im Entwurf der EU-Datenschutz-Grundverordnung, Datenschutz Nachrichten Nr. 1, 2012, S. 7 ff.; Ronellenfitsch, Fortentwicklung des Datenschutzes, DuD 2012, 652 ff.; ders., Europäisierung des Datenschutzes bei der Bahn, DVBl 2012, 1521 ff.; Schneider/Härting, Wird der Datenschutz nun endlich internettauglich? – Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht, ZD 2012, 199 ff.; Spary, Die neue Datenschutz-Grundverordnung – Überblick und Problemaufriss, Datenschutz Nachrichten Nr. 1, 2012, S. 4 ff.). Der Bundesrat erhob am 30. März 2012 die Subsidiaritätsrüge (BRDrucks. 52/12) – hierüber Mitteilung des Rechtsausschusses des Europäischen Parlaments an die Mitglieder – MittRA [0046/2012]). Ebenfalls die Subsidiaritätsrüge machten geltend der schwedische Reichstag, MittRA (0042/2012), die Abgeordnetenkammer der Republik Italien, MittRA (0045/2012) und die belgische Abgeordnetenkammer, MittRA (0041/2012). Gegenwärtig befindet sich der Kommissionsentwurf in der parlamentarischen Beratung. Die Stellungnahme des Rechtsausschusses für den federführenden Ausschuss für bürgerliche Freiheiten, Justiz und Inneres zu einem Gesamtkonzept für den Datenschutz in der Europäischen Union (2011/2025(INI)) vom 25. Mai 2012 geht auf die kompetenzrechtliche Thematik nicht näher ein. Der Ausschuss bürgerliche Freiheiten, Justiz und Inneres (LIBE) hat den GVE im Juli 2012 beraten. In dem Beratungsbericht (Working document vom 6. Juli 2012 – DT\905569EN.doc.) werden die Harmonisierungsbemühungen grundsätzlich begrüßt. Weiterer Diskussionsbedarf wird aber vor allem in den folgenden Bereichen gesehen: Rolle der Kommission, Erstreckung der Regelung auf EU-Organe, Begriffsklärungen. Diese Anregungen flossen ein in die Ergänzungsvorschläge des Rechtsausschusses vom 29. November 2012 (Amendments 72 – 451, 2012/0011[COD]).

1.2.2
Kritik

Zur Würdigung des Reformpakets ist zunächst auf die von mir mitgetragenen Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21./22. März 2012 und vom 7./8. November 2012 (vgl. unten Ziff. 6.2 und 6.8) und auf die Stellungnahmen der Konferenz vom 11. Juni 2012 zur Datenschutz-Grundverordnung (vgl. unten Ziff. 8.1) und zur Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (vgl. unten Ziff. 8.2) hinzuweisen. Nachfolgend soll auf einige rechtliche Kritikpunkte am Reformpaket besonders aufmerksam gemacht werden, die ich in einer Stel-

lungnahme vor dem Unterausschuss Datenschutz des Hessischen Landtags am 13. März 2012 bereits dargelegt habe.

Bei aller Anerkennung der mit dem Reformpaket angestrebten Anhebung des europäischen Datenschutzniveaus sollte Konsens bestehen, dass auch im Datenschutzrecht die europäischen Kompetenzgrenzen strikt zu beachten sind. Insofern bestehen gegen den Kommissionsentwurf jedoch Bedenken.

Bedenken bestehen erstens im Hinblick auf den Grundsatz der begrenzten Einzelermächtigung. Nach Art. 4 Abs. 1 EUV verbleiben alle der EU nicht in den Verträgen ausdrücklich übertragenen Zuständigkeiten bei den Mitgliedstaaten. Daraus folgt zwingend der erwähnte Grundsatz der begrenzten Einzelermächtigung, der in Art. 5 Abs. 1 EUV verankert ist. Eine Ausweitung der EU-Kompetenzen ist – vom Sonderfall der Abrundungskompetenz abgesehen – nach Art. 352 AEUV nicht möglich.

Art. 4 EUV

(1) Alle der Union nicht in den Verträgen übertragenen Zuständigkeiten verbleiben gemäß Artikel 5 bei den Mitgliedstaaten.

Art. 5 EUV

(1) Für die Abgrenzung der Zuständigkeiten der Union gilt der Grundsatz der begrenzten Einzelermächtigung. Für die Ausübung der Zuständigkeiten der Union gelten die Grundsätze der Subsidiarität und der Verhältnismäßigkeit.

(2) Nach dem Grundsatz der begrenzten Einzelermächtigung wird die Union nur innerhalb der Grenzen der Zuständigkeiten tätig, die die Mitgliedstaaten ihr in den Verträgen zur Verwirklichung der darin niedergelegten Ziele übertragen haben. Alle der Union nicht in den Verträgen übertragenen Zuständigkeiten verbleiben bei den Mitgliedstaaten.

(3) Nach dem Subsidiaritätsprinzip wird die Union in den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten weder auf zentraler noch auf regionaler oder lokaler Ebene ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind.

Die Organe der Union wenden das Subsidiaritätsprinzip nach dem Protokoll über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit an. Die nationalen Parlamente achten auf die Einhaltung des Subsidiaritätsprinzips nach dem in jenem Protokoll vorgesehenen Verfahren.

(4) Nach dem Grundsatz der Verhältnismäßigkeit gehen die Maßnahmen der Union inhaltlich wie formal nicht über das zur Erreichung der Ziele der Verträge erforderliche Maß hinaus.

Die Organe der Union wenden den Grundsatz der Verhältnismäßigkeit nach dem Protokoll über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit an.

Art. 352 AEUV

(1) Erscheint ein Tätigwerden der Union im Rahmen der in den Verträgen festgelegten Politikbereiche erforderlich, um eines der Ziele der Verträge zu verwirklichen, und sind in den

Verträgen die hierfür erforderlichen Befugnisse nicht vorgesehen, so erlässt der Rat einstimmig auf Vorschlag der Kommission und nach Zustimmung des Europäischen Parlaments die geeigneten Vorschriften. Werden diese Vorschriften vom Rat gemäß einem besonderen Gesetzgebungsverfahren erlassen, so beschließt er ebenfalls einstimmig auf Vorschlag der Kommission und nach Zustimmung des Europäischen Parlaments.

(2) Die Kommission macht die nationalen Parlamente im Rahmen des Verfahrens zur Kontrolle der Einhaltung des Subsidiaritätsprinzips nach Artikel 5 Absatz 3 des Vertrags über die Europäische Union auf die Vorschläge aufmerksam, die sich auf diesen Artikel stützen.

(3) Die auf diesem Artikel beruhenden Maßnahmen dürfen keine Harmonisierung der Rechtsvorschriften der Mitgliedstaaten in den Fällen beinhalten, in denen die Verträge eine solche Harmonisierung ausschließen.

(4) Dieser Artikel kann nicht als Grundlage für die Verwirklichung von Zielen der Gemeinsamen Außen- und Sicherheitspolitik dienen, und Rechtsakte, die nach diesem Artikel erlassen werden, müssen innerhalb der in Artikel 40 Absatz 2 des Vertrags über die Europäische Union festgelegten Grenzen bleiben.

Der GVE erfasst den gesamten „freien Datenverkehr". Eine EU-Kompetenz für datenschutzrelevante Vorgänge ohne europäische Relevanz scheidet indessen aus. Art. 16 Abs. 1 S. 1 AEUV normiert kein Grundrecht auf Datenschutz, sondern dient als Kompetenznorm, die durch Art. 16 Abs. 2 AEUV konkretisiert wird. Die Begrenzung der EU-Kompetenz wird aus den anderen Sprachfassungen der Vorschrift deutlich.

Art. 16 AEUV (deutsche Fassung)

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

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

Die auf der Grundlage dieses Artikels erlassenen Vorschriften lassen die spezifischen Bestimmungen des Artikels 39 des Vertrags über die Europäische Union unberührt.

Art. 16 AEUV (englische Fassung)

1. *Everyone has the right to the protection of personal data concerning them.*
2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

Art. 16 AEUV (französische Fassung)

1. *Toute personne a droit à la protection des données à caractère personnel la concernant.*
2. *Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données.*

Le respect de ces règles est soumis au contrôle d'autorités indépendantes. Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne.

Wo somit der freie Datenverkehr personenbezogene Daten umfasst, kann durch EU-Recht die Schranke des Datenverkehrs mitgeregelt werden, soweit eine EU Kompetenz für den Datenschutz besteht. Die europäischen Grundrechte wirken dabei nur kompetenzbegrenzend, nicht kompetenzbegründend (vgl. Paul Kirchhof, Stabilität von Recht und Geldwert in der Europäischen Union, NJW 2013, 1 ff., 4). In Teilen fehlt dem GVE die Regelungskompetenz.

Der RLE ist ebenfalls auf Art. 16 Abs. 2 AEUV gestützt. Das widerspricht zwar dem Grundsatz, dass bereichsspezifisches Sekundärrecht bereichsspezifische Ermächtigungsgrundlagen erfordert, wird aber primärrechtlich durch Erklärung 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte zum Vertrag von Lissabon gedeckt.

Selbst wo eine eindeutige Regelungskompetenz der EU besteht, verstößt die Wahl einer Verordnung zumindest partiell gegen das Subsidiaritätsprinzip. Nach der Begründung des GVE verlangt das Recht auf Schutz personenbezogener Daten einen unionsweit einheitlichen Datenschutz. Ohne gemeinsame EU-Vorschriften bestehe die Gefahr, dass der Datenschutz in den Mitgliedstaaten nicht in gleichem Maße gewährleistet sei. Das erfordert einen gemeinsamen Mindeststandard, rechtfertigt es aber nicht, einzelnen Mitgliedstaaten zumindest im öffentlichen Bereich ein höheres Datenschutzniveau zu versagen, an dem sich künftig die Weiterentwicklung des europäischen Datenschutzrechts ausrichten könnte. Für die Fortentwicklung des Datenschutzes sind Experimentiermöglichkeiten vielmehr unverzichtbar.

Die Vorbehalte gegen die Regelungsform einer Verordnung bestehen bei einer Richtlinie nicht. In der Begründung zum GVE heißt es: „Nach dem Verhältnismäßigkeitsprinzip muss jedes Handeln zielgerichtet sein und darf nicht über das hinaus gehen, was für die Erreichung der angestrebten Ziele notwendig ist.“ Ob dies der Fall ist, hängt mit der Legitimation des Reform-

pakets zusammen. Die erwähnten Eckpunkte der Reform legitimieren nur dann die Novellierung des EU-Datenschutzrechts, wenn sie wirklich zu seiner zeitgemäßen Modernisierung beitragen. Dies ist bei der konkreten Ausgestaltung zweifelhaft. Das Recht auf Vergessenwerden (Art. 17 GVE) ist im Ansatz begrüßenswert. Die konkrete Regelung dürfte gleichwohl an den Realitäten des Internets vorbeigehen (vgl. Gstrein: Die umfassende Verfügungsbefugnis über die eigenen Daten – Das „Recht auf Vergessenwerden" und seine konkrete Umsetzbarkeit ZD 2012, 424). Transparenz ist im Hinblick auf nicht erkennbare Überwachungsmaßnahmen unerlässlich. Wo aber Maßnahmen erkennbar datenschutzrechtlich relevant sind, sollte die Eigenverantwortlichkeit gestärkt werden. Zu einer ausgewogenen Datenschutzkultur gehört auch, dass jedem bewusst sein muss, was er mit seinen Daten anrichtet. Transparenz als solche ist kein Legitimationsgrund. Dass alle, die mit personenbezogenen Daten umgehen, dies verantwortlich mit dem gebotenen technischen Aufwand tun müssen, versteht sich von selbst. Die Gestaltung des Datenschutzes kann auch reglementiert werden. Fraglich ist nur, ob das wirklich auf europäischer Ebene geschehen muss (vgl. Richter, Datenschutz durch Technik und die Grundverordnung der EU-Kommission, DuD 2012, 576 ff.). Auch hier spricht alles für die Beschränkung auf eine Richtlinie. Die Datenschutzkontrolle muss schließlich unabhängig sein, wenn sie die Daten effektiv schützen soll. Dazu gehören Durchsetzungsmöglichkeiten, Sanktionsmöglichkeiten und organisatorische Vorkehrungen. Die „völlige" Unabhängigkeit der Datenschutzbehörden ist in Deutschland verfassungsrechtlich nur akzeptabel, wenn die parlamentarische Verantwortlichkeit der als Einheit zu sehenden Verwaltung gewährleistet bleibt. Die parlamentarische Verantwortlichkeit der Datenschutzbeauftragten muss dann qualitativ mit der Ministerverantwortlichkeit vergleichbar sein. Dies ist nicht der Fall, wenn die Kommission beim Datenschutz in die Stellung einer Kontrolleurin der Kontrolleure einrückt.

Zur nationalen Identität der Bundesrepublik Deutschland gehört die Möglichkeit einer systemimmanenten Fortbildung der Grundrechtsordnung durch das Bundesverfassungsgericht (vgl. Ronellenfitsch, in: Kühl/Reichold/Ronellenfitsch, Einführung in die Rechtswissenschaft 2011, § 25). Diese offene Grundrechtsordnung ist integrativer Bestandteil des Grundgesetzes. Die Entwürfe der Kommission schließen eine derartige Entwicklung aus. Sie gehen auch staatsorganisatorisch zu weit, weil sie hoheitliche Maßnahmen der Datenschutzbehörden gegen andere Hoheitsträger vorsehen (hierzu unter Ziff. 1.2.2). Durchsetzbare Zwangsmaßnahmen, Vollstreckungsmaßnahmen bis hin zur Ersatzvornahme, Verhängung von Bußgeldern kommen nur in Überordnungsverhältnissen in Betracht. Eine Vollstreckung gegen Hoheitsträger ist ausgeschlossen (§ 17 VwVG). Dadurch, dass der GVE hinsichtlich der

Sanktionsmöglichkeiten der Datenschutzbeauftragten gegenüber Privaten und Hoheitsträgern im nicht polizeilichen Bereich keine Unterschiede macht, bringt er die Datenschutzbehörden in die untragbare Situation, etwa gegen die Finanzverwaltung Bußgeldbescheide oder gegen die Polizei Ordnungsverfügungen erlassen zu müssen. Zur Durchsetzung von Anordnungen müssten sich die Datenschutzbehörden der Machtmittel der Behörden bedienen, gegen die sie gerade vorgehen sollen. Nicht einmal der nationale Gesetzgeber könnte dem gegensteuern, da nach der ständigen Rechtsprechung des EuGH eine nationale Regelung nicht in die Befugnisse nationaler Behörden eingreifen darf, die unmittelbar Unionsrecht durchzusetzen haben (EuGH, Urteile vom 3. Dezember 2009 – Rs. C-424/07 – Kommission/Deutschland, Slg. 2009, I-1143 Rdnr. 78,91 und vom 11. März 2010 – Rs. C–522/08 – Telekommunikacja Polska, Slg. 2010, I-2079 Rdnr. 27). Das ist auch deswegen problematisch, weil sich die Kommission bei Verstößen gegen EU-Recht die letzte Entscheidungsgewalt vorbehalten hat. Damit wird ein Überordnungsverhältnis der Kommission gegenüber allen staatlichen Organen der Mitgliedstaaten begründet. Eine derart weitgehende Entstaatlichung Deutschlands ist mit Art. 23 Abs. 1 Satz 3 GG unvereinbar.

Art. 23 GG

(1) Zur Verwirklichung eines vereinten Europas wirkt die Bundesrepublik Deutschland bei der Entwicklung der Europäischen Union mit, die demokratischen, rechtsstaatlichen, sozialen und föderativen Grundsätzen und dem Grundsatz der Subsidiarität verpflichtet ist und einen diesem Grundgesetz im wesentlichen vergleichbaren Grundrechtsschutz gewährleistet. Der Bund kann hierzu durch Gesetz mit Zustimmung des Bundesrates Hoheitsrechte übertragen. Für die Begründung der Europäischen Union sowie für Änderungen ihrer vertraglichen Grundlagen und vergleichbare Regelungen, durch die dieses Grundgesetz seinem Inhalt nach geändert oder ergänzt wird oder solche Änderungen oder Ergänzungen ermöglicht werden, gilt Artikel 79 Abs. 2 und 3.

Art. 79 GG

(1) Das Grundgesetz kann nur durch ein Gesetz geändert werden, das den Wortlaut des Grundgesetzes ausdrücklich ändert oder ergänzt. Bei völkerrechtlichen Verträgen, die eine Friedensregelung, die Vorbereitung einer Friedensregelung oder den Abbau einer besatzungsrechtlichen Ordnung zum Gegenstand haben oder der Verteidigung der Bundesrepublik zu dienen bestimmt sind, genügt zur Klarstellung, dass die Bestimmungen des Grundgesetzes dem Abschluss und dem Inkraftsetzen der Verträge nicht entgegenstehen, eine Ergänzung des Wortlautes des Grundgesetzes, die sich auf diese Klarstellung beschränkt.

(2) Ein solches Gesetz bedarf der Zustimmung von zwei Dritteln der Mitglieder des Bundestages und zwei Dritteln der Stimmen des Bundesrates.

(3) Eine Änderung dieses Grundgesetzes, durch welche die Gliederung des Bundes in Länder, die grundsätzliche Mitwirkung der Länder bei der Gesetzgebung oder die in den Artikeln 1 und 20 niedergelegten Grundsätze berührt werden, ist unzulässig.

1.2.3
Fazit

Die grundsätzlich zu begrüßende Modernisierung des europäischen Datenschutzrechts kann dazu führen, dass das deutsche Datenschutzrecht auch in seiner identitätsstiftenden Gestalt verabschiedet werden muss. Dass ist inakzeptabel und bedarf der Korrektur.

1.3
Stellung des Hessischen Datenschutzbeauftragten und Aufgabenzuwachs

1.3.1
Ausgangslage

Die Rechts- und Aufgabenstellung des Hessischen Datenschutzbeauftragten wurde schon im 34. Tätigkeitsbericht, Ziff. 2.1, näher dargestellt. Seither sind gravierende Änderungen eingetreten oder eingeleitet, auf die anschließend eingegangen wird.

1.3.2
Rechtsstellung

Die Rechtsstellung des Hessischen Datenschutzbeauftragten als Amtsträger, der sein Amt unabhängig ausübt, blieb im Berichtszeitraum unverändert.

1.3.3
Aufgabenstellung

1.3.3.1
Kriterien des Behördenbegriffs

Nach § 22 HDSG ist der Hessische Datenschutzbeauftragte „als oberste Landesbehörde“ in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen.

§ 22 HDSG

Der Hessische Datenschutzbeauftragte ist als oberste Landesbehörde in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen.

Diese Regelung war bereits in der Fassung des HDSG vom 7. Januar 1999 (GVBl. I S. 98) enthalten. Gleichwohl wurde die Stellung des Hessischen Datenschutzbeauftragten als oberste Landesbehörde selbst in den juristischen Fachpublikationen nur selten wahrgenommen. In den Aufzählungen der obersten Landesbehörden taucht jedenfalls der Datenschutzbeauftragte nicht auf (vgl. etwa Maurer, Allgemeines Verwaltungsrecht, 18. Aufl. 2011, § 22 Rdnr. 19; Burgi, in: Erichsen/Ehlers, Allgemeines Verwaltungsrecht, 14. Aufl. 2010, Rdnr. 15; Detterbeck, Allgemeines Verwaltungsrecht mit Verwaltungsprozessrecht, 9. Aufl. 2011, § 5 Rdnr. 220; Peine, Allgemeines Verwaltungsrecht, 10. Aufl. 2011, Rdnr. 72). Das dürfte damit zusammenhängen, dass bereits der Behördenbegriff mehrdeutig ist. So unterscheidet man heute den organisatorisch-institutionellen Behördenbegriff vom Begriff der Behörde im funktionellen Sinn (vgl. BVerwG, Urteil vom 7. November 2011 – 7C 3.11 –, BVerwGE 141, 122, 124; Ronellenfitsch, in: Ronellenfitsch/Bader, VwVfG, Online Kommentar 2012, § 1 Rdnr. 65). Während etwa Walter Jellinek die organisatorische Einheit als Wesensmerkmal der Behörde bezeichnete (Verwaltungsrecht, 3. Aufl. 1931/1948, S. 359), brachte Otto Mayer, der als Verwaltungsbehörden die Stellen charakterisierte, von welchen der obrigkeitliche Akt in der Verwaltung (der Verwaltungsakt) auszugehen habe (Deutsches Verwaltungsrecht I, 3. Aufl. 1923, S. 93), den funktionellen Begriff um Ausdruck. Der organisationsrechtliche Behördenbegriff erfordert eine organisatorische Eigenständigkeit, die sich in der Unabhängigkeit vom Wechsel des Amtsinhabers, der Selbständigkeit der Aufgabenerledigung und in der Möglichkeit der Eigengestaltung der Angelegenheiten innerhalb des zugeordneten Zuständigkeitsbereichs ausdrückt. Behörde ist danach das Organ eines Verwaltungsträgers, das berechtigt ist, mit Außenwirkung Aufgaben öffentlicher Verwaltung wahrzunehmen (BVerwG 141, 122, 125; OVG Bremen, Beschluss vom 7. April 2011 – 1 A 200/09 –, NVwZ 2011, 1146). § 1 Abs. 4 VwVfG (Bund) bzw. § 1 Abs. 2 HVwVfG liegt demgegenüber der funktionelle Behördenbegriff zugrunde. Maßgeblich ist hier die Rechtsnatur der Verwaltungstätigkeit (OVG Münster, Urteil vom 26. Oktober 2011 – 8 A 2593/10 –, AfP 2012, 94). Die Bezeichnung der Einrichtung, die diese Tätigkeit vornimmt, ist irrelevant. Es genügt, dass es sich um eine „Stelle“ handelt. Ein gewisses Maß an organisatorischer Selbständigkeit ist dennoch notwendig. Selbständigkeit besteht nur im Rahmen der Zuständigkeit. Äußeres Zeichen der Selbständigkeit ist häufig das Auftreten unter eigenem Namen. Erforderlich ist trotz des weiten Gesetzeswortlauts, dass die Behörde außenwirksam Verwaltungsaufgaben erfüllt. Beide Behördenbegriffe schließen sich nicht aus, sondern weisen gemeinsame Kriterien auf, die erfüllt werden müssen, damit man überhaupt von einer Behörde sprechen kann. Als Behörde in diesem Sinn versteht

man diejenige Amtsinstitution (und auch die in ihr tätigen Personen), die mit Wirkung nach außen Verwaltungstätigkeiten ausüben (Forsthoff, Lehrbuch des Verwaltungsrechts, 10. Aufl. 1973, S. 444). Kriterien des Behördenbegriffs sind:

- eine Stelle als organisatorische-institutionelle Einheit,
- hinreichende organisatorische Selbständigkeit,
- die Wahrnehmung öffentlicher administrativer Aufgaben und
- öffentlich-rechtliches außenwirksames Handeln.

1.3.3.2
Bisherige Aufgabenstellung des Hessischen Datenschutzbeauftragten

Nach der ursprünglichen Aufgabenstellung des Hessischen Datenschutzbeauftragten war fraglich, ob die Kriterien einer obersten Landesbehörde in der Sache erfüllt waren oder ob es sich letztlich nur um eine Fiktion handelte. Zwar verfügte der Hessische Datenschutzbeauftragte über die für eine Stelle als organisatorische Einheit erforderliche hinreichende organisatorische Selbständigkeit. Schwierigkeiten bereitet aber bereits die funktionale Zuordnung der Datenschutzkontrolle zu den einzelnen Staatsgewalten (vgl. Maurer, a. a. O., § 1 Rdnr. 6). Die Verlegenheitslösung, Datenschutzbehörden als Kontrollinstanzen sui generis zu qualifizieren (so etwa Petri/Tinnefeld, Völlige Unabhängigkeit der Datenschutzkontrolle. Demokratische Legitimation und unabhängige parlamentarische Kontrolle als moderne Konzeption der Gewaltenteilung, MMR 2009, 157 ff.), entbindet nicht von der Notwendigkeit, institutionell und funktionell die Datenschutzkontrolle durch öffentliche Stellen einer der klassischen Staatsgewalten zuzuordnen. Dabei zeigt sich, dass die Datenschutzkontrolle eindeutig nicht zu Gesetzgebung, Rechtsprechung oder Regierung zählt. Es kann sich folglich nach der Subtraktionsmethode nur um Verwaltung handeln, um die planmäßige und dauerhafte Tätigkeit des Staates zur Erreichung seiner Zwecke mit Ausnahme der Gesetzgebung, Rechtsprechung und Regierung (Ronellenfitsch, in: Kühl/Reichold/Ronellenfitsch, Einführung in die Rechtswissenschaft, 2011, § 27 Rdnr. 4). Die Kontrollbefugnisse des Hessischen Datenschutzbeauftragten betrafen indessen kein öffentlich-rechtliches außenwirksames Verhalten. Insbesondere gingen und gehen nach wie vor von der Beanstandung keine unmittelbaren Rechtwirkungen aus (BVerwG, Beschluss vom 5. Februar 1992 – 7 B 15.92, NVwZ-RR 1992, 31). Von den unionsrechtlich nur als Regelungsoption akzeptablen Möglichkeiten des Art. 2 Abs. 3 RL 95/46/EG hat der deutsche Gesetzgeber die als Eingriffsbefugnisse zu qualifizierenden Einwirkungsmöglichkeiten gegenüber Hoheitsträgern nicht übernommen. Ob er dies überhaupt gekonnt hätte, ist fraglich,

da nach deutscher Verfassungstradition Meinungsverschiedenheiten zwischen gleichrangigen Hoheitsträgern nicht mit Zwangsmitteln ausgetragen werden dürfen (Grundlegend: BVerwG, Urteil vom 16. Januar 1968 – A 1.67 –, BVerwGE 29, 52; Urteil vom 10. Januar 1996 – 1 C 3.94 –, NVwZ-RR 1997, 350, 352; HessVGH, Beschluss vom 7. März 1996 – 14 TG 3967/95 –, NVwZ 1997, 304, 305; Schenke, Polizei- und Ordnungsrecht, 7. Aufl. 2011, Rdnr. 234; a.A. Schoch, in Schmidt-Aßmann/Schoch, Besonderes Verwaltungsrecht, 14. Aufl., 2008, 2 Rdnr. 125; Britz, Abschied vom Grundsatz fehlender Polizeipflicht von Hoheitsträgern, DÖV 2002, 891 ff.; Borowski, Die formelle und materielle Polizeipflicht von Hoheitsträgern, VerwArch. 2010, 58 ff.). Soweit das Bundesverwaltungsgericht Abweichungen durch das Fachrecht zulässt (BVerwG, Urteil vom 27. Juli 2002 – 7 C 24.01 BVerwGE 117, 1; Urteil vom 25. September 2008 – 7 A 4.0, NVwZ 2009, 588), entspricht das ebenfalls der deutschen Verfassungstradition (vgl. bereits PrOVG, Urteil vom 5. Mai 1877 – Rep. C.94/77, PrOVGE 2, 400, 409). Danach muss das Fachrecht aber auch die Durchsetzbarkeit der Eingriffsmaßnahmen gegen andere Hoheitsträger sicherstellen. Das lässt sich ohne Preisgabe der Unabhängigkeit des Hessischen Datenschutzbeauftragten schwerlich realisieren.

1.3.3.3
Aufgabenzuwachs

Die Zusammenlegung des privaten und öffentlichen Bereichs beim Hessischen Datenschutzbeauftragten hat diesen definitiv zu einer Behörde im organisatorischen und funktionellen Sinn gemacht. Im privaten Bereich ist die Aufgabenstellung durch außenwirksames Handeln gefragt. Die hierfür nötigen Eingriffsbefugnisse ergeben sich insbesondere aus § 38 Abs. 5 BDSG. Wie im 40. Tätigkeitsbericht dargelegt, darf organisatorische Vereinheitlichung die grundlegenden strukturellen Unterschiede der beiden Bereiche nicht einebnen. Dieser Gesichtspunkt verdient bei der Umgestaltung des Datenschutzrechts auf EU-Ebene besondere Beachtung.

Bei der Aufstellung des neuen Organisationsplans wurde gleichwohl nach Fachbereichen organisiert. Eine Aufteilung der Abteilungen und Referate in öffentlichen und nicht öffentlichen Datenschutz wurde nicht gewählt, weil in aller Regel die Fachaufgaben die Datenschutzregelungen prägen, auch wenn bei den Durchsetzungsinstrumenten und im Ergebnis natürlich Unterscheidungen notwendig sind. Inzwischen haben nahezu alle Referate ein Spektrum, das Datenschutzfragen im öffentlichen und nicht öffentlichen Bereich umfasst. Dies ist auch der Trend bei den Kontrollstellen in den anderen Bundesländern, da sich mit einer derartigen Organisation am besten Synergieeffekte erzielen lassen.

Die neue Organisationsstruktur stand ab 1. Januar 2012 zur Verfügung. Zwei Leitungsfunktionen der neuen Organisation wurden durch Umsetzungen bereits zum 1. Januar 2012 besetzt. Drei Sachbearbeiterpositionen konnten durch Übernahme von Beschäftigten des Regierungspräsidiums Darmstadt ebenfalls bereits zum 1. Januar 2012 besetzt werden. Die verbliebenen vakanten Aufgabenbereiche wurden vorübergehend durch vorhandene Beschäftigte mitbetreut. Ab 1. Januar 2012 waren trotz des Wegfalls des Großteils der bisherigen Bearbeiterinnen und Bearbeiter aus der Aufsichtsbehörde auf diese Weise alle Aufgabenbereiche betreut.

Da zum Jahresbeginn noch die meisten der neuen Positionen unbesetzt waren, wurde das Organigramm zunächst von der Homepage entfernt und stattdessen für jeweilige Fachaufgaben Ansprechpartner eingestellt. Im vierten Quartal waren bereits viele Positionen wieder besetzt. Deshalb ist seit 1. Oktober 2012 das Organigramm auch wieder auf die Homepage eingestellt.

Das Jahr 2012 war durch eine Vielzahl von Personalgewinnungsmaßnahmen geprägt. Bereits Ende 2011 wurden drei Auswahlverfahren begonnen, die direkt nach Beschluss des Haushaltes abgeschlossen wurden. Auf diese Weise konnten die Servicebereiche Geschäftsstelle und Informationstechnik als erste mit jeweils einer Person verstärkt und bereits die wichtige Referatsleitung Beschäftigtendatenschutz und internationaler Datenverkehr besetzt werden. Von den 16 neuen Stellen waren 2012 noch 11 durch Ausschreibungen zu besetzen.

Im Berichtszeitraum wurden zehn Auswahlverfahren durchgeführt. Die Anzahl übersteigt die vakanten Stellen, weil wegen der Auswahl von zwei internen Bewerbern zusätzliche Ausschreibungen für die Nachbesetzung dieser Positionen erforderlich wurden.

Durch die Auswahlverfahren wurden im Jahr 2012 besetzt:

- Eine Stelle in der Sachbearbeitung im Bereich Kreditinstitute, Auskunfteien, Inkasso, ab 1. Mai 2012 eine weitere dort zum 1. Oktober 2012
- Eine Stelle in der Sachbearbeitung Videoüberwachung, automatisierte Personaldatenverarbeitung ab 1. Juli 2012
- Eine Stelle persönliche Referentin zum 1. August 2012
- Eine Stelle in der Sachbearbeitung Gesundheitswesen, Forschung, Statistik ab 1. September 2012
- Eine Stelle Referent Gesundheitswesen, Forschung, Statistik ab 1. Oktober 2012

- Eine Stelle Referatsleitung Kreditinstitute, Auskunfteien, Inkasso ab 1. Oktober 2012
- Eine Stelle Referentin Verkehr, Daseinsvorsorge, Bauen, Wohnen, Geodaten, Umwelt, Landwirtschaft und Forsten ab 15. November 2012
- Eine Stelle Referatsleitung Hochschulen, Schulen, Bibliotheken, Archive zum 1. Dezember 2012.

Im Berichtszeitraum abgeschlossen wurde außerdem ein Auswahlverfahren für eine Referentenposition jeweils zur Hälfte im Referat Justiz, Polizei, Ordnungswidrigkeiten sowie im Referat Europäischer und internationaler Datenschutz und Ausländerrecht; die Einstellung von zwei Teilzeitkräften erfolgt zum 1. bzw. 15. Januar 2013. Eine weitere Referentenposition ist ausgeschrieben, die Bewerbungsfrist läuft noch bis zum Ende des Berichtszeitraums.

Für das Jahr 2013 steht nur noch eine Position zur Ausschreibung und Besetzung an.

Insgesamt wurden im Jahr 2012

- 10 Auswahlverfahren abgeschlossen und ein weiteres begonnen,
- 557 Bewerbungen auf Ausschreibungen und zahlreiche Initiativbewerbungen gesichtet,
- 87 Vorstellungsgespräche (Erst- und Zweitgespräche) geführt, wovon 41 mit einem getrennten Praxistest verbunden waren.

Bis zur Einstellung und Einarbeitung der neuen Kolleginnen und Kollegen mussten alle Beschäftigten erhebliche Mehrbelastungen tragen.

Das zusätzliche Personal konnte auf der bisherigen Mietfläche nicht untergebracht werden; es mussten zusätzliche Räume gefunden werden. Wie bereits im 40. Tätigkeitsbericht (Ziff. 1.2.2) geschildert, wurde Ende November 2011 als Interimslösung ein auf zwei Jahre angelegter Mietvertrag (mit Verlängerungsoption für sechs Monate) über zusätzliche Flächen in einem benachbarten Gebäude abgeschlossen. Nach diesem Zeitpunkt stehen voraussichtlich Flächen im Haupthaus zur Verfügung, auf die eine Option eingeräumt wurde, damit die Dienststelle räumlich zusammengeführt werden kann. Aufgrund der speziellen Situation des Vermieters hatte dieser jede Investition in die vermieteten Flächen abgelehnt, so dass die Mietfläche unter Regie meiner Dienststelle und auf deren Kosten brandschutztechnisch zu ertüchtigen und auf die Bedürfnisse anzupassen war. Im Ausgleich dazu konnte die Miete so reduziert werden, dass sich die Investitionen während der 2-jährigen Mietzeit amortisieren. Mit der Bauausführung wurde das vom Vermieter benannte Architektenbüro beauftragt, das die Ausschreibungsunterlagen sowie den Antrag für die erforderliche Bauge-

nehmigung zu den Brandschutzmaßnahmen erstellte. Die Baugenehmigung wurde im Januar 2012 beantragt, im Februar 2012 erteilt. Die Umbauarbeiten waren Mitte April 2012 abgeschlossen und von der Bauaufsicht abgenommen, so dass die Fläche ab 23. April 2012 bezogen werden konnte. In der Bauphase erfolgten auch die erforderlichen Um- und Einbauten für die IT (Serverraum mit entsprechender Ausstattung), die Telefonausstattung (Telefonanlage) und die Sicherheitsausstattung (Türsicherung und Alarmanlage). Die Baukosten sind im geplanten Rahmen geblieben.

1.4
Arbeitsschwerpunkte und Statistik

1.4.1
Arbeitsschwerpunkte

Für anlassunabhängige Prüfungen war durch die Bewältigung der neuen Aufgaben mit dem vorhandenen Personal und dem erst schrittweise neu eingestellten Personal keine Kapazität vorhanden. Zu Jahresbeginn waren noch zwölf Stellen unbesetzt; zum Jahresende immer noch drei Stellen. Zudem mussten die neu hinzugekommenen Beschäftigten eingearbeitet werden.

Deshalb wurden im Berichtszeitraum 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, Adresshandel/Werbung, Justiz/Polizei/Strafverfolgung, Gesundheit und Soziales sowie Kreditwirtschaft.

Arbeitsintensiv und sehr komplex sind ferner die Fragestellungen auf dem Gebiet des internationalen Datenverkehrs. Dort gibt es einen erheblichen Beratungsbedarf der Unternehmen. Hier stehen Fragestellungen der konzerninternen wie -externen Datenverarbeitung in das außereuropäische Ausland im Vordergrund. Häufig zu klären ist die Frage, ob solche Datenverarbeitungen bzw. unter welchen Rahmenbedingungen diese zulässig sind. Oft sind aufwändige Ermittlungen erforderlich und die Sachlage ist mit technischen Fragen, wie etwa dem Thema Cloud Computing, verbunden.

Für das Einleiten und Betreiben von Ordnungswidrigkeitenverfahren sowie andere Sanktions- und Meldungsregelungen nach dem BDSG (Zwangsgelder, Meldung von Datenpannen) sind sowohl organisatorische Strukturen

geschaffen als auch Maßnahmen zur Sicherstellung einer einheitlichen Handhabung und Abstimmung mit den anderen Aufsichtsbehörden – u. a. in der AG Sanktionen des Düsseldorfer Kreises – ergriffen worden (zu den Ordnungswidrigkeitenverfahren s. auch Ziff. 4.1).

In der Zeit seit der Übernahme der neuen Aufgabe war der Gesprächsbedarf auch seitens großer Unternehmen recht groß. So habe ich Grundsatzgespräche, z. B. mit einer Vielzahl von Kreditinstituten mit Sitz im Raum Frankfurt, der SCHUFA und dem Verband der Auskunfteien, der Deutschen Bahn, einem internationalen Pharmaunternehmen und diversen anderen mittleren und großen in Hessen ansässigen Unternehmen geführt.

1.4.2
Statistik

In nebenstehender Tabelle sind Angaben zur Anzahl der Eingaben und Beratungsanfragen enthalten. Um nicht unnötig Kapazitäten von den Kernaufgaben abzuziehen, wurde die Statistik 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.

Beratungen waren in aller Regel deutlich aufwändiger als die Bearbeitung von Eingaben (wie z. B. die Beratung zur Ausgestaltung eines Online-Bewerbungsverfahrens für ein Studentenwohnheim, zum Datenschutzkonzept für ein europäisches Lungenregister bei Kindern, zu Sicherheitskonzepten für diverse IT-Verfahren, zum Einsatz von Videoüberwachungen). Das Spektrum ist ebenso breit wie bei den Eingaben.

Die Zahlen für die Ordnungswidrigkeitenverfahren finden sich im Beitrag der Hessische Datenschutzbeauftragte als Bußgeldbehörde (Ziff. 4.1).

Arbeitsstatistik des Hessischen Datenschutzbeauftragten

Dokumentierte Eingaben

Fachgebiet	Anzahl
Auskunfteien und Inkassounternehmen	307
Elektronische Kommunikation	187
Beschäftigtendatenschutz	131
Wohnen, Miete und Nachbarschaft	126
Polizei, Justiz, Strafvollzug und Gerichte	91
Werbung und Adresshandel	86
Gesundheitswesen	83
Kreditwirtschaft	83
Soziales	74
Kommunen	71
Handel und Handwerk	70
Verkehr und Daseinsvorsorge	68
Versicherungen	29
Vereine und Verbände	27
Schulen und Hochschulen	19
Forschung, Planung und Statistik	11
Sonstiges	59
Summe der dokumentierten Eingaben	**1.522**
Summe der dokumentierten Beratungsanfragen	**279**
Summe der telefonischen Eingaben und Beratungen	**4.032**
Gesamtsumme	**5.833**

1.4.3
Publikationen und Vorträge

Aufsätze

Verkehrsmobilität und Datenschutz – Grundrechte im Wechselspiel, in: Alexander Dix u. a. (Hrsg.), Informationsfreiheit und Informationsrecht, Jahrbuch 2011, 2012, S. 253–264

Fortentwicklung des Datenschutzes, DuD 2012, S. 561–563

Durchsetzung von Großprojekten (Stuttgart 21), in: Michael Ronellenfitsch/Ralf Schweinsberg/Iris Henseler-Unger (Hrsg.), Aktuelle Probleme des Eisenbahnrechts XVII, 2012, S. 13–24

Die Unart des Artenschutzes, in: Michael Ronellenfitsch/Ralf Schweinsberg/Iris Henseler-Unger (Hrsg.), Aktuelle Probleme des Eisenbahnrechts XVII, 2012, S. 217–220

Entwicklung und Tendenzen privatwirtschaftlicher Betätigung der Gemeinden, in: Werner Hoppe/Michael Uechtritz/Hans-Joachim Reck (Hrsg.), Handbuch Kommunale Unternehmen, 3. Aufl. Köln 2012, §§ 1–5, S. 1–62 (teilweise mit Lisa Ronellenfitsch)

Europäisierung des Datenschutzes bei der Bahn, DVBl. 2012, 1521–1530

Mobilität unter Aufsicht – Freie Fahrt und jeder weiß wohin in: Norbert Kartmann/Michael Ronellenfitsch (Hrsg.), 40 Jahre Datenschutz in Hessen 2011, 2012, 59 f.

Gisela Quiring-Kock, Anforderungen an ein Datenschutzmanagementsystem – Aufbau und Zertifizierung, DuD 11/2012, S. 832–836)

Kommentierungen

Schild/Ronellenfitsch und andere, Kommentar zum Hessischen Datenschutzgesetz, Stand März 2012

Marschall, FStrG, 6. Aufl. 2012, Einleitung, S. 31–36, §§ 16–17 f. S. 404–610

Michael Ronellenfitsch/Johann Bader, Verwaltungsverfahrensgesetz, Kommentar, 2012, §§ 1–3, § 78

Vorträge und Schulungen

In insgesamt 36 Veranstaltungen war ich selbst oder Beschäftigte meiner Dienstelle mit Vorträgen zum Datenschutz oder als Moderatoren vertreten. Die Themen umspannten dabei ein großes Spektrum angefangen von der europarechtlichen Entwicklung über Datenschutzthemen aus dem Gesundheitsbereich, der Arbeitslosen-, Sozial-, Kinder- und Jugendhilfe, Datenschutz bei Finanzdienstleistungen, in der Partei, im Verein und spezielle Fragen für Existenzgründer sowie zu den Rechten Beschuldigter und Strafverteidiger, Datenschutz in pädagogischen Netzen, in sozialen Netzwerken und bei mobilen Datenträgern und Geräten, bei Cloud Computing, Fragen der sicheren Datenübertragung, Schnittstellenproblematiken zum Verbraucherschutz, zu Informationsfreiheit und Transparenz bis hin zu speziellen Fragen wie z. B. dem Informationsgehalt der Spielerkarte.

Wie jedes Jahr waren Beschäftigte meiner Dienststelle auch als Referenten bei insgesamt 14 Datenschutzseminaren tätig, die von Lehrgangsveranstaltern aus dem öffentlichen Bereich – wie dem Verwaltungsschulverband – im Einzelfall auch von öffentlichen Stellen selbst organisiert werden.

1.5
Rechtsentwicklung

1.5.1
Europäischer Gerichtshof

Aus der Rechtsprechung des EuGH ist hinzuweisen auf das Urteil vom 16. Oktober 2012 – C-614/10 (ZD 2012, 563). Danach hat Österreich dadurch gegen seine Verpflichtungen aus der RL 95/46/EG verstoßen, da es nicht alle Vorschriften erlassen hat, die erforderlich sind, damit die in Österreich bestehende Rechtslage in Bezug auf die Datenschutzkommission dem Kriterium der Unabhängigkeit genügt, und zwar im Einzelnen dadurch, dass es eine Regelung eingeführt hat, wonach das geschäftsführende Mitglied der Datenschutzkommission in das Bundeskanzleramt eingegliedert ist und der Bundeskanzler über ein unbedingtes Recht verfügt, sich über alle Gegenstände der Geschäftsführung der Datenschutzkommission zu unterrichten.

Ähnlich bedeutsam ist das Urteil vom 16. Februar 2012 – C-360/10 (Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA [SABAM]/Netlog NV) SABAM/Netlog (GRUR 2012, 382), das eine Pflicht für Betreiber sozialer Netzwerke zu umfassenden Überwachungs- und Filtersystemen verneint.

1.5.2
Bundesverfassungsgericht

Das Verständnis der Konzeption der informationellen Selbstbestimmung als gleitende Skala zwischen den Eckpunkten des Art. 1 Abs. 1 und 2 Abs. 1 GG, das in den vorangegangenen Tätigkeitsberichten näher erläutert wurde, fand Bestätigung in einer weiteren Grundsatzentscheidung des Bundesverfassungsgerichts, nämlich in dem – im Berichtszeitrum mit zu berücksichtigenden – Beschluss vom 7. Dezember 2011 – 2 BvR 2500/09 und 2 BvR 1857/10 (BVerfGE 130, 1) zur Verwertbarkeit rechtswidrig erhobener personenbezogener Informationen im Strafprozess. Den Schutz des Kernbereichs privater Lebensgestaltung stützt das Bundesverfassungsgericht unmittelbar auf Art. 1 Abs. 1 GG, behandelt aber den Streitgegenstand unter dem Aspekt des Schutzes personenbezogener Daten. Das ist bedeut-

sam für andere datenschutzrechtliche Fragestellungen. Der isolierte Schutz der Menschenwürde und der allgemeinen Handlungsfreiheit bleibt Datenschutz und fällt in den Kompetenzbereich der Datenschutzbehörden. So können Maßnahmen nach § 6b BDSG auch gegen Attrappen gerichtet werden.

1.5.3
Rechtsprechung der Fachgerichte

Grundsatzcharakter haben folgende Entscheidungen der obersten Fachgerichte:

Das Urteil des Bundesverwaltungsgerichts vom 25. Juli 2012 – 6 C 14.11 (ZUM-RD 2012,688 = ZD 2012, 576) – ist von erheblicher Bedeutung für die legislatorische Ausgestaltung der Telekommunikationsunternehmen treffenden Überlassungspflicht von Teilnehmerdaten an andere Unternehmen. Die Brisanz der Entscheidung für den Datenschutz liegt in der Abgrenzung der unions- und nationalrechtlichen Regelungskompetenz, zu der sich der Gerichtshof der Europäischen Union schon im Urteil vom 5. Mai 2011 – Rs. C-543/09 (Deutsche Telekom u. a. (EuZW 2011, 483)) – geäußert hatte. Materiell datenschutzrechtlich ist nach Ansicht des Bundesverwaltungsgerichts die informationelle Selbstbestimmung der Telefonkunden nur am Rande berührt, da diese durch ihre Bereitschaft, mit ihren Daten in die Teilnehmer- und Auskunftsverzeichnisse eines Anbieters aufgenommen zu werden, der Weitergabe ihrer Daten an unbestimmte Dritte bereits zugestimmt hätten.

Materielles Datenschutzrecht, nämlich das allgemeine Persönlichkeitsrecht einer bekannten Entertainerin bei der (Bild-)Berichterstattung über deren Erkrankung, steht demgegenüber im Mittelpunkt des Urteils des Bundesgerichtshofs vom 18. September 2012 – VI ZR 291/10 – (NJW 2012, 3645). Im Streitfall waren das Interesse der Klägerin am durch Art. 1 Abs. 1, Art. 2 Abs. 1 GG, Art. 8 EMRK gewährleisteten Schutz ihrer Persönlichkeit einerseits und die durch Art. 5 Abs. 1 GG, Art. 10 EMRK geschützten Äußerungsinteressen der Beklagten andererseits abzuwägen. Diese Abwägung fiel zugunsten der Beklagten aus. Der Senat sah auch das abgestufte Schutzkonzept der §§ 22, 23 KUG gewahrt.

Mit der datenschutzrechtlich problematischen verdeckten Videoüberwachung von Arbeitnehmern befasst sich das Urteil des Bundesarbeitsgerichts vom 21. Juni 2012 – 2 AZR 153/11 (NJW 2012, 3594 = NZA 2012, 1025 = ZD 2012, 568). Danach kann eine heimliche Videoüberwachung zulässig sein und zu verwertbaren Beweismitteln führen, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfeh-

lung zu Lasten des Arbeitgebers besteht, es keine Möglichkeit zur Aufklärung durch weniger einschneidende Maßnahmen (mehr) gibt und die Videoüberwachung insgesamt nicht unverhältnismäßig ist. Trotz erheblichen Argumentationsaufwands bleibt fraglich, ob sich diese Auffassung mit § 6b Abs. 2 BDSG vereinbaren lässt. Bei konkretem Verdacht einer Straftat sollte sich der Arbeitgeber an die zuständigen Strafverfolgungsorgane wenden.

Aus der Rechtsprechung der hessischen Instanzgerichte ist darauf aufmerksam zu machen, dass nach dem Urteil des OLG Frankfurt am Main vom 8. März 2012 – 16 U 125/11 (NJW 2012, 2896) ein Arzt, der sich Bewertungen in einem frei zugänglichen Internetportal ausgesetzt sieht, keinen Anspruch gegen den Betreiber des Portals auf Löschung des Eintrags hat. Zum Hessischen Kinderschutzgesetz hat das VG Frankfurt am Main mit Beschluss vom 11. Mai 2012 – 7L 179/12 (NJW 2012, 3528) ausgeführt: „Das Gesetz verletzt nach seinem Wortlaut weder die Grundrechte von Eltern nach Art. 6 Abs. 1 und 2 GG noch Art. 4 HessVerf. Es ist grundsätzlich geeignet, das Ziel des Gesundheitsschutzes und die Verhinderung von Kindeswohlgefährdungen in seinem Spannungsverhältnis zum Elternrecht zu wahren. Denn durch die verpflichtende Teilnahme an den Vorsorgeuntersuchungen erlangt der Staat Kenntnis über den gesundheitlichen Zustand aller Kinder, wodurch er sein Wächteramt aus Art. 6 Abs. 2 Satz 2 GG ausüben kann.“ Dies ist auch meine Ansicht (vgl. 36. Tätigkeitsbericht, Ziff. 5.8.2).

1.5.4
Publikationen

An Publikationen ist für den Berichtszeitraum insbesondere hinzuweisen auf die Monographien von Ruth Weidner-Braun, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung am Beispiel des personenbezogenen Datenverkehrs im WWW nach deutschem öffentlichem Recht, 2012 sowie von Bernd Liedke, Die Einwilligung im Datenschutzrecht 2012. Von der Aufsatzliteratur sind zu erwähnen: Klar, Der Rechtsrahmen des Datenschutzrechts für Visualisierungen des öffentlichen Raums – Ein taugliches Konzept zum Schutz der Betroffeneninteressen? MMR 2012, 788 ff.; Debus, Die behördlichen Beauftragten für Datenschutz und Informationsfreiheit, DÖV 2012, 917 ff.; Krämer, Die Verarbeitung personenbezogener Daten durch Wirtschaftsauskunfteien, NJW 2012, 320 ff.; Klug/Gola, Die Entwicklung des Datenschutzrechts in den Jahren 2012, 2489.

2. Übergreifende Themen (öffentlicher und nicht öffentlicher Bereich)

2.1 Querschnittsthemen

2.1.1 Geplante EU-Verordnung über elektronische Identifizierung und Vertrauensdienste

Der Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt befasst sich mit elektronischer Identifizierung und Authentisierung einerseits und mit Vertrauensdiensten wie Signatur, Siegeln und Zeitstempeln andererseits. Hinsichtlich der Vertrauensdienste soll sie die EU-Signaturrichtlinie ersetzen. Der Beitrag setzt sich mit den Stärken und Schwächen des Entwurfes auseinander und schlägt Verbesserungen vor.

Die Europäische Kommission hat mit ihrem Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (COM [2012] 238 final) neue Vorschriften erarbeitet, um grenzüberschreitende und sichere elektronische Transaktionen in Europa zu ermöglichen. Die Verordnung soll dafür sorgen, dass Personen und Unternehmen mit ihren eigenen nationalen elektronischen Identifizierungssystemen (eID-Systemen) öffentliche Dienste in anderen EU-Ländern benutzen können, sofern dort eine elektronische Identifizierung verwendet wird. Außerdem will sie einen Binnenmarkt für die grenzüberschreitende Verwendung elektronischer Signaturen (eSignaturen) und anderer einschlägiger Vertrauensdienste schaffen, indem sie dafür sorgt, dass diese Dienste grenzübergreifend funktionieren (Interoperabilität) und den gleichen Rechtsstatus haben wie herkömmliche papiergestützte Verfahren. Über Studien im Auftrag der Kommission ist die Abkürzung eIAS für „elektronische Identifizierung, Authentisierung und Signatur“ entstanden; daher wird im Folgenden der Verordnungsentwurf kurz als „EUVO eIAS“ bezeichnet.

Eine Kurzfassung und meine ausführliche Stellungnahme sind unter Ziff. 8.3 und 8.4 abgedruckt.

2.1.1.1
Grundsätzliches/Vorbemerkungen

Obwohl hier viele neue elektronische Vertrauensdienste erstmals definiert werden, ist die erforderliche klare Trennung der Funktionen, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits seit 2006 ständig fordert, immer noch nicht gegeben. Dies kann man bspw. an der Definition der Authentifizierung sehen, die die eigentliche Authentifizierung mit den Anforderungen an ein Siegel vermischt. Ohne eine strikte Trennung der Begriffe und der Funktionen kann es die erforderliche Transparenz für die Bürgerinnen und Bürger nicht geben, die für eine breite Akzeptanz ebenso unabdingbar ist wie eine faire Kostenverteilung.

Verschiedene Qualitätsniveaus bei Signatur, Zeitstempel, Authentisierung und Siegel sind überflüssig (Näheres hierzu s. Ziff. 8.4). Sie führen neben aufwändigen, im Wesentlichen überflüssigen Diskussionen über das jeweils erforderliche Qualitätsniveau zu einer Zersplitterung des Marktes. Das Beispiel der elektronischen Signatur zeigt, dass sich letztendlich weder die qualifizierte noch die fortgeschrittene Signatur durchgesetzt hat.

Die zahlreichen handwerklichen Schwächen des Entwurfs, bspw. bezüglich der Erhaltung des Beweiswertes von Signaturen und bei verschiedenen Definitionen, und seiner Übersetzung ins Deutsche werden hier nicht dargestellt. Sie sind in den im Anhang beigefügten Stellungnahmen enthalten.

2.1.1.2
Elektronische Identifizierung (eID)

2.1.1.2.1
Datenschutzanforderungen

Viele europäische Länder verfügen – wie Deutschland – bereits über ein eigenes eID-System.

2.1.1.2.1.1
Die eID-Funktion des neuen Personalausweises

Der deutsche Ansatz einer eID, der auf dem neuen Personalausweis umgesetzt wurde, ist datenschutzgerecht ausgestaltet: Diese eID erlaubt zum einen die gezielte Übermittlung erforderlicher Identitätsdaten über das Internet an den Diensteanbieter nach vorheriger Zustimmung des Betroffenen

durch Freischaltung der Datenfelder. Dabei kann es sich bspw. um eine Altersverifikation, den Volljährigkeitsnachweis oder eine Wohnortbestätigung handeln. Die Diensteanbieter müssen gegenüber dem Bundesverwaltungsamt begründen, welche Felder sie wofür benötigen; nur für die erforderlichen Daten bekommen sie ein Zertifikat ausgestellt. Dieses Zertifikat ist kostenpflichtig. Zum anderen erhalten Diensteanbieter die Personalausweisnummer nicht im Klartext, sondern in einer für sie spezifisch verschlüsselten Form, sodass sie die Daten einer Person nicht mit denen bei einem anderen Unternehmen vorhandenen abgleichen oder zusammenführen können. Es ist auch möglich, sich mit einem Pseudonym bei einem Diensteanbieter zu identifizieren. Für diesen Anbieter ändert sich das Pseudonym nicht, aber für jeden Anbieter wird ein anderes Pseudonym generiert.

2.1.1.2.1.2
Schwachpunkte des EU-Entwurfs zur eID

Im Gegensatz dazu legt der Entwurf nicht einmal fest, was Identifikationsdaten sind. Eine klare und differenzierte Definition fehlt ebenso wie ein Datenschutzartikel, in dem für diesen Bereich Datenvermeidung und Datensparsamkeit sowie Pseudonymfunktionen verankert werden. Pseudonyme werden in vielen Fällen ausreichen. Hier sind Nachbesserungen dringend erforderlich.

Ferner sollte die Bundesregierung die datenschutzgerechten Regelungen der eID-Funktion des neuen Personalausweises in die europäische Verordnung einbringen. Dies ist bisher zumindest nicht im erforderlichen Umfang erfolgt.

2.1.1.2.2
Notifizierung der deutschen eID-Funktion

Die eID-Funktion des neuen Personalausweises kann nicht nach dem vorliegenden Verordnungsentwurf notifiziert werden. Denn hier wird gefordert, dass die eID rund um die Uhr, ohne besondere Anforderungen an (zusätzliche) Hard- oder Software und kostenlos geprüft werden kann. Der Diensteanbieter benötigt aber in Deutschland ein kostenpflichtiges Zertifikat, sodass zwei der drei Anforderungen nicht erfüllt sind.

2.1.1.2.3
Interoperabilität

Der Verordnungsentwurf sieht Folgendes vor: Wenn in einem Land für den Zugang zu einem Online-Dienst nach nationalem Recht oder nationaler Ver-

waltungspraxis eine elektronische Identifizierung mit einem elektronischen Identifizierungsmittel erforderlich ist, muss für den Zugang zu diesem Dienst jedes in einem anderen Mitgliedsstaat ausgestellte elektronische Identifizierungsmittel, das einem notifizierten eID-System unterliegt, anerkannt und akzeptiert werden. Dies gilt nach der Verordnung auch dann, wenn das nationale eID-System selbst nicht notifiziert ist.

Hier wird deutlich, dass es nicht um die Schaffung eines einzigen – ggf. zusätzlich zu dem nationalen System – grenzübergreifend funktionierenden eID-Systems geht. Vielmehr wird allen Anbietern von Online-Diensten, die ein eID-System verwenden, vorgeschrieben, diesen Dienst für alle notifizierten eID-Systeme zu öffnen. Dies erfordert für jeden einzelnen dieser Online-Dienste einen enormen Aufwand. Und das unabhängig davon, ob der Dienst von Bürgern anderer Länder überhaupt sinnvoll in Anspruch genommen werden kann und ob das fremde eID-System den Anforderungen des Datenschutzes insbesondere bezüglich Datenvermeidung, Datensparsamkeit und pseudonymer Nutzung genügt.

Selbst wenn der Verordnung eine datenschutzgerechte Definition der eID-Funktion zugrunde gelegt würde, wird damit keine Interoperabilität erreicht.

Als Alternative sollte unter Aspekten der Praktikabilität, der Akzeptanz und der Wirtschaftlichkeit über ein EU-weites, datenschutzgerechtes, einheitliches eID-System nachgedacht werden, das ggf. auch neben einem nationalen System – und unabhängig von der jeweiligen nationalen Identitätskarte – genutzt werden kann. Ob damit alle Anforderungen der Verordnung an notifizierte eID-Systeme erfüllt werden können, ohne den Datenschutz zu beeinträchtigen, muss geprüft werden. Die Schaffung einer zentralen Datenbank für die Online-Authentisierung bzw. Identifizierung muss auf jeden Fall vermieden werden.

2.1.1.3
Vertrauensdienste

Die Verordnung definiert eine Reihe von elektronischen Vertrauensdiensten: Signatur, Siegel, Zeitstempel, Dokumente, Zustelldienste und Website-Authentifizierung. Diese Dienste sollen von Vertrauensdiensteanbietern angeboten werden, die für ihre Tätigkeit zertifiziert sein müssen.

Wieder wird hier Interoperabilität versprochen, ohne dass sie erreicht wird. Auch wegen der zahlreichen von der EU-Kommission noch zu erlassenden delegierten und Durchführungs-Rechtsakte, die fast in jeden Artikel aufgenommen wurden, entspricht die Verordnung nicht den Vorgaben des

Art. 290 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV), da sie vielfach wesentliche Bestimmungen betreffen, die in der Verordnung selbst zu regeln sind. Eine Zustimmung der Mitgliedsstaaten zu dieser Verordnung ist wegen der fehlenden Transparenz und Normenklarheit mit einer Blanko-Unterschrift vergleichbar.

Die Beschränkung der Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß darf nicht nur für die Vertrauensdiensteanbieter, sondern muss auch für die akzeptierenden Instanzen und die Datenübermittlung an sie gelten.

Was die konkreten elektronischen Vertrauensdienste angeht, sind viele positive Ansätze erkennbar, die aber oft nicht zu Ende gebracht werden.

2.1.1.3.1
Elektronische Signaturen und elektronische Zeitstempel

Die Verordnung bzw. dieser Abschnitt der Verordnung soll die EU Signaturrichtlinie 1999/93/EG vom 13. Dezember 1999 (ABl. EG 2000, Nr. L 13 S. 12 ff.) ersetzen. Damit gilt dann auch das deutsche Signaturgesetz in der vorliegenden Form nicht mehr.

Positiv ist die sachgerechte, bisher nur in Deutschland verbindliche Prüfung qualifizierter elektronischer Signaturen (QES) auf den Zeitpunkt der Erstellung. Sie entspricht der Gültigkeit der manuellen Unterschrift ab dem Zeitpunkt der Unterzeichnung. Unverständlich bleibt, warum dies nicht auch für fortgeschrittene Signaturen so festgelegt wird. Wobei die fortgeschrittene Signatur aus meiner Sicht überflüssig ist: Zum einen kann ich nicht „ein bisschen“ unterschreiben und meinen Willen kann ich auch nur erklären oder nicht, sodass inhaltlich eine Abschwächung nicht sinnvoll ist. Entweder signiere ich ein Dokument mit einem qualifizierten Verfahren, oder ich halte meine Unterschrift nicht für erforderlich. Zum anderen gibt es keine Prüfverfahren – weder manuell noch automatisiert – für fortgeschrittene Signaturen, Zeitstempel und Siegel.

Fatal sind ferner die Folgen einer Abschwächung der QES in dem Entwurf EUVO eIAS: Die Zertifikatssignaturen der „qualifizierten“ Vertrauensdiensteanbieter und der Root dürfen zukünftig „fortgeschritten“ sein. Und das ohne einen nachvollziehbaren Grund. Damit ist dieser Dienst entgegen seiner Bezeichnung nicht mehr wirklich qualifiziert und das Prüfmodell wird problematisch (die Zertifikatssignaturen sind nicht auf den Zeitpunkt der Erstellung festgelegt).

Dasselbe gilt für die qualifizierten Zeitstempel.

Vor allem aber werden die Verfahren ArchiSig und ArchiSafe, die fortschrittlichen deutschen Konzepte zur Sicherung des Beweiswertes elektronischer Signaturen und zur Archivierung signierter bzw. zeitgestempelter Dokumente, die mit erheblichem Aufwand im Auftrag der Bundesregierung entwickelt wurden, mit den veränderten Regelungen der EU Verordnung nicht mehr einsetzbar sein, wenn es auf den Erhalt der Beweiskraft ankommt. Aber auch eine Beweiswerterhaltung außerhalb dieser Verfahren ist damit nicht mehr zu erzielen.

Die Aufweichungen der bisherigen „alleinigen Kontrolle“ des Schlüsselinhabers werden bei der Zurechnung und den Rechtsfolgen ebenfalls nicht akzeptable Folgen haben.

2.1.1.3.2
Elektronisches Siegel

Nicht jedes elektronische Dokument beinhaltet eine Willenserklärung oder erfordert eine inhaltliche Zustimmung oder gar den Ersatz der manuellen Unterschrift. Auch wenn die Verwendung der QES im deutschen Recht mit den entsprechenden Regelungen in den Verwaltungsverfahrensgesetzen, dem Bürgerlichen Gesetzbuch und der Zivilprozessordnung das nahe legt. Vielmehr geht es oft lediglich darum, dass ein Dokument von dem angegebenen Absender stammt, also authentisch ist, und dass es beim Transport nicht verändert wurde. Es geht also um eine eher technische, keine inhaltliche Signatur, wie sie von meiner Mitarbeiterin schon bei einem Vortrag im Herbst 2009 als „Siegel“ für juristische und als „Paraphe“ für natürliche Personen gefordert wurde. Diese wurde nun mit dem elektronischen Siegel geschaffen. Bedauerlicherweise aber nur für juristische und nicht für natürliche Personen, obwohl sie für letztere in gleicher Weise von Bedeutung ist; bspw. als Bestätigung „habe ich gelesen bzw. gesehen“ und eben nicht „damit bin ich einverstanden“ oder „dem stimme ich zu“, also ohne Zustimmung zum Inhalt.

2.1.1.3.3
Elektronische Dokumente als Vertrauensdienst?

Unklar ist, warum elektronische Dokumente als Vertrauensdienst in die EU VO eIAS aufgenommen wurden. Ein elektronisches Dokument kann aus meiner Sicht lediglich die Basis für einen Vertrauensdienst darstellen, ein Objekt, das bspw. zugestellt, gespeichert oder transportiert wird.

In der Formulierung dieses Abschnitts ist nur von „Originalen oder beglaubigten Kopien für die Erbringung eines von einer öffentlichen Stelle ange-

botenen Online-Dienstes“ die Rede. Die Vertrauensdiensteanbieter werden hier nicht erwähnt. Stattdessen geht es speziell um Dokumente mit einer QES oder einem qualifizierten Siegel der für seine Ausstellung zuständigen Person. Diese liegen eindeutig außerhalb des Wirkungsbereiches der Vertrauensdiensteanbieter, der lediglich die Validierung und Bewahrung elektronischer Signaturen und Siegel von Dokumenten umfasst.

2.1.1.3.4
Website-Authentifizierung

Die Website-Authentifizierung sollte auch für die zahlreichen Websites von natürlichen Personen definiert und umgesetzt werden. Nur so wird sie den Sicherheitsanforderungen und der Realität des Internet gerecht.

2.1.1.4
Weiteres Vorgehen

2.1.1.4.1
Aktivitäten des Hessischen Datenschutzbeauftragten

Die Stellungnahme meines Hauses zu dem Verordnungsentwurf eIAS wurde breit gestreut. Sie war Thema im Europa- und im Datenschutzausschuss des Hessischen Landtages. Eine meiner Mitarbeiterinnen nimmt an der erweiterten Projektgruppe eID-Strategie des IT-Planungsrates teil, in der die nationale eID-Strategie erarbeitet werden soll; hier wurden die im Anhang abgedruckten Stellungnahmen meine Hauses verteilt und eine sehr zurückhaltende Stellungnahme der Kerngruppe zum Verordnungsentwurf vorgelegt.

2.1.1.4.2
Forderungen

Der Entwurf der EU-Verordnung eIAS muss inhaltlich bezüglich der Datenschutzaspekte wesentlich überarbeitet werden. Hier könnten die Regelungen der eID des neuen deutschen Personalausweises wegweisend und zielführend sein. Dazu müssen sie auf EU-Ebene bekannt gemacht und in das Verfahren eingebracht werden. Wenn der bisherige, unklare Begriff „Identitätsdaten“ weiter verwendet wird, besteht die Gefahr, dass diese bald nicht mehr ihre Funktion erfüllen können, da sie nicht mehr unter der alleinigen Verfügungsgewalt der Betroffenen bleiben, sondern zu weit verbreitet werden und dann auch von Dritten im Sinne des Identitätsdiebstahls genutzt werden könnten.

Die guten Ansätze bspw. beim Siegel und der Website-Authentifizierung sollten auch für natürliche Personen zugelassen werden.

Auf verschiedene Qualitätsniveaus sollte der Übersichtlichkeit, Transparenz und Akzeptanz wegen verzichtet werden. Sie sind überflüssig. Die qualifizierten Vertrauensdienste müssen wirklich lückenlos „qualifiziert“ sein, um vertrauenswürdig zu sein und die erforderliche (Rechts-)Sicherheit zu gewährleisten. Der zusätzliche Aufwand hierfür ist vernachlässigbar.

Signaturen, Siegel und Zeitstempel müssen auf Anwender- und auf Zertifikats-Ebene auf den Zeitpunkt der Erstellung geprüft werden.

Falls diese Forderungen nicht durchgesetzt werden können, sollte Deutschland darauf achten, dass die eID des neuen Personalausweises ebenso wie die qualifizierten Signaturen und die mit ihnen verbundenen Verfahren ArchiSig und ArchiSafe zumindest national ohne Einschränkungen oder Verschlechterungen weiter genutzt werden können.

Die Vorgaben, die zur Erreichung der Interoperabilität erforderlich sind, sollten direkt in die VO, ggf. in einen Anhang aufgenommen werden.

Eine Überarbeitung der Definitionen und der Regelungen zur Beweiswerterhaltung ist ebenso erforderlich wie die Beseitigung weiterer handwerklicher Mängel im Verordnungstext selbst und von sinnentstellenden Übersetzungsfehlern in der deutschen Übersetzung.

2.1.1.4.3
Fazit

Der Entwurf der EU-Verordnung eIAS ist mit seinen verschiedenen Vertrauensdiensten ein Schritt in die richtige Richtung, der auch in das nationale E-Government-Gesetz übernommen werden sollte. Gleichwohl sind sowohl konkrete Vorgaben zum Erreichen der Interoperabilität als auch eine gründliche Überarbeitung zur Beseitigung der Schwächen erforderlich.

2.1.2
Dauerbrenner: Anforderung von Personalausweiskopien

Das Fotokopieren von Personalausweisen ist neben den gesetzlich geregelten Fällen nur in wenigen Ausnahmefällen zulässig. In der Regel ist es ausreichend zu vermerken, dass ein gültiger Personalausweis zur Feststellung der Identität vorgelegen hat.

Im vergangenen Berichtsjahr haben sich die Fälle gehäuft, in denen sich Bürger bei meiner Behörde darüber beschwert haben, dass von ihnen bei

Beantragung einer Leistung, der Auskunft bei der SCHUFA etc. die Vorlage einer Kopie ihres Personalausweises verlangt wurde.

Das Personalausweisgesetz in der Fassung vom 22. Dezember 2011 normiert, dass vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Zur Frage der Rechtmäßigkeit der Erstellung von Kopien sagt das Personalausweisgesetz nichts aus. Allerdings gibt es in Spezialgesetzen wie etwa dem Geldwäschegesetz, dem Telekommunikationsgesetz, der Signaturverordnung sowie der Fahrerlaubnisverordnung Vorschriften, die die Vorlage einer Ausweiskopie verlangen. Für Bereiche außerhalb dieser spezialgesetzlichen Regelungen hat das Bundesministerium des Innern mit Blick auf die Erstellung von Kopien von Personalausweisen folgende Rahmenbedingungen formuliert, mit denen den sicherheits- und datenschutzrechtlichen Bedenken gegen die Anfertigung von Ausweiskopien ausreichend Rechnung getragen wird:

- *Die Erstellung einer Kopie muss erforderlich sein. Dabei ist insbesondere zu prüfen, ob nicht die Vorlage des Personalausweises und ggf. die Anfertigung eines entsprechenden Vermerks (z. B. „Personalausweis hat vorgelegen“) ausreichend ist.*
- *Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden.*
- *Die Kopie muss als solche erkennbar sein.*
- *Daten, die nicht zur Identifizierung benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen.*
- *Die Kopie ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist.*
- *Eine automatisierte Speicherung der Ausweisdaten ist nach Personalausweisgesetz unzulässig.*

Für die verschiedenen an meine Dienststelle gerichteten Anfragen ergibt sich daher die unten geschilderte Bewertung.

2.1.2.1
Anforderungen durch Versicherungen

Ein Bürger bat mit seiner Eingabe um datenschutzrechtliche Überprüfung folgenden Sachverhalts: Eine Versicherung fordere Versicherungsnehmer auf, eine Kopie des Personalausweises vorzulegen, dessen Daten dann von der Versicherung gespeichert würden. Der Eingeber wertete dies als Datenschutzverstoß.

Nach Maßgabe des Geldwäschegesetzes (GWG) besteht die Berechtigung, eine Personalausweiskopie im Versicherungsbereich zu verlangen, soweit

es um Lebens- und Unfallversicherungen geht (§ 2 Abs. 1 Nr. 4 GWG). Insoweit besteht für die Versicherer die Pflicht, einen Vertragspartner zu identifizieren (§ 4 Abs. 4 GWG). Da nach diesem Gesetz die durchgeführte Identifizierung zu dokumentieren ist, müssen die Personalausweiskopien gemäß den Aufbewahrungsbestimmungen des GWG auch vorgehalten werden (§ 8 GWG). Die Eingabe bezog sich auf eine Abwicklung im Bereich der Lebensversicherung. Die Erstellung der Personalausweiskopie war daher rechtmäßig.

2.1.2.2
Personalausweiskopien bei der Anforderung von SCHUFA-Selbstauskünften

Verschiedentlich wurde ich gefragt, ob die SCHUFA bei der Beantragung einer Selbstauskunft die Vorlage einer Personalausweiskopie verlangen kann.

Auf dem Bestellformular Datenübersicht nach § 34 BDSG, das die SCHUFA bereitstellt, ist Folgendes zu lesen:

> *Zur Vermeidung von Rückfragen und im Sinne einer schnelleren Bearbeitung sowie zu Ihrer eindeutigen Identifizierung bitten wir Sie, Ihrer Bestellung eine beidseitige Kopie Ihres Ausweisdokuments beizulegen, auf der die Angaben Name, Vorname, Adresse, Geburtsdatum, Geburtsort, und Gültigkeitsdatum gut lesbar sind. Nicht erforderliche Angaben, wie z. B. Nationalität, Augenfarbe und Größe können Sie in Ihrem eigenen Interesse schwärzen.*

In einer Stellungnahme der SCHUFA wird ausgeführt, dass die Auskunft nach § 34 BDSG auch ohne Vorliegen einer Personalausweiskopie erteilt werde, wenn der Betroffene bei der SCHUFA identifiziert werden könne.

Der Düsseldorfer Kreis hat sich mit dieser Problematik befasst und folgende Position vertreten:

> *Ein generelles Vervielfältigungsverbot von Pässen und Personalausweisen würde zu erheblichen Schwierigkeiten bei der praktischen Umsetzung des Auskunftsrechts der Betroffenen nach § 34 BDSG in den Fällen führen, in denen die Vorlage einer Personalausweis- oder Reisepasskopie zum Zwecke der Identitätsnachweises in strittigen Fällen erforderlich ist. Ist die Vorlage einer Ausweis- oder Passkopie erforderlich, sind die Grundsätze der Datensparsamkeit und Erforderlichkeit zu beachten.*

Ich habe das Verlangen nach der Vorlage der Ausweiskopie unter Zugrundlegung der skizzierten Grundsätze dann für gerechtfertigt gehalten, wenn dies zu Identifizierungszwecken notwendig sein sollte und diese Vorgehensweise nicht den Regelfall darstellt.

2.1.2.3
Personalausweiskopien bei der Einholung von anderen Selbstauskünften nach § 34 BDSG

In dieselbe Kategorie gehört die Anfrage einer Betreiberin von Gewinnspielen, die Auskunftsersuchen nach § 34 BDSG über das Internetportal „Selbstauskunft.net“ erhalten hat. Hier wollte die Firma wissen, ob und unter welchen Voraussetzungen sie die Identität eines Anfragers durch Vorlage einer Personalausweiskopie bestätigen lassen kann. Auch hier habe ich die Vorlage einer Personalausweiskopie der anfragenden Gewinnspielteilnehmer nur dann für zulässig gehalten, wenn eine nachweisliche Verwechslungsgefahr besteht. Dem Anfrager gegenüber muss diese Verwechslungsgefahr bei der Bitte um Vorlage der Personalausweiskopie mitgeteilt werden.

Auch habe ich es für erforderlich gehalten, dass der Anfragende darauf hingewiesen wird, dass alle Personalausweisdaten außer Vorname, Name, Geburtsdatum, Anschrift und Gültigkeitsdauer in der Kopie zu schwärzen sind; denn die zusätzlichen Daten sind für eine Identifikation nicht erforderlich. Die Ausweiskopie darf ausschließlich für die Identitätsprüfung verwendet werden und ist danach sicher zu vernichten.

2.1.2.4
Kontrolle von Speditionsmitarbeitern am Frankfurter Flughafen

Im Berichtszeitraum erreichten mich mehrere Eingaben von Speditionsmitarbeitern. Sie berichteten, dass sie bei der Auslieferung bzw. Entgegennahme von Frachtgütern am Frankfurter Flughafen gezwungen würden, hinzunehmen, dass ihr Personalausweis kopiert wird. Eine Rücksprache bei Fraport ergab, dass es dort seit einigen Jahren ein detailliertes Überprüfungssystem gibt, um Betrugs- und Diebstahlsfällen entgegenzuwirken. Dieses System ist von der Polizei, Fraport, der Datenschutzbeauftragten von Fraport und dem Regierungspräsidium Darmstadt – der ehemaligen Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich – erarbeitet worden. Danach folgt die Anlieferung und Abholung von Frachtgut durch Speditionsmitarbeiter einem Kontrollverfahren, in dem Daten des Speditionsmitarbeiters wie Name, Vorname und Geburtsdatum erfasst und mit den Daten des Personalausweises oder eines anderen Legitimationspapiers abgeglichen werden. Von der Erstellung einer Kopie des Bundespersonalausweises ist hier nicht die Rede.

Vielmehr weist auch das Luftfahrtbundesamt in seinen Regularien „Datenschutz und Berechtigung der Anlieferung“ vom 12. März 2012 darauf hin, dass eine Berechtigung zur Erstellung von Kopien nicht existiert.

In diesem Zusammenhang nicht gerechtfertigt ist es, Kopien von Ausweisdokumenten anzufertigen, Fahrerlisten oder -daten zu übermitteln oder personenbezogene Daten zu sammeln. Dies kann nicht nur einen Verstoß gegen datenschutzrechtliche Bestimmungen, sondern auch gegen solche des Personalausweisgesetzes darstellen. Das gilt für alle Beteiligten an der sicheren Lieferkette.

Daraus folgt, dass die Regularien bei der Abholung und Anlieferung von Waren durchaus die oben skizzierten Grundsätze zur Erforderlichkeit der Datenerhebung berücksichtigen. Allerdings scheint es konkret ein Vollzugsdefizit bei der Umsetzung dieser Regeln zu geben. Hier ist Fraport gefordert, durch entsprechende Mitarbeiterschulung für Abhilfe zu sorgen.

2.2
Fachthemen

2.2.1
Hessisches Spielhallengesetz

Das Hessische Spielhallengesetz bedarf noch einiger Präzisierungen, die auch in einer Rechtsverordnung erfolgen können.

2.2.1.1
Bundesweites System für Spielersperren

Am 30. Juni 2012 ist das Hessische Spielhallengesetz in Kraft getreten (Hessisches Spielhallengesetz vom 28. Juni 2012, GVBl. I S. 213). Das Gesetz berücksichtigt nur einen Teil der Einwände, die ich im Gesetzgebungsverfahren geäußert habe.

Zu den Hauptanliegen des Gesetzes zählen der Schutz der Spieler und die Suchtprävention. Zu diesem Zweck werden die Erlaubnisinhaber verpflichtet, an einem bundesweiten Sperrsystem mitzuwirken, in dem vom Spiel ausgeschlossene Spieler registriert werden (§ 6 Abs. 1 Hessisches Spielhallengesetz). In die Sperrdatei dürfen eingetragen 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.

Außerdem dürfen die Dokumente, die zur Sperrung geführt haben, gespeichert werden (§ 11 Abs. 1 Hessisches Spielhallengesetz). An dem Sperrsystem nehmen auch die Spielbanken und die Veranstalter von Sportwetten und Lotterien mit besonderem Gefährdungspotential teil (Art. 1, § 8 Abs. 1 und 2 Erster GlüÄndStV vom 15. Dezember 2011, GVBl. 2012, S. 190 Gliederungs-Nr. 316-33). Die Sperrdatei wird zentral von der für das Glücksspielwesen zuständigen Behörde des Landes Hessen geführt (Art. 1, § 23 Abs. 1 Erster GlüÄndStV).

2.2.1.2
Unbestimmte Kriterien für Fremdsperren

Problematisch ist besonders die in § 6 Abs. 3 Hessisches Spielhallengesetz enthaltene Regelung zur Fremdsperre.

> *§ 6 Abs. 3 Hessisches Spielhallengesetz*
>
> *Die Erlaubnisinhaberin oder der Erlaubnisinhaber sperrt Personen, die dies bei ihr oder ihm beantragen (Selbstsperre) und schließt den 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 (Fremdsperren).*

Die Vorschrift weist dieselben Schwächen auf, wie die Regelung in § 8 Abs. 2 Glücksspielstaatsvertrag (seit 1. Juli 2012 Erster GlüÄndStV), der sie nachgebildet ist.

Unbestimmt bleibt, wer die Dritten sind, die eine Spielersperre herbeiführen können. Daraus resultiert eine erhebliche Missbrauchsgefahr, da nach dieser Vorschrift jeder eine andere Person als spielsüchtig denunzieren könnte.

Es müssten objektivierbare Kriterien benannt werden, nach denen das Personal von einer Suchtgefährdung eines Spielers ausgehen kann. Stattdessen bleibt es dem Personal überlassen, nach eigenen Vorstellungen einen Spieler als suchtgefährdet einzuordnen.

Unklar ist, wie der Erlaubnisinhaber wissen soll, ob die Spieleinsätze außer Verhältnis zum Einkommen und Vermögen des Spielers stehen, da ihm die Einkommens- und Vermögensverhältnisse der Spieler in der Regel nicht bekannt sein dürften.

Dies gilt auch für den Sperrungsgrund, dass ein Spieler seinen finanziellen Verpflichtungen nicht nachkommt. Darüber hinaus ist die Erforderlichkeit ei-

ner Sperre aus einem solchen Grund zweifelhaft. Zum Schutz der Erlaubnisinhaber vor Ausfallrisiken ist die Sperre nicht erforderlich, denn sie erbringen ihre Leistung gegen Vorauszahlung. Soll die Sperre dem Schutz der Spieler dienen, stellt sich die Frage, warum jemand, der finanzielle Verpflichtungen wie z. B. Unterhalts-, Miet- oder Kaufpreiszahlungen nicht erfüllt, vom Glücksspiel in einer Spielhalle ausgeschlossen werden muss.

2.2.1.3
Fehlende Bedingungen für die Aufhebung der Sperren

§ 6 Abs. 5 Hessisches Spielhallengesetz bestimmt lediglich, dass die Sperre frühestens nach einem Jahr auf schriftlichen Antrag des Spielers aufgehoben werden kann. Die Entscheidung über die Aufhebung der Sperre wird an keinerlei Voraussetzungen gebunden, sondern bleibt dem alleinigen Ermessen des Erlaubnisinhabers überlassen. Um Willkürmaßnahmen zu verhindern, müsste zumindest vorgegeben werden, dass die Sperre aufzuheben ist, wenn im Zeitpunkt der Entscheidung kein gesetzlicher Grund vorliegt, der das Verhängen einer erneuten Sperre zuließe.

2.2.1.4
Notwendigkeit konkreter Übermittlungsbeschränkungen

Die Erlaubnisinhaber müssen durch Identitätskontrollen und Abgleich mit der zentralen Sperrdatei die Durchsetzung der Spielersperre gewährleisten (§ 5 Abs. 2 Hessisches Spielhallengesetz). Nach § 11 Abs. 2 Hessisches Spielhallengesetz sind ihnen die in der Sperrdatei gespeicherten Daten im für die Überwachung der Spielersperre erforderlichen Umfang zu übermitteln. Für diesen Zweck dürfte es genügen, die Übermittlung auf die zum Identitätsabgleich notwendigen Daten (§ 11 Abs. 1 Nr. 1 bis 6) und die Tatsache, dass eine Spielersperre eingetragen ist, zu beschränken. Den Grund und die Dauer der Sperre, sowie die meldende Stelle (Nr. 7 bis 9) muss der Erlaubnisinhaber nicht kennen. Die Übermittlungsbefugnis sollte daher entsprechend eingeschränkt werden.

2.2.1.5
Rechtsverordnung

§ 11 Abs. 7 ermächtigt die für das Glücksspielwesen zuständige Behörde, Einzelheiten zur Einrichtung und Ausgestaltung des Sperrsystems zu regeln. Ich erwarte, dass zumindest dort die im Spielhallengesetz selbst nicht berücksichtigten notwendigen Präzisierungen und Einschränkungen noch erfolgen.

2.2.2
Die elektronische Gesundheitskarte mit Lichtbild wird eingeführt

Auch in Hessen ist im Berichtszeitraum die elektronische Gesundheitskarte an die Versicherten ausgeteilt worden. Aufgrund zahlreicher Anfragen und Beschwerden habe ich die aktuelle Verfahrensweise in den hessischen Krankenkassen überprüft. Die Verfahrensweise war datenschutzgerecht ausgestaltet. Zentrale Fragen der künftigen Nutzung der elektronischen Gesundheitskarte sind noch bundesweit offen.

2.2.2.1
Einleitung

§ 291a SGB V regelt, dass die Krankenversichertenkarte „bis spätestens zum 1. Januar 2006“ zu einer elektronischen Gesundheitskarte (eGK) erweitert wird. In den Jahren 2011 bis 2013 wird nunmehr die elektronische Gesundheitskarte tatsächlich an die Versicherten ausgeteilt, schwerpunktmäßig im Berichtszeitraum. Hierzu habe ich zahlreiche Anfragen und Beschwerden erhalten, insbesondere zu den Fragen, inwieweit die Versicherten verpflichtet sind, künftig eine eGK zu verwenden und ihrer Krankenkasse ein Lichtbild für die Erstellung der eGK zur Verfügung zu stellen, ferner, in welchem Umfang und für welche Zwecke in diesem Zusammenhang ihre Daten verarbeitet werden und welche Rechte ihnen zustehen.

2.2.2.2
Aktueller Sachstand

Alle gesetzlich Versicherten erhalten eine elektronische Gesundheitskarte mit Mikroprozessor. Die Karte ist die Basis für den Ausbau einer modernen Informations- und Kommunikationsstruktur im Gesundheitswesen (Telematikinfrastruktur). Sie wird zunächst nur die Funktion der bisherigen Krankenversichertenkarte übernehmen, ist aber technisch bereits so ausgestattet, dass sie schrittweise weitere Anwendungen aufnehmen kann, sobald sich diese Anwendungen in den vorgesehenen Testverfahren bewährt haben und die hierfür erforderliche technische Infrastruktur bei den Leistungserbringern vorhanden ist.

Auf der eGK werden – wie auf der Krankenversichertenkarte – administrative Daten der Versicherten, z. B. Name, Geburtsdatum und Anschrift sowie Angaben zur Krankenversicherung, wie die Krankenversichertennummer und der Versichertenstatus gespeichert. Neu im Vergleich zur Krankenversichertenkarte ist die Angabe zum Geschlecht und die Aufnahme eines

Lichtbildes. Damit sollen Verwechslungen und Missbrauch der Karte soweit wie möglich verhindert werden. Die Rückseite der elektronischen Gesundheitskarte kann für die Europäische Krankenversicherungskarte verwendet werden, die eine unbürokratische Behandlung innerhalb Europas ermöglicht.

2.2.2.3
Die gesetzlichen Regelungen

Die grundlegenden Regelungen – einschließlich detaillierter Festlegungen zum Datenschutz und zur Datensicherheit – wurden bereits 2003 im GKV-Modernisierungsgesetz (Gesetz zur Modernisierung der gesetzlichen Krankenversicherung vom 4. November 2003, BGBl. I S. 2190) getroffen und lediglich in Details später geändert bzw. ergänzt.

Die gesetzlichen Krankenkassen sind nach den o. a. Regelungen verpflichtet, ihre Versicherten mit der eGK auszustatten, die bestimmte Anforderungen erfüllen muss:

- § 290 SGB V enthält Vorgaben zu Inhalt und Verfahren der auf der Gesundheitskarte aufzubringenden Krankenversichertennummer, die durch ihren unveränderbaren Teil eine eindeutige lebenslange Identifizierung des Versicherten ermöglichen soll.
- Die §§ 291, 291a SGB V regeln den Inhalt der eGK. Sie besteht aus einem Pflichtteil, den alle Versicherten nutzen müssen (insbesondere administrative Daten und Verordnungsdaten für das elektronische Rezept), und einem für den Versicherten freiwilligen Teil (insbesondere Notfalldaten, Arzneimitteldokumentation, elektronischer Arztbrief, elektronische Patientenakte, Patientenfach).

  Die Vorschriften regeln darüber hinaus zentrale datenschutzrechtliche Anforderungen an das System der Gesundheitskarte: rechtliche Anforderungen an die Zugriffsmöglichkeit durch die Leistungserbringer und dafür einzusetzende Sicherheitskomponenten (z. B. Heilberufsausweis), Entscheidungsrechte der Versicherten und Maßnahmen des technischen Datenschutzes.

2010 wurde ergänzend in § 291 Abs. 2b SGB V die Verpflichtung der Krankenkassen festgelegt, Dienste anzubieten, mit denen die Leistungserbringer (z. B. Ärzte) die Gültigkeit und die Aktualität der Versichertenstammdaten bei den Krankenkassen online überprüfen und auf der elektronischen Gesundheitskarte aktualisieren können (Gesetz zur Änderung krankenversicherungsrechtlicher und anderer Vorschriften (KVRuaÄndG) vom 24. Juli 2010, BGBl. I S. 983).

Nach den im Berichtszeitraum mit dem Gesetz zur Regelung der Entscheidungslösung im Transplantationsgesetz vom 12. Juli 2012 (BGBl. I S. 1504) beschlossenen Ergänzungen von § 291a SGB V wird die Gesundheitskarte zukünftig auch Erklärungen zur Organ- und Gewebespende sowie Hinweise auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten und Patientenverfügungen nach § 1901a BGB enthalten. Die Versicherten werden hierfür eigenständige PIN-geschützte Zugriffsrechte zum Schreiben, Lesen, Ändern, Sperren und Löschen erhalten.

2.2.2.4
Die Position der Datenschutzbeauftragten

Meine Dienststelle wie auch alle Datenschutzbeauftragten des Bundes und der Länder haben sich intensiv an der Diskussion über die gesetzlichen Regelungen zur eGK beteiligt. Die Datenschutzbeauftragten sind übereingekommen, dass die datenschutzrechtlichen Anforderungen in den Regelungen des GKV-Modernisierungsgesetzes, insbesondere in § 291a SGB V hinreichend berücksichtigt sind und es nunmehr bei dem Ausbau des Projekts darauf ankommt, dass diese Anforderungen auch im Detail angemessen umgesetzt werden (zu den Einzelheiten s. auch http://www.datenschutz.hessen.de/dg003.htm). Von zentraler Bedeutung war hierbei der Aspekt, dass jeder Versicherte selbst entscheiden kann, ob und in welchem Umfang er von den neuen Möglichkeiten der elektronischen Gesundheitskarte – wie z. B. Notfalldaten, Arzneimitteldokumentation und elektronische Patientenakte – Gebrauch machen möchte. Der Versicherte hat darüber hinaus das Recht, seine auf der Karte oder auf zentralen Servern elektronisch gespeicherten Daten einzusehen.

In einer Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom März 2005 wurde Folgendes ausgeführt (http://www.datenschutz.hessen.de/k69e2.htm):

> *Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.*

2.2.2.5
Aktuelle Pläne zur Erweiterung der Anwendungen der eGK

Nach dem derzeitigen Sachstand soll zunächst mit der Einführung der folgenden zusätzlichen Anwendungen begonnen werden (http://www.bmg.bund.de/krankenversicherung/elektronische-gesundheitskarte/funktionen.html):

– Notfalldatensatz (offline)

  Im Notfall kommt es darauf an, dass der Arzt oder Rettungsassistent in kürzester Zeit die erforderlichen Maßnahmen der Notfallrettung ergreift und hierbei möglichst auch wichtige Informationen z. B. über bestehende Vorerkrankungen, Allergien oder Unverträglichkeiten des Versicherten zur Verfügung hat. In der nächsten Ausbaustufe der eGK ist daher vorgesehen, dass der Versicherte wichtige medizinische Daten für die Notfallversorgung auf der Gesundheitskarte speichern lassen kann, wenn er dies wünscht. Im Notfall können diese Daten von Ärzten bzw. Rettungsassistenten dann auch ohne Mitwirkung des Versicherten ausgelesen werden. Die Zugriffe auf den Notfalldatensatz werden protokolliert und sind damit überprüfbar. Der technisch mögliche Zugriff auf die Notfalldaten ohne die PIN des Patienten darf nur dann genutzt werden, wenn die Daten zum Zweck der Notfallversorgung benötigt werden. Will hingegen ein Arzt im Rahmen eines anamnestischen Gesprächs auf die Daten zugreifen, so darf er dies nur nach technischer Autorisierung durch den Versicherten, wie es auch generell für den Zugriff auf Daten der freiwilligen Anwendungen im Gesetz vorgesehen ist.

– Online-Versichertendatenmanagement

  § 291 Abs. 2b Nr. 1 SGB V enthält die gesetzliche Verpflichtung für die Kassen, Dienste für den Online-Abgleich der Versichertenstammdaten anzubieten. Hierbei geht es um den Abgleich der auf der Gesundheitskarte gespeicherten Versichertenstammdaten mit den in den Systemen der Krankenkassen gespeicherten Daten. Mit Hilfe des Online-Abgleichs der Versichertenstammdaten können Daten auf der eGK aktualisiert werden, ohne dass ein Austausch der Karten zwingend erforderlich ist. Im Fall von Verlust oder Diebstahl einer eGK kann zeitnah eine Sperrung der Karte erfolgen, so dass mögliche Fälle von Leistungsmissbrauch besser verhindert werden können.

Hinsichtlich der weiteren zukünftig geplanten neuen Anwendungen und der konkreten Umsetzung der Versichertenrechte (insbesondere bei der lebenslangen elektronischen Patientenakte) sind noch zahlreiche Fragen bezüglich der konkreten datenschutzgerechten Ausgestaltung offen.

2.2.2.6
Funktionen der neuen Karte und Pflichten der Versicherten

Zum Nachweis seines Leistungsanspruchs hat der Versicherte die eGK vor jeder Behandlung dem Leistungserbringer vorzulegen (§ 291 Abs. 2a i. V. m. § 15 Abs. 2 SGB V). Die Karte enthält auch ein Lichtbild.

Die Verpflichtung der Krankenkassen, ein Lichtbild aufzubringen, bestand bereits für die Krankenversichertenkarte (§ 291 Abs. 2 SGB V). Aus wirtschaftlichen Gründen wurde es den Krankenkassen jedoch zugebilligt, das Lichtbild erst mit der eGK einzuführen. Ziel ist es, mit Hilfe des Lichtbildes die missbräuchliche Inanspruchnahme von Leistungen in der GKV zu reduzieren. Gesetzliche Vorgaben zur Qualität des Lichtbildes sowie zum Verfahren der Lichtbildübermittlung des Versicherten enthält § 291 SGB V nicht. Vorgaben zu Größe und Qualität des Lichtbildes finden sich in der von der Gesellschaft für Telematik für die Anwender verbindlich festgelegten Spezifikation der eGK (http://www.gematik.de). Für die Festlegung des Verfahrens der Lichtbildübermittlung ist jede einzelne Krankenkasse zuständig. Nicht alle Versicherten erhalten eine Gesundheitskarte mit Lichtbild. Nach § 291 Abs. 2 SGB V erhalten Kinder und Jugendliche bis zur Vollendung des 15. Lebensjahres sowie Personen, deren Mitwirkung an der Erstellung eines Lichtbilds nicht möglich ist, eine eGK ohne Lichtbild. Übermittelt der Versicherte der Krankenkasse kein Lichtbild, so kann diese aber für ihn auch keine eGK ausstellen, da das Lichtbild – außer in den o. a. Fällen – zwingend Bestandteil der eGK ist.

2.2.2.7
Zur Verfahrensweise in Hessen

Bis auf eine Krankenkasse haben alle Krankenkassen in meinem Zuständigkeitsbereich 2012 mit der Austeilung der eGK begonnen. Bei diesen Krankenkassen habe ich mich informiert, wie sie die Einführung der eGK in der Praxis umsetzen.

2.2.2.7.1
Information der Versicherten

Gem. § 291a Abs. 3 SGB V muss die Krankenkasse die Versicherten spätestens bei der Versendung der Karte umfassend über deren Funktionsweise einschließlich der Art der auf ihr oder durch sie zu erhebenden, zu verarbeitenden oder zu nutzenden personenbezogenen Daten informieren. Da die Einzelheiten bezüglich der künftigen Anwendungen noch nicht ab-

schließend geklärt sind, kann sich diese Informationspflicht nur auf den aktuellen Sachstand beziehen. In diesem Sinne haben alle Krankenkassen im Rahmen der Lichtbildbeschaffung und Versendung der eGK mit persönlichen Anschreiben, Flyern, Internetauftritt und ihren Kundenzeitschriften ihre Mitglieder über die eGK und die damit zusammenhängende Verarbeitung ihrer Daten informiert.

2.2.2.7.2
Lichtbildbeschaffung und Ausstellung der eGK

Für die Ausstellung einer eGK wird zusätzlich zu den administrativen Daten, die auch bisher auf der Krankenversichertenkarte gespeichert waren, ein Lichtbild des Versicherten benötigt. Zur Beschaffung und Weiterverarbeitung des Lichtbilds haben alle in meinem Zuständigkeitsbereich liegenden Krankenkassen Verträge mit externen Dienstleistern geschlossen. Dabei werden jeweils zwei Verfahren zur Übermittlung des Lichtbilds angeboten: Entweder der Versicherte übermittelt das Foto per Post mit einem Lichtbildformular oder er nutzt die Möglichkeit, das Lichtbild über eine spezielle Internetseite hochzuladen. Die Lichtbilder werden dann vor der Weiterverarbeitung von den beauftragten Dienstleistern geprüft und bei Beanstandungen z. B. der Qualität vom Versicherten neu angefordert.

Im zweiten Schritt nach der Lichtbildbeschaffung erfolgt die Herstellung und der Versand der eGK an die Versicherten durch beauftragte Dienstleister. Technische Probleme wie z. B. fehlerhafte Karten sind dabei bei den von mir befragten Krankenkassen nicht aufgetreten. Bis Ende September 2012 waren bereits über 70 % der gesetzlich Versicherten in Hessen mit einer eGK ausgestattet. Spätestens Ende 2013 soll dann jeder Versicherte mit einer eGK ausgestattet sein.

Nach Auskunft der Krankenkassen sind bislang kaum Fälle aufgetreten, in denen ein Versicherter gezielt ein falsches Bild (z. B. eines Prominenten) übersandt hat, und von 1,4 Mio. Versicherten waren nur ca. 300 (Stand September 2012) (zunächst) nicht bereit, ein Lichtbild einzusenden. Diesen Versicherten wird keine eGK ausgestellt. Wie nach dem Auslaufen der bisherigen Krankenversichertenkarte dann verfahren wird, wenn Versicherte ohne eGK eine Leistung der gesetzlichen Krankenversicherung in Anspruch nehmen wollen, ist im Einzelnen noch nicht geklärt.

2.2.2.7.3
Informationen über den Inhalt der eGK

§ 291a SGB V legt fest, dass bezüglich der eGK § 6c BDSG Anwendung findet. Diese 2001 neu geschaffene Vorschrift im BDSG greift das Problem auf, dass mobile personenbezogene Speicher- und Verarbeitungsmedien nicht nur als Datenträger dienen, sondern auf ihnen Daten auch verarbeitet werden können, ohne dass diese Verarbeitungen von den Betroffenen unmittelbar nachvollzogen werden können (Smart Cards). Bei den künftigen Anwendungen der eGK – d. h. noch nicht bei dem aktuellen Sachstand, wird das der Fall sein.

§ 6c Abs. 2 BDSG verpflichtet die Karten ausgebende Stelle, die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung zu stellen. Mit dieser Verpflichtung soll es dem Betroffenen ermöglicht werden, die auf dem Speichermedium ablaufende Verarbeitung seiner Daten nachzuvollziehen, denn ohne technische Hilfsmittel ist er nicht in der Lage zu erkennen, welche Daten auf der Karte gespeichert sind. Diese Transparenz ist zur Wahrung des Rechts auf informationelle Selbstbestimmung notwendig, da die personenbezogenen Daten auch von Dritten ausgelesen und verarbeitet werden können.

Die Verpflichtung richtet sich an die Krankenkassen. Sie haben die infrastrukturellen Voraussetzungen zu schaffen, damit der Versicherte sein Auskunftsrecht wahrnehmen kann. Die Krankenkasse darf jedoch nicht die Möglichkeit haben, über von ihr zur Verfügung gestellte Lesegeräte selbst Einsicht in die Daten zu nehmen. In der Diskussion sind öffentlich zugängliche Terminals, mit Hilfe derer die Versicherten ihr Auskunftsrecht wahrnehmen können. Auf meine Nachfrage haben die Krankenkassen mitgeteilt, dass derzeit noch keine derartigen Terminals zur Verfügung stehen, aber der Einsatz von Lesegeräten für die Versicherten entsprechend der gesetzlichen Regelung für die künftigen Anwendungen vorbereitet wird.

Insgesamt habe ich bei meiner stichprobenhaften Prüfung des Verfahrens bei der Austeilung der eGK keine Anhaltspunkte für evtl. Verstöße gegen datenschutzrechtliche Vorschriften festgestellt.

2.2.3
Telefondatenüberwachung von Personal- bzw. Betriebsratsmitgliedern

Die Kontrolle des Kommunikationsverhaltens von Personal- und Betriebsräten ist nur sehr eingeschränkt zulässig. Bei einem Diensthandy, das sowohl

dienstlich als auch für Gespräche des Personal- oder Betriebsrates in dieser Funktion genutzt wird, können Geräte mit zwei SIM-Karten oder die getrennte Abrechnung, die von einigen Telefondienstleistern angeboten werden, eine praktikable Lösung sein.

Die Geschäftsführung eines kommunalen Zweckverbandes fragte an, ob der Personalratsvorsitzende zu Recht fordern könne, dass keine Einzelverbindungsnachweise für sein dienstlich zur Verfügung gestelltes Mobiltelefon erstellt werden dürfen, da für ihn ein generelles Verbot der Überwachung seiner Telekommunikation gelte.

Im Grundsatz dürfen Personal- bzw. Betriebsratsmitglieder in der Ausübung ihrer Tätigkeit nicht gestört oder behindert werden (§ 64 Abs. 1 Hessisches Personalvertretungsgesetz (HPVG), § 78 Abs. 1 Betriebsverfassungsgesetz (BetrVG)). Es soll sichergestellt werden, dass Personal- bzw. Betriebsratsmitglieder ihrer Tätigkeit mit der gebotenen Unabhängigkeit nachgehen können. Dazu gehört auch, dass ein gewisses Maß an Vertraulichkeit ihrer Gespräche und auch der Gesprächspartner gewahrt werden muss, da sonst die Gefahr besteht, dass sich Beschäftigte nicht mit ihren Problemen an die Interessenvertretung wenden. Hieraus folgt, dass eine umfassende Kontrolle der Mitglieder der Mitarbeitervertretungen und deren Kommunikationsverhalten grundsätzlich unzulässig ist.

Bei Anschlüssen, die jedoch von Betriebs- bzw. Personalratsmitgliedern genutzt werden, die für diese Tätigkeit nicht vollständig freigestellt sind, ergibt sich die Problematik, dass nicht ohne Weiteres unterschieden werden kann, welche Telefonate rein dienstlicher Natur sind und welche aufgrund der Betriebs- bzw. Personalratstätigkeit geführt wurden.

Da es im Ausgangsfall um Einzelverbindungsnachweise für ein dienstlich bereitgestelltes Mobiltelefon ging, habe ich empfohlen, zunächst dafür Sorge zu tragen, dass diese Unterscheidung möglich ist. Dies lässt sich z. B. mit zwei unterschiedlichen SIM-Karten oder mit zwei verschiedenen Abrechnungskonten für eine SIM-Karte erreichen.

Diese Vorgehensweise ermöglicht es dem Arbeitgeber, die Kontrolle der Telefonkosten jeweils getrennt durchzuführen. So können die unterschiedlichen Maßstäbe, die bei der Kontrolle normaler Dienstgespräche einerseits und der von Gesprächen des Personal- bzw. Betriebsrates andererseits anzulegen sind, zur Geltung gebracht werden.

Dabei ist die Erstellung von Einzelverbindungsnachweisen auch für die Gespräche der Mitarbeiter, die diese in ihrer Funktion als Betriebs- bzw. Personalrat führen, nicht gänzlich ausgeschlossen. Nach § 42 Abs. 1 HPVG bzw. § 40 BetrVG hat der Dienstherr bzw. der Arbeitgeber für die Kosten von Per-

sonal- bzw. Betriebsratsarbeit aufzukommen. Vor diesem Hintergrund kann es gerechtfertigt sein, dass der Arbeitgeber bei entsprechendem Anlass, wie z. B. der Verursachung von überhöhten Kosten durch Ferngespräche oder durch Gespräche mit dem Mobiltelefon, anhand von Einzelverbindungsnachweisen kontrolliert, ob ein Missbrauch stattfindet. Je nach Lage des Falles muss hier aber auch abgewogen werden, ob ein um die letzten drei Ziffern gekürzter Einzelverbindungsnachweis ausreicht oder ob tatsächlich ein solcher mit den vollständigen angewählten Rufnummern erforderlich ist.

2.2.4
Auskunftsanspruch des Kunden eines Gasanbieters

Kunden von Energielieferanten haben auch nach Beendigung eines Vertragsverhältnisses einen Anspruch auf Auskunft über die zu ihrer Person gespeicherten Daten. Gelegentlich ist es nötig, Betroffene bei der Durchsetzung ihres Auskunftsverlangens zu unterstützen.

Ein Einwohner aus Köln hat sich an seinen in Hessen ansässigen ehemaligen Gaslieferanten gewandt und um Auskunft nach § 34 BDSG gebeten.

Er schrieb, er habe keine Antwort erhalten. Die Hotline würde telefonische Auskunftsersuchen automatisch beenden. E-Mails blieben unbeantwortet. Er legte mir eine Kopie seines per E-Mail gestellten Auskunftsverlangens vor und bat mich um Unterstützung bei seinem Anliegen.

Ich schrieb den Gasanbieter an und konfrontierte ihn mit dem unbeantwortet gebliebenen Auskunftsersuchen. Ich bat ihn, nunmehr gem. § 38 Abs. 3 BDSG mir die gewünschte Auskunft innerhalb einer bestimmten Frist zu erteilen. Außerdem bat ich um Mitteilung der Gründe, weshalb das Auskunftsersuchen nicht beantwortet wurde. Ich kündigte an, die Auskunft an den Betroffenen weiterzuleiten.

Das Unternehmen meldete sich nach wenigen Tagen. Es schrieb, leider liege ihm die E-Mail des Betroffenen nicht vor. Es müsse sich um ein Versehen handeln, dafür entschuldigte es sich.

Es folgte die Auskunft über die Belieferungszeiten und die Vertragsdauer bis zum 30. Juni 2011. Da keine entsprechende Zustimmung vorliege, finde keine Verwendung der Daten zu Marketingzwecken statt. Die Daten würden nur noch zur Erfüllung gesetzlicher Archivierungspflichten nach §§ 147 AO und 257 HGB aufbewahrt.

Die Antwort reichte ich an den Anfrager weiter. Seinem Auskunftsverlangen war damit Rechnung getragen.

2.2.5
Auskunftsanspruch des (Mit-)Eigentümers über zu seiner Wohnung aufgenommene Daten

Auch bei den zum Zustand einer Wohnung vor Kanalbauarbeiten zum Zwecke der Beweissicherung aufgenommenen Daten handelt es sich um personenbezogene Daten des Eigentümers. Dem Betroffenen steht ein Auskunftsanspruch zu.

Eine kommunale Kanalbaufirma ließ vor der Durchführung von Kanalbauarbeiten an einer Straße durch ein Ingenieurbüro eine Bestandsaufnahme über den baulichen Zustand der angrenzenden Immobilien durchführen. Dies geschah zur Beweissicherung und zur Geltendmachung oder Abwehr späterer Schadensersatzansprüche, die durch die Tiefbaumaßnahme an der Immobilie hätten entstehen können. Das von dem kommunalen Kanalbauunternehmen beauftragte Ingenieurbüro führte eine Begehung der Wohnung und des Grundstückes des als Miteigentümer Betroffenen durch und fertigte ein Protokoll und mehrere Fotografien an. Im Vorfeld bat der Miteigentümer um eine Kopie der Dokumentation. Dies wurde ihm zugesagt. Daraufhin erteilte er sein Einverständnis für die Datenerhebung.

Danach bat er über die Hausverwaltung um Auskunft über die zu seinem Eigentum festgehaltenen Daten. Nach Rücksprache mit dem Ingenieurbüro, das die Beweissicherung vorgenommen hatte, bezifferte die Hausverwaltung die Kosten für eine Kopie der Dokumentation auf 500 EUR. Er hielt dies für prohibitiv und bat mich, ihn bei der Durchsetzung seines Rechtes auf kostenlose Auskunft über die zu seiner Person gespeicherten Daten zu unterstützen. Zuvor hatte er noch versucht, sein Recht bei dem kommunalen Kanalbauunternehmen selbst durchzusetzen. Doch dieses beschied ihn, es handele sich nicht um personenbezogene Daten.

Dem kommunalen Bauunternehmen habe ich mitgeteilt, dass es sich natürlich um personenbezogene Daten handelt. Auch sachliche Verhältnisse – hier also z. B. der Wert oder die Schäden an einer Immobilie –, die einer bestimmbaren Person zugeordnet werden können, sind personenbezogene Daten.

Der Betroffene hatte sich mit seinem Auskunftsanspruch zutreffend an das kommunale Kanalbauunternehmen gewendet, denn das Ingenieurbüro war nur in dessen Auftrag tätig. Da das Kanalbauunternehmen zwar eine öffentliche Stelle nach dem HDSG ist, aber am Wettbewerb teilnimmt, gilt über § 3 Abs. 6 HDSG für den Auskunftsanspruch § 34 BDSG. Die Auskunft ist nach § 34 Abs. 8 Satz 1 BDSG unentgeltlich.

Das Angebot, gegen eine Kostenerstattung von 500 EUR eine Kopie der Dokumentation herzustellen, war nicht mit der Unentgeltlichkeit der Auskunft vereinbar.

Ich verlangte von dem Unternehmen deshalb, dem Anfrager umgehend Auskunft gem. § 34 BDSG erteilen, hilfsweise ihm Akteneinsicht zu gewähren.

Dem Betroffenen ging es nämlich nicht unbedingt um eine Kopie der gesamten Dokumentation. Er verlangte nur eine Information darüber, ob und welche Schäden an der Immobilie festgestellt wurden. Deshalb war anzunehmen, dass dem Verlangen auch durch die Gewährung von Akteneinsicht abgeholfen werden konnte.

Fast postwendend meldete sich der Betroffene, ihm sei kostenlos Akteneinsicht gewährt worden. Sein Informationsrecht sei umfassend erfüllt worden.

2.3
Entwicklungen und Empfehlungen im Bereich der Technik

2.3.1
Nutzung von Smartphones für dienstliche bzw. berufliche Zwecke

In den vergangenen Jahren gab es größere Veränderungen auf dem Markt für mobile Endgeräte im Unternehmens-/Behördeneinsatz, die aus meiner Sicht zu einer Verschlechterung für den Datenschutz geführt haben. Immer wieder erreichen mich Anfragen, ob und wie die neuen Produkte – insbesondere Smartphones und Tablet-Computer – genutzt werden können.

In den letzten Jahren hat es einen Umbruch bei der Mobilkommunikation gegeben. Aus dem Handy wurde mit einem Umweg über PDAs das Smartphone und als besondere Ausprägung bei der reinen Datenverarbeitung der Tablet-PC. Es handelt sich um Computer mit einer Leistungsfähigkeit, die bis vor kurzem PCs vorbehalten waren. Der Chic liegt in der intuitiven Bedienung, die sich für den Nutzer wohltuend von den bekannten Rechnern abhebt. Nicht zuletzt aus diesem Grund gibt es dringliche Wünsche, die Geräte auch im dienstlichen Umfeld nutzen zu können.

Die Smartphones wurden aber nicht für den Einsatz im dienstlichen Umfeld konzipiert. Es gibt daher eine Reihe von Einschränkungen, die sich als Hindernis erweisen. Ich habe eine Handreichung erarbeitet, in der auf die gängigen Ausprägungen von Smartphones eingegangen wird und datenschutzrechtliche Fragestellungen und Probleme benannt werden. Sie finden sie auf meiner Homepage (www.datenschutz.hessen.de, Rubrik Fachthemen, technische Orientierungshilfen).

2.3.2
Orientierungshilfen Smart-Metering, IPv6 und Mandantenfähigkeit

Auch im Jahr 2012 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, teilweise zusammen mit dem Düsseldorfer Kreis, Orientierungshilfen erarbeitet und veröffentlicht. Sie behandeln die Themen Smart-Metering, IPv6 und Mandantenfähigkeit aus Sicht des Datenschutzes.

2.3.2.1
Smart-Metering

Beim Smart-Metering geht es um intelligente Verbrauchszähler beispielsweise für Strom oder Gas. In der Orientierungshilfe wird versucht aufzuzeigen, wie zentrale Forderungen des Datenschutzes erfüllt werden können. Dazu werden verschiedene Anwendungsfälle (Use Cases) betrachtet und Anforderungen an die Technik und Abläufe aus Sicht des Datenschutzes formuliert. Die Orientierungshilfe ist auf meiner Homepage veröffentlicht (www.datenschutz.hessen.de, Rubrik Fachthemen, technische Orientierungshilfen).

2.3.2.2
IPv6

IPv6 steht für Internet-Protokoll Version 6. Dabei handelt es sich um die Fortentwicklung des IP-Protokolls in der Version 4, das bis vor Kurzem alleinige technische Basis des Internets war. Eine wesentliche Neuerung ist dabei die Möglichkeit, jedes vernetzte Gerät mit einer eigenen, leider nicht zwangsläufig änderbaren, Kommunikationsadresse zu versehen. Hieraus und aus anderen Aspekten ergeben sich Risiken. Das Protokoll eröffnet aber auch neue Möglichkeiten. In der Orientierungshilfe werden Risiken, Chancen und Lösungsansätze beschrieben, die sich aus IPv6 ergeben. Die Orientierungshilfe ist auf meiner Homepage veröffentlicht (www.datenschutz.hessen.de, Rubrik Fachthemen, technische Orientierungshilfen).

2.3.2.3
Mandantenfähigkeit

Unter Mandantenfähigkeit versteht man, wenn in einem IT-System die Daten von im datenschutzrechtlichen Sinne verantwortlichen Stellen so

gegeneinander abgeschottet werden können, dass wechselseitige Datenzugriffe nicht oder nur unter ganz restriktiven rechtlich zulässigen Bedingungen technisch möglich sind. In der Orientierungshilfe wird der Begriff präzisiert und es werden verschiedene technische Lösungsmöglichkeiten dargestellt. Die Orientierungshilfe ist auf meiner Homepage veröffentlicht (www.datenschutz.hessen.de, Rubrik Fachthemen, technische Orientierungshilfen).

3. Datenschutz im öffentlichen Bereich

3.1
Europa

3.1.1
Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrnehmung der Interessen der Landesdatenschutzbeauftragten in der Europäischen Kontrollinstanz des Schengener Informationssystems übertragen. Meine Mitarbeiterin hat im Berichtszeitraum an vier Sitzungen in Brüssel teilgenommen. Der Beitrag stellt die Arbeitsschwerpunkte im Jahr 2012 dar.

3.1.1.1
Schengener Informationssystem der zweiten Generation (SIS II)

Nach neuesten Informationen soll der Start von SIS II in der ersten Hälfte des Jahres 2013 erfolgen. Aufgrund dieser Zeitangabe hat die Gemeinsame Kontrollinstanz (GKI) beschlossen – anders als im 40. Tätigkeitsbericht (Ziff. 2.1.1) berichtet – keine Kontrollen des zurzeit im Betrieb befindlichen SIS I plus mehr vorzunehmen, sondern sich auf die datenschutzrechtliche Begleitung der Migration von Daten aus dem SIS I plus nach SIS II zu konzentrieren. Nach jetzigem Stand (Entwurf für eine Verordnung für die Migration von SIS I plus zu SIS II vom 30. April 2012 [KOM 2012, 81 endgültig]) ist vorgesehen, dass die GKI in Abstimmung mit dem Europäischen Datenschutzbeauftragten für die Überwachung der Migration solange zuständig bleibt, bis einer der Schengen-Mitgliedstaaten das SIS II als Informationssystem übernommen hat. Ab diesem Zeitpunkt soll nicht mehr das Schengener Durchführungsübereinkommen (SDÜ), sondern die für das SIS II verabschiedeten Rechtsgrundlagen Anwendung finden. Die datenschutzrechtliche Kontrolle liegt dann nicht mehr bei der GKI, sondern beim Europäischen Datenschutzbeauftragten (z. B. Art. 61 des Beschlusses über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) vom 12. Juni 2007, ABl. L 205 S. 63) und den Kontrollinstanzen der Mitgliedstaaten. Zur Formalisierung der Zusammenarbeit ist vorgesehen, dass sich die nationalen Kontrollinstanzen und der Europäische Datenschutzbeauftragte mindestens zweimal im Jahr treffen.

Art. 62 Abs. 3 Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)

Die nationalen Kontrollinstanzen und der Europäische Datenschutzbeauftragte treffen zu diesem Zweck mindestens zweimal jährlich zusammen. Die Kosten und die Ausrichtung dieser Sitzung gehen zu Lasten des Europäischen Datenschutzbeauftragten. In der ersten Sitzung wird eine Geschäftsordnung aufgenommen. 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.

3.1.1.2
Gemeinsame Überprüfungen der Ausschreibungen zur Festnahme im Schengener Informationssystem

Im letzten Tätigkeitsbericht (Ziff. 2.1.2) hatte ich berichtet, dass in allen dem Schengener Durchführungsübereinkommen (SDÜ) angeschlossenen Staaten eine Überprüfung der Ausschreibung nach Art. 95 SDÜ vorgenommen wird. Es geht 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.

Stellvertretend für die anderen Bundesländer habe ich bei verschiedenen Staatsanwaltschaften etwa 30 Akten geprüft, denen Ausschreibungen im SIS nach Art. 95 SDÜ zugrunde lagen. Ich habe dabei keine datenschutzrechtlichen Mängel festgestellt. Nach den Aussagen unserer Gesprächspartner ist insbesondere die frühzeitige Löschung der Ausschreibungen im SIS nach Wegfall der Voraussetzungen schon deshalb gewährleistet, weil sie im ureigensten Interesse der Richter und Staatsanwälte liegt, da eine zu lange Aufbewahrung eventuell strafrechtliche Konsequenzen (z. B: Freiheitsberaubung) für den Einzelnen haben könnte.

Da noch nicht alle Datenschutzbehörden der Schengen-Staaten die erforderlichen Informationen geliefert haben, steht eine endgültige Auswertung der Fragebögen noch aus.

3.1.1.3
Fragebogen zum Auskunftsrecht

Die Möglichkeit der Geltendmachung des Rechts auf Auskunft, Löschung und Berichtigung stellt einen wichtigen Bestandteil des im Grundgesetz enthaltenen Rechts auf informationelle Selbstbestimmung und auf europä-

ischer Ebene des in Artikel 8 der Charta der Grundrechte postulierten Schutzes personenbezogener Daten dar. Um sich ein Bild über die Realisierung des Rechts auf Auskunft und anderer Rechte von Betroffenen in den einzelnen Schengen-Staaten zu machen, hat die GKI beschlossen, in einem Fragebogen dazu verschiedene Informationen zu erheben.

Das SDÜ sieht vor, dass jede Person unabhängig von ihrem Aufenthaltsort in jedem Schengen-Mitgliedstaat das Recht auf Auskunft, Berichtigung, Löschung der über sie selbst im SIS gespeicherten Daten besitzt.

Art. 109 Abs. 1 SDÜ

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

Art. 110 SDÜ

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

Die Rechte der Betroffenen ergeben sich also aus dem nationalen Recht desjenigen Staates, auf dessen Hoheitsgebiet die Rechte geltend gemacht werden. Wird Auskunft in Deutschland begehrt, richtet sich das Auskunftsgesuch an das Bundeskriminalamt als nationale Zentralstelle oder an den Bundesbeauftragten für Datenschutz und Informationsfreiheit. Stellt dieser fest, dass es sich bei der ausschreibenden Behörde um eine Landesbehörde handelt, lässt er die erforderlichen Anfragen durch die zuständige Landesdatenschutzbehörde vornehmen. Stammt die Ausschreibung von der Behörde eines anderen Schengen-Staates, muss der ausländischen Stelle vor Auskunftserteilung Gelegenheit zur Stellungnahme gegeben werden. Nach der Systematik des SDÜ bleibt die Erteilung der Auskunft also bei der Stelle, an die sich der Betroffene gewandt hat; sie geht nicht auf die ausschreibende Stelle über.

Die Auskunftserteilung kann nur aus den in Art. 109 Abs. 2 genannten Gründen verweigert werden.

Art. 109 Abs. 2 SDÜ

Die Auskunftserteilung an den Betroffenen unterbleibt, wenn dies zur Durchführung einer rechtmäßigen Aufgabe im Zusammenhang mit der Ausschreibung oder zum Schutz der Rechte und Freiheiten Dritter unerlässlich ist. Sie unterbleibt immer während der Ausschreibung zur verdeckten Registrierung.

Weitere sich evtl. aus dem nationalen Recht ergebende Auskunftsverweigerungsgründe können nicht herangezogen werden, da es sich um eine abschließende Vorschrift handelt.

Fest steht bis jetzt, dass Deutschland eines der Länder mit den meisten Anfragen von Betroffenen ist: 2010 waren es 751; 2011 waren es bereits 1.097 Fälle. Leider konnte die für das Schengener Informationssystem zuständige Kontaktstelle im Bundeskriminalamt (SIRENE) bis jetzt keine Zahlen darüber liefern, in wie viel Fällen eine Auskunft erteilt bzw. abgelehnt wurde.

Da sich das Auskunftsrecht nach dem jeweiligen nationalen Recht richtet, ist zu erwarten, dass sich auch aufgrund der unterschiedlichen rechtlichen Situation Unterschiede zwischen den einzelnen Schengen-Staaten ergeben.

3.1.2
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.

3.1.2.1
Neues Konzept für Analysearbeitsdateien

Im 40. Tätigkeitsbericht (Ziff. 2.2.2) hatte ich berichtet, dass die Struktur der von Europol betriebenen Analysearbeitsdateien umgestellt werden soll. Ich hatte dargestellt, dass dadurch Probleme im Hinblick auf die Zweckbestimmung der Dateien sowie die Einhaltung von Lösch- und Prüffristen entstehen, da die Regelungen des Europol-Beschlusses nach dem Wortlaut nicht mehr anwendbar sind. In verschiedenen Gesprächen mit Vertretern von Europol wurde eine Lösung entwickelt, nach der die erforderlichen datenschutzrechtlichen Vorkehrungen im Text der jeweiligen Analysearbeitsdatei festgelegt werden. Mit dem jetzt realisierten Modell konnte sich die Gemeinsame Kontrollinstanz (GKI) einverstanden erklären. Dabei spielte eine Rolle, dass es demnächst eine neue Rechtsgrundlage für Europol geben soll, die die neue Struktur – soweit sie beibehalten werden soll – widerspiegeln muss.

3.1.2.2
Einbeziehung von Europol in das Terrorist Finance Tracking Program (TFTP)

Ich hatte im 40. Tätigkeitsbericht (Ziff. 2.2.1) berichtet, dass die GKI Kontrollen bei Europol durchgeführt hat, in denen es um die Rolle Europols im Rahmen des TFTP-Abkommens ging. Dabei handelte es sich um ein Abkommen, das die Übermittlung von Zahlungsverkehrsdaten von der EU an die USA und deren Verarbeitung dort vorsieht.

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.

Da an diesen Kontrollberichten ein starkes öffentliches Interesse besteht, hat die GKI beschlossen, einen öffentlich zugänglichen Bericht und einen als geheim eingestuften Bericht anzufertigen. Allerdings haben verschiedene Institutionen, wie die entsprechenden Ausschüsse nationaler Parlamente und insbesondere des europäischen Parlaments, den Wunsch geäußert, auch den als geheim eingestuften Bericht zu erhalten, um sich ein vollständiges Bild über die datenschutzrechtlichen Probleme machen zu können.

Die GKI hat nunmehr hinsichtlich des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des europäischen Parlaments entschieden, dass der eingestufte Bericht an zur Geheimhaltung verpflichtete Personen unter bestimmten Konditionen herausgegeben werden darf.

3.1.2.3
Neue Rechtsgrundlage für Europol

Geplant ist, dass die Kommission in der ersten Hälfte des Jahres 2012 einen Vorschlag für eine neue Rechtsgrundlage für die Tätigkeit von Europol vorlegt. Bisher bestand die Rechtsgrundlage von Europol in dem Europol-Beschluss, der am 1. Januar 2010 in Kraft getreten ist. Nach dem Vertrag von Lissabon ist nach Art. 88 Abs. 2 des Vertrages über die Arbeitsweise der europäischen Union (AEUV i. d. F. der Bekanntmachung vom 9. Mai 2008, ABl. C115 S. 47) die Handlungsform der Verordnung zu wählen. Diese wird auf Vorschlag der Kommission oder auf Initiative eines Viertels der Mitgliedsstaaten von Rat und Parlament im ordentlichen Gesetzgebungsverfahren erlassen, womit erstmals für Europol eine Aufwertung des europäischen Parlaments zum „Mitgesetzgeber“ erfolgt. Weitere Vorteile der Änderungen durch den Vertrag von Lissabon bestehen darin, dass zum ersten

Mal besondere Regelungen über den gerichtlichen Rechtsschutz beim europäischen Gerichtshof vorzusehen sind (Art. 263 Abs. 4 AEUV) und die Kontrolle von Europol durch das europäische Parlament und die nationalen Parlamente geregelt werden muss (Art. 2 Satz 3 AEUV).

Diese geplanten bereichsspezifischen Regelungen für Europol passen zur Systematik des Entwurfs für eine Richtlinie des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr vom 25. Dezember 2012 (KOM 2012/10 endgültig; Ziff. 1.2.1). Dieser Entwurf für eine Datenschutzrichtlinie nimmt in Art. 2 Abs. 3 Einrichtungen und Organe der Europäischen Union – wie z. B. Europol – von seinem Anwendungsbereich aus. Bleibt es dabei, besteht für Europol ein eigenes Datenschutzregime, das keinen Rückgriff auf die in der Datenschutzrichtlinie vorgesehenen allgemeinen Datenschutzregelungen zulässt.

Die GKI hat sich im Vorfeld der demnächst zu erwartenden Verordnung gegenüber der Kommission geäußert und einige aus ihrer Sicht wichtige Forderungen aufgestellt:

- Das Ziel, Europol zu einem „information hub“ (Drehscheibe für Informationen) auszubauen, muss die unterschiedlichen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten der Mitgliedsstaaten und von Europol berücksichtigen.
- Sollte das neue Konzept für die Analysearbeitsdateien beibehalten werden, muss sich dies in der Rechtsgrundlage widerspiegeln.
- Im Rahmen des Auskunftsrechts ist sicherzustellen, dass während des Auskunftsverfahrens die erforderlichen Unterlagen bei Europol beibehalten werden.
- Die datenschutzrechtliche Kontrolle von Europol muss weiter gewährleistet sein. Ungeachtet der Frage, ob das bisherige Modell der GKI beibehalten oder andere Formen aufgegriffen werden (z. B. eine gemeinsame Kontrollinstanz für die verschiedenen Informationssysteme, wie Schengen, Eurodac, Zoll), ist sicher zu stellen, dass die nationalen Datenschutzbehörden wie bisher in die Kontrolle einbezogen werden. Da es sich bei den durch Europol verarbeiteten Daten zum größten Teil um Daten der Mitgliedstaaten handelt, ist deren maßgebliche Beteiligung an der Kontrolle wichtig.

3.2
Bund

3.2.1
Bundesmeldegesetz

Der Gesetzentwurf zur Fortentwicklung des Meldewesens hat seit dem im Jahr 2011 vorgelegten Regierungsentwurf in den parlamentarischen Beratungen des Bundestages erhebliche Verschlechterungen erfahren. Es bleibt zu hoffen, dass die von Datenschutzbeauftragten vorgebrachten Kritikpunkte wenigstens teilweise in den Beratungen des Vermittlungsausschusses Berücksichtigung finden.

Die Föderalismusreform I hat das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Mit der Vorlage des Gesetzes zur Fortentwicklung des Meldewesens am 16. November 2011 hat der Bund diese Gesetzgebungskompetenz ausgefüllt, indem er das Melderechtsrahmengesetz aus dem Jahr 1980 mit den Landesmeldegesetzen in einem Bundesgesetz zusammenführt (BTDrucks. 17/7746).

Im Gesetzentwurf der Bundesregierung waren einige Forderungen der Datenschutzbeauftragten unberücksichtigt geblieben, wie etwa die Abschaffung der Hotelmeldepflicht oder der Verzicht auf die Mitwirkung des Wohnungsgebers bei der Anmeldung. Auch die Forderung nach einem Opt-In-Verfahren beim automatisierten Abruf eigener Meldedaten fand keine Berücksichtigung.

Allerdings sah der Regierungsentwurf zu den einfachen Melderegisterauskünften datenschutzfreundliche Regelungen vor. So sollten gem. § 44 Abs. 3 Nr. 2 des Gesetzentwurfs Melderegisterauskünfte zu Werbezwecken sowie für den Adresshandel nur dann erteilt werden dürfen, wenn die betroffene Person in die Übermittlung für jeweils diesen Zweck eingewilligt hat. In der Begründung zu § 44 Abs. 3 Nr. 2 heißt es:

> *Die in Absatz 3 Nummer 2 neu formulierte Voraussetzung für die Zulässigkeit dient dem stärkeren Schutz der betroffenen Person bei der Verwendung ihrer Daten für die genannten Zwecke. So wird gewährleistet, dass – den Regelungen in § 28 Absatz 3 BDSG entsprechend – keine Auskünfte ohne Beteiligung der betroffenen Person für Zwecke der Werbung und des Adresshandels erteilt werden. Der Anfragende muss die Einwilligung der betroffenen Person für Zwecke der Werbung und des Adresshandels nachweisen, außer diese Information liegt der Meldebehörde bereits vor.*

Im Laufe der parlamentarischen Beratungen hat gerade diese Norm eine wundersame Wandlung erfahren, die dann in einer Nacht- und Nebelaktion von einer guten Handvoll Abgeordneter des Bundestages am 22. Juni 2012

verabschiedet wurde. Aus der ursprünglich vorgesehenen Einwilligungslösung wurde eine Widerspruchslösung, die nochmals Einschränkungen unterliegen sollte. Das Widerspruchsrecht gegen eine Melderegisterauskunft zu Werbezwecken oder zu Zwecken des Adresshandels sollte nämlich dann nicht gelten, wenn eine Firma die Auskunft lediglich zur Korrektur vorhandener Datenbestände erhalten wollte. Damit war eine ursprünglich daten- und verbraucherschutzfreundliche Regelung nahezu ins Gegenteil verkehrt worden.

Diese Entwicklung löste in der Bevölkerung einen Sturm der Entrüstung aus; zahlreiche Beschwerden gingen auch bei mir ein.

Die Datenschutzbeauftragten des Bundes und der Länder verständigten sich auf gemeinsame Positionen und darauf, die Innenminister ihrer Länder zu bitten, das Gesetz in der vom Bundestag beschlossenen Form im Bundesrat zu stoppen. Am 22. August 2012 fassten sie mit dem Titel „Melderecht datenschutzkonform gestalten!“ eine gemeinsame Entschließung (Ziff. 6.7), die zunächst die Rückgängigmachung der Auskünfte zu Werbezwecken und zu Zwecken des Adresshandels zum Inhalt hatte, die aber auch die oben angesprochenen Punkte wie Verzicht auf Hotelmeldepflicht und auf die Mitwirkung des Wohnungsgebers an der Meldepflicht beinhaltete. Weiterhin forderten sie eine stärkere Ausgestaltung der Zweckbindung für Daten, die aufgrund von Melderegisterauskünften übermittelt werden. Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Abrufs sollte nach der Forderung der Datenschutzkonferenz nur möglich sein, wenn die betroffene Person dieser Form der Auskunftserteilung nicht widerspricht.

Ich habe die Gelegenheit genutzt, den Hessischen Innenminister auf weitere Defizite des Gesetzentwurfs hinzuweisen, und ihn gebeten, auch diese Punkte in das weitere Verfahren einzubringen. Im Einzelnen handelte es sich um folgende Vorschläge:

– Für den Abruf der eigenen Meldedaten über das Internet (§ 10 des Gesetzentwurfs) sollte ein Opt-In-Verfahren mit Nachweis des Besitzes eines Identitätsdokuments, das zur sicheren elektronischen Identitätsfeststellung geeignet ist, vorgesehen werden. Wegen der hohen Gefährdung und des Umfangs der übermittelten Daten sollte die Auskunft an den Betroffenen über das Internet zunächst für alle Bürger gesperrt sein. Interessierten Bürgern kann – ggf. nach Aufklärung über die Risiken und die zur Absicherung getroffenen Maßnahmen – auf ihren persönlichen Antrag im Meldeamt nach Vorlage eines gültigen Identitätsdokuments, das zur sicheren elektronischen Identitätsfeststellung geeignet ist, der Zugang frei geschaltet werden (Opt-In-Verfahren).

– Melderegisterauskünfte in besonderen Fällen nach § 50 des Gesetzentwurfs (Auskünfte an Parteien zu Wahlwerbezwecken, an Mandatsträger, Presse oder Rundfunk über Alters- und Ehejubiläen sowie Adressbuchverlage) sollten nach meiner Auffassung nur mit Einwilligung der Meldepflichtigen zulässig sein. Die Erfahrungen meiner Behörde haben gezeigt, dass dies dem Bedürfnis Vieler in der Bevölkerung entspricht.

Die Hessische Landesregierung hat frühzeitig signalisiert, dass sie jedenfalls die Regelung der einfachen Melderegisterauskunft zu Werbezwecken und zu Zwecken des Adresshandels in der vom Bundestag verabschiedeten Form nicht mittragen werde. So gehörte Hessen neben Nordrhein-Westfalen, Sachsen, Bayern, Brandenburg, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt und Thüringen zu den Ländern, die zum Gesetz zur Fortentwicklung des Meldewesens am 19. September 2012 einen Antrag im Bundesrat einbrachten, mit dem Ziel den Vermittlungsausschuss anzurufen. Der Antrag hat zum Inhalt, dass für die Melderegisterauskünfte zu den Zwecken des Adresshandels und der Werbung wieder die Einwilligung der Betroffenen vorliegen muss. Auch sieht er eine Stärkung der Zweckbindung für die so übermittelten Daten vor.

Am 21. September 2012 hat der Bundesrat beschlossen, den Vermittlungsausschuss anzurufen. Der Beschluss greift den o. g. Antrag auf und schlägt eine Änderung des § 44 (einfache Melderegisterauskunft) dergestalt vor, dass für die Weitergabe zu Werbezwecken und für Zwecke des Adresshandels die Einwilligung der betroffenen Personen vorliegen muss. In der Begründung heißt es, dass das durch den Bundestag beschlossene Gesetz zur Fortentwicklung des Meldewesens dem grundgesetzlich geschützten Recht auf informationelle Selbstbestimmung nicht in hinreichendem Maße Rechnung trage. Die jetzt vorgeschlagenen Änderungen führten die Vorschriften im Wesentlichen auf die von der Bundesregierung unter Berücksichtigung des Anliegens des Bundesrates formulierten Regelungen zurück.

Die weitergehenden Vorschläge der Datenschutzbeauftragten fanden in dem Beschluss des Vermittlungsausschusses leider keine Berücksichtigung.

Bis zum Ende des Berichtszeitraums hat sich der Vermittlungsausschuss noch nicht mit dem Bundesmeldegesetz befasst.

3.3
Hessen

3.3.1
Querschnitt

3.3.1.1
Ein Rahmen zur Nutzung von facebook durch hessische Behörden

Das soziale Netzwerk facebook ist auch in Deutschland weit verbreitet. Es gibt viele Bürger, die facebook ausgiebig nutzen, aber außerhalb des sozialen Netzwerkes im Internet kaum noch unterwegs sind. Es soll eine Möglichkeit dargestellt werden, wie die öffentliche Verwaltung in Hessen nur in facebook aktive Bürger erreichen kann, ohne gegen Datenschutzprinzipien verstoßen zu müssen.

3.3.1.1.1
Allgemeine Anmerkungen

3.3.1.1.1.1
Soziale Netzwerke

Seit einigen Jahren haben sich soziale Netzwerke etabliert. Sie sind Teil des sog. web 2.0, in dem die Nutzer sich aktiv einbringen. Die Entwicklung startete mit einer ganzen Reihe von Anbietern, von denen Schüler-VZ, Studi-VZ, Wer-kennt-wen oder XING in Deutschland am bekanntesten waren. Seit einigen Jahren hat sich facebook, aus den USA kommend (2012 ca. 16 Millionen Nutzer) in Deutschland als Marktführer positioniert.

In jüngeren Bevölkerungsgruppen gehört facebook zum Alltag, Kommunikation findet hier fast ausschließlich über die Nutzung sozialer Netzwerke statt. Diese Gruppen können über das Internet nur noch erreicht oder mobilisiert werden, wenn man facebook nutzt.

Neben den sozialen Netzwerken immanenten Datenschutzproblemen zwischen den Nutzern (beispielsweise zu freizügig gesetzte Zugriffsrechte, üble Nachrede u. Ä.) ergeben sich weitere Datenschutzprobleme aus den Geschäftsmodellen. Es ist das Ziel der Anbieter sozialer Netzwerke, möglichst viele Daten zu den Nutzenden zu sammeln, um diese Daten beispielsweise für gezielte Werbung zu vermarkten.

Die Nutzungsbedingungen gerade von facebook sind unzweifelhaft schwer verständlich und für den Nutzer kaum transparent. Viele Millionen Nutzer haben sich aber für facebook entschieden und nutzen es in großem Maße

in Kenntnis oder Unkenntnis der Rahmenbedingungen. Dieser Tatsache können sich auch öffentliche Stellen nicht verschließen.

3.3.1.1.1.2
Wie facebook Daten sammelt

Facebook sammelt Daten über verschiedene Wege. Für die weiteren Betrachtungen sind zwei Komponenten wichtig, bei denen Behörden eine Rolle spielen können.

Dies sind zum einen die sogenannten „Social Plug-Ins“ und andererseits die „Fan-Pages“ bei facebook.

3.3.1.1.1.2.1
Social Plug-in

Social-Plug-Ins sind Programme, die ein soziales Netzwerk zur Verfügung stellt und die auf fremden Webseiten, beispielsweise der Homepage einer Behörde, eingebunden werden. Im Fall von facebook ist dies der „gefällt-mir“-Button. Das Plug-In wird in der ursprünglich von facebook vorgesehenen Ausprägung auf interessanten Seiten eines Internetangebots platziert, so dass es bei facebook registrierte Personen, aber auch jeder andere Besucher der Seite, direkt anklicken können, wenn ihnen die Seite gefallen hat.

In der von facebook gegenwärtig bereit gestellten Form hat das Plug-In jedoch Folgen, die datenschutzrechtlich nicht akzeptabel sind. Bereits beim Aufruf der Seite wird der Programmcode ausgeführt und facebook erfährt von jedem Besuch der Seite, nicht nur durch das Drücken des Buttons. Falls der Besucher noch nie den Internetauftritt von facebook aufgerufen hat, wird die IP-Adresse und die gerade besuchte Seite an facebook übertragen. Handelt es sich um einen facebook-Nutzer, so sind auf dessen Rechner Cookies gespeichert, deren Daten an facebook gehen. In diesem Fall ist facebook der Rechner und damit in aller Regel auch die Person bekannt, die diese Seite besucht. Der Nutzer hat keine Kontrolle über die Weitergabe der Daten, da vor der Übertragung seine Einwilligung nicht eingeholt wird.

Auch wenn nicht alle rechtlichen Fragen abschließend geklärt sind, kann man feststellen, dass der Nutzer keine Kontrolle über die Datenübertragung an facebook hat. Um dieses Defizit weitgehend auszugleichen, hat man die sogenannte „Doppelklick-Lösung“ gefunden. Der Programmcode steht zwischenzeitlich in verschiedenen Varianten im Internet zur Verfügung. Bei dieser Lösung ist das Plug-In nicht direkt auf der Webseite eingebunden. Stattdessen ist ein Button vorhanden, den man drücken muss, wenn der Programmcode für den eigentlichen „gefällt-mir“-Button geladen werden

soll. Erst nach diesem ersten Klick wird der Programmcode mit den oben dargestellten Implikationen geladen. Die Webseitenbetreiber geben dabei vor dem ersten Klick Erläuterungen zu den Datenübertragungen an facebook. Mit dieser Lösung wird erreicht, dass nicht schon beim Aufruf einer Seite Daten an facebook übertragen werden, sondern erst, wenn der Nutzer willentlich durch seinen ersten Klick den „gefällt-mir"-Button aktiviert. Ein facebook-Nutzer, der seinen Freunden etwas sagen will, kann das mit zwei Klicks tun.

Die Einbindung eines Social-Plug-In mit einer Doppelklick-Lösung, bei der ein Besucher vor dem ersten Klick über die folgende Datenübertragung unterrichtet wird, halte ich im Gegensatz zur direkten Einbindung eines Social-Plug-In für datenschutzgerecht.

3.3.1.1.1.2.2
Fanpage

Facebook bietet ferner Behörden und anderen Institutionen an, auf den Servern von facebook und als Teil der facebook-Site eigene Angebote zu platzieren. Nutzer, die eine Fanpage besuchen, sind facebook bekannt. Was sie auf facebook tun, wird umfassend protokolliert. Wenn also Nutzende auf die Fanpage einer Institution beispielsweise einer Kommune gehen, so ist dies für facebook genau nachvollziehbar. Das betrifft auch Daten, die Nutzende in facebook als Kommentar oder auf andere Weise eintragen, wobei die Daten mit großer Wahrscheinlichkeit auch auf außereuropäischen Servern gespeichert werden.

Allerdings haben sich Nutzende bei ihrer Registrierung gegenüber facebook mit diesem Vorgehen einverstanden erklärt, wobei man sich jedoch fragen kann, ob angesichts des Umfangs der AGBs eine informierte Einwilligung tatsächlich möglich ist.

Die in meinem 40. Tätigkeitsbericht unter Ziff. 8.10 abgedruckte Entschließung der Datenschutzbeauftragten des Bundes und der Länder zu sozialen Netzwerken enthält die Empfehlung, dass öffentliche Stellen auf Plattformen wie facebook etc. keine Profilseiten oder Fanpages einrichten sollten. Zu anderen Nutzungsformen ist damit nichts gesagt.

3.3.1.1.2
Konsequenzen für Behörden

Für Behörden gilt es zu beachten:

– Die Verwaltung darf niemanden dazu veranlassen, Spuren bei facebook zu hinterlassen.

– Die Verwaltung darf niemanden, auch keinen facebook-Nutzenden, dazu zwingen, Verwaltungsdaten bei facebook bekannt zu geben.

D. h. es dürfen über facebook keine unmittelbaren Interaktionen zwischen Verwaltung und Bürger stattfinden. Das schließt z. B. die Bereitstellung von Formularen aus oder die Abgabe von Bewertungen.

Andererseits ist aber nicht ausgeschlossen, dass eine Behörde facebook-Nutzende, die anders mit Informationen gar nicht mehr erreicht werden könnten, über sonstige Angebote informiert. Dass der facebook-Nutzende dabei die oben genannten Spuren hinterlässt, nimmt dieser ja billigend in Kauf. Für Fanpages kommt deshalb nur eine Lösung in Frage, bei der alle Informationen der Fanpage auch auf der eigentlichen Homepage zu finden sind. Die Fanpage stellt somit eine Untermenge der Daten bereit, die sich auf der Homepage befinden. Die facebook-Nutzenden dürfen auch keine Einträge auf der Fanpage vornehmen können. Sollte eine Reaktion erwünscht sein, so muss diese auf der eigentlichen Homepage erfolgen.

Bezüglich der Social-Plug-Ins kommt für Behörden nur die beschriebene Doppel-Klick-Lösung in Frage.

3.3.1.1.3
Fanpages der Polizei – Öffentlichkeitsfahndung

Auch für die Polizei gibt es verschiedene Bereiche, für die über die Nutzung einer Fanpage nachgedacht wird oder dies auch schon erfolgt. Als Anwendungsgebiete kommen zum einen die klassischen Themen wie Informationen zu spezifischen Fragen aber auch Nachwuchswerbung in Betracht. Eine spezifische Nutzung im Bereich der Polizei ist auch der Einsatz im Zusammenhang mit Öffentlichkeitsfahndungen.

Die Brisanz der Öffentlichkeitsfahndung – erst recht unter der Nutzung von Internetangeboten – wird schon seit langem thematisiert. Grundlage ist die Regelung des § 131 Abs. 3 StPO.

§ 131 Abs. 3 StPO

Bei einer Straftat von erheblicher Bedeutung können in den Fällen der Absätze 1 und 2 der Richter und die Staatsanwaltschaft auch Öffentlichkeitsfahndungen veranlassen, wenn andere Formen der Aufenthaltsermittlung erheblich weniger Erfolg versprechend oder wesentlich erschwert wären. Unter den gleichen Voraussetzungen steht diese Befugnis bei Gefahr im Verzug und wenn der Richter oder die Staatsanwaltschaft nicht rechtzeitig erreichbar ist, auch den Ermittlungspersonen der Staatsanwaltschaft (§ 152 des Gerichtsverfassungsgesetzes) zu. In den Fällen des Satzes 2 ist die Entscheidung der Staatsanwaltschaft unverzüglich herbeizuführen. Die Anordnung tritt außer Kraft, wenn diese Bestätigung nicht binnen 24 Stunden erfolgt.

Details sind in den Richtlinien für das Strafverfahren und Bußgeldverfahren (RiStBV) geregelt. Dabei handelt es sich um eine Verwaltungsvorschrift, die deshalb einerseits den Anwendungsbereich der StPO Regelung nicht erweitern kann, andererseits aber den Ermittlungsbehörden den Rahmen für ihr Handeln näher umschreibt. Zur Öffentlichkeitsfahndung gibt es zudem eine weitere Erläuterung durch einen Runderlass des Justizministeriums „Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung im Rahmen von Strafverfahren“ vom 21. Oktober 2010 (Justizministerialblatt 2010 S. 341 ff.). Neben Erläuterungen zum Einsatz der Öffentlichkeitsfahndung unter Berücksichtigung des Verhältnismäßigkeitsprinzips gibt es dort auch einige Ausführungen zur Nutzung des Internets.

> *3.2 Nutzung des Internets*
>
> *Um die Aufmerksamkeit der Internet-Nutzer für die Öffentlichkeitsfahndung zu erlangen, ist es zweckmäßig, die staatlichen Fahndungsaufrufe im Internet auf speziellen Seiten – etwa der Polizei – zu bündeln. Private Internetanbieter sollen grundsätzlich nicht eingeschaltet werden.*
>
> *Sobald das Fahndungsziel erreicht ist oder die Ausschreibungsvoraussetzungen aus sonstigen Gründen nicht mehr vorliegen, ist die Nutzung des Internets zu Fahndungszwecken unverzüglich zu beenden. Darüber hinaus sind Internetfahndungen von der Staatsanwaltschaft – in den Fällen der Nr. 2.4 von der Vollstreckungsbehörde – regelmäßig, spätestens in halbjährlichen Abständen, hinsichtlich des weiteren Vorliegens der Ausschreibungsvoraussetzungen, insbesondere der weiteren Erfolgsaussichten dieser Fahndungsmethode, zu prüfen.*

Auf dieser Grundlage hat es in Hessen inzwischen einige Fahndungen auf einer Fanpage gegeben. Dabei hat die Polizei ihr Vorgehen mit mir abgestimmt. Entscheidend sind dabei vor allem zwei Punkte:

- Auf der Fanpage erfolgt im Wesentlichen ein Hinweis, dass die Polizei zu einem bestimmten Ereignis nach Personen fahndet. Um Bilder und Details auf dem Bildschirm des Nutzenden darzustellen, werden i-frames (kurz für inlineframes) genutzt. Dabei handelt es sich um Rahmen (engl. Frames), die auf der Fanpage-Seite für die Anzeige von Bildern oder anderen Daten definiert werden, deren Inhalt jedoch von einer anderen Quelle, hier der Homepage der Polizei, auf den Rechner geladen werden. Die auf dem Bildschirm dargestellten Bilder oder Details werden direkt von der Homepage der Polizei geladen; sie werden nicht über den Server von facebook geleitet.
- Es wird auf die Internet-Seite der Polizei und insbesondere auf das Angebot der sog. Online-Wache verwiesen. Auf diesem Weg ist es möglich, der Polizei Informationen zukommen zu lassen, ohne dass Dritte in der Lage sind, dieses zur Kenntnis zu nehmen.

3.3.2
Justiz und Polizei

3.3.2.1
Prüfung des Einsatzes der Quellen-TKÜ

Auch in Hessen kam im Rahmen von Ermittlungsverfahren die Software der Firma DigiTask zum Einsatz. Meine Überprüfung ergab, dass für die Realisierung der „Quellen-TKÜ“ noch erheblicher Nachbesserungsbedarf besteht.

Die sog. Quellen-TKÜ ist eine Reaktion auf die zunehmende Verbreitung verschlüsselter Kommunikation sowie auf die Telefonie im Internet. Die klassische Form der Überwachung der Telekommunikation durch Mithören oder -schneiden der Gesprächsinhalte verschlüsselter Kommunikation ist dabei unmöglich oder zumindest sinnlos. Für die neue Methode wird auf dem Computer, mit der die zu überwachende Kommunikation getätigt wird, ein Programm installiert, welches die Kommunikation vor der Verschlüsselung mitschneidet und an die Ermittlungsbehörde übermittelt.

Im Anschluss an die bundesweite Diskussion zur Durchführung von Maßnahmen der „Quellen-TKÜ“ habe ich mich seit Ende 2011 ebenfalls mit der Thematik befasst. Dabei habe ich mich beschränkt auf die Organisation des Verfahrens bei der Polizei – insbesondere im Landeskriminalamt – sowie die Auswertung der durch die Software der Fa. DigiTask ausgeleiteten Daten in drei der vier in Hessen erfolgten Einsätze dieser Software. Grundlage meiner Überprüfung waren dabei die in einem Gespräch beim LKA gegenüber meinen Mitarbeitern gemachten Angaben, den in der Folge dazu vom LKA erstellten Unterlagen, ein Schriftwechsel mit dem Landespolizeipräsidium sowie Antworten auf verschiedene Landtagsanfragen. Bei meiner Beurteilung habe ich zudem die Feststellungen einzelner Datenschutzbeauftragter des Bundes und anderer Länder, soweit sie mir zugänglich waren und sich mit grundsätzlichen Fragestellungen – über den Einzelfall hinaus – beschäftigen, mit einbezogen.

3.3.2.1.1
Fehlende Rechtsgrundlage in der Strafprozessordnung

Für den Einsatz der Quellen-TKÜ im Rahmen eines Strafverfahrens existiert derzeit keine ausreichende Rechtsgrundlage.

In diesem Sinne hatte sich schon die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 16./17. März 2011 geäußert (vgl. 40. Tätigkeitsbericht, Ziff. 8.2). Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist

durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts im Urteil vom 27. Februar 2008 zur Online-Durchsuchung (NJW 2008, S. 822 bis 837) entsprochen.

Die Strafprozessordnung enthält keine Regelung, die diesen Anforderungen gerecht wird. Im grundrechtsrelevanten Bereich muss der Gesetzgeber alle wesentlichen Vorgaben selbst treffen. Es reicht nicht aus, wenn derartige Schutzvorkehrungen nur im Rahmen eines Gerichtsbeschlusses auf der Grundlage von §§ 100a, 100b StPO angeordnet werden. Vielmehr müssen die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben und technischen Vorkehrungen gesetzlich verankert sein.

Für den präventiven Einsatz ist seit 2010 mit § 15b HSOG im Prinzip eine Rechtsgrundlage vorhanden. Allerdings sind auch hier die notwendigen Rahmenbedingungen nicht sehr konkret festgelegt.

§ 15b HSOG

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

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

(2) Es ist technisch sicherzustellen, dass

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

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

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

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

Die Protokolldaten dürfen nur verwendet werden, um der betroffenen Person oder einer hierzu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme nach Abs. 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des

auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, wenn sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

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

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

3.3.2.1.2
Die überprüften hessischen Fälle

Die Quellen-TKÜ kam im Zusammenhang mit Ermittlungsverfahren in Hessen in vier Fällen zur Anwendung. Jedem Einsatz lag eine richterliche Anordnung zugrunde. Meine Überprüfung dieser Fälle bezieht sich im Kern auf die Fragestellung, ob der Einsatz der entsprechenden Software durch die Polizei jeweils in dem Rahmen erfolgte, der durch die richterlichen Überwachungsanordnungen vorgegeben war. Ein weiteres Augenmerk richtete sich auf die allgemeine Organisation der Einsätze – insbesondere im Zusammenhang mit der Beschaffung der Software und Vorbereitung des Einsatzes.

Grundsätzlich sind die Ergebnisse selbstverständlich auch relevant für die Durchführung entsprechender Maßnahmen auf Grundlage des § 15b HSOG.

3.3.2.1.2.1
Vorgaben der richterlichen Überwachungsanordnungen

Gegenstand meiner Prüfung war ausdrücklich nicht, ob im Einzelfall die Voraussetzungen für die richterlichen Anordnungen vorlagen (unabhängig von der Frage, ob § 100a StPO als Rechtsgrundlage überhaupt anwendbar ist), sondern ich habe die Umsetzung der angeordneten Maßnahmen überprüft. Insbesondere lag der Fokus darauf, ob die formulierten Rahmenbedingungen für einen solchen Software-Einsatz eingehalten worden sind.

Fall 1 (Anordnung im August 2007)
„Überwachung und Aufzeichnung der Internetkommunikation bzgl. des durch den Beschuldigten bei XXX genutzten Computers.“

Fall 2 (Anordnung im März 2009)
„Überwachung und Aufzeichnung der Telekommunikation für den Anschluss XXX.“

Im Fall 2 gab es zumindest im Antrag der Staatsanwaltschaft konkretere Ausführungen, was in der Vorstellung der Ermittlungsbehörden möglich sein sollte:

„Mit umfasst von dieser Anordnung ist auch die Direktanwahl der Mailbox und der technischen Schaltung.

Angeordnet wird insbesondere auch die Überwachung und Aufzeichnung der über den oben genannten Anschluss geführten verschlüsselten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen im Rahmen einer Fernsteuerung.

Auch insoweit sind nur solche Maßnahmen zulässig, die der Überwachung der Telekommunikation dienen und die für die technische Umsetzung der Überwachung zwingend erforderlich sind. Unzulässig sind die Durchsuchung eines Computers nach bestimmten auf diesen gespeicherten Daten sowie das Kopieren und Übertragen von Daten von einem Computer, die nicht der Telekommunikation des Beschuldigten über das Internet mittels voice-over-IP betreffen. Auch das Abhören von Gesprächen, die außerhalb eines Telekommunikationsvorgangs im Sinne des § 100a StPO erfolgen, ist unzulässig."

Fall 3 (Anordnung im Januar 2010)

„... die Überwachung und Aufzeichnung der verschlüsselten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen im Rahmen einer Fernsteuerung in dem nach der Telekommunikations- Überwachungsverordnung zulässigem Umfang für folgende Anschlüsse XXX angeordnet.

Es sind nur solche Maßnahmen zulässig, die der Überwachung der Telekommunikation dienen und die für die technische Umsetzung der Überwachung zwingend erforderlich sind. Unzulässig sind die Durchsuchung eines Computers nach bestimmten auf diesem gespeicherten Daten sowie das Kopieren und Übertragen von Daten von einem Computer, die nicht die Telekommunikation des Beschuldigten über das Internet mittels Voice-over-IP betreffen. Auch das Abhören von Gesprächen, die Außerhalb eines Telekommunikationsvorgangs im Sinne des § 100a StPO erfolgen, ist unzulässig. Das Betreten der Wohnung des Betroffenen zum Zweck der Installation der Quellen-TKÜ wird nicht genehmigt."

Fall 4 (Anordnung im November 2010)

„Überwachung und Aufnahme der Telekommunikation auf Tonträger für nachbenannten Anschluss XXX mittels Installation einer Software, die eine unverschlüsselte Überwachung ermöglichen."

Inwieweit die Formulierungen durch die konkrete Antragstellung von Seiten der Staatsanwaltschaft bzw. durch Anregungen der Polizei beeinflusst wurden, ist mir nicht bekannt. Unabhängig davon, dass der eigentliche Gegenstand der Anordnungen eher nicht konkret umschrieben ist, enthalten die Anordnungen mit Ausnahme im Fall 3 keine Aussage zu den näheren Umständen und zur technischen Organisation der Maßnahme.

Ob die vorhandenen Vorgaben für den Einsatz der Quellen-TKÜ aus den richterlichen Anordnungen eingehalten worden sind, lässt sich (im Nachhinein) nur eingeschränkt feststellen, da nicht mehr nachvollzogen werden kann, was die konkret eingesetzte Software leisten konnte.

3.3.2.1.2.2
Organisation der durchgeführten Maßnahmen

In der Besprechung beim LKA sowie durch die in der Folge überlassenen Unterlagen, die dort zu den durchgeführten Maßnahmen (noch) vorhanden waren bzw. im November 2011 als Reaktion auf die allgemeine Diskussion der Problematik erstellt worden sind, wurde dargestellt, dass für vier Ermittlungsverfahren die Quellen-TKÜ durchgeführt wurde. In einem Fall (hier ist auch der Zoll involviert) erfolgte die Durchführung durch das BKA, in einem weiteren Fall durch das Bayerische LKA. Grund dafür war, dass in Hessen die Kapazitäten zum entsprechenden Zeitpunkt für eine Quellen-TKÜ nicht vorhanden waren. Das bezieht sich sowohl auf die technischen als auch auf die personellen Anforderungen.

3.3.2.1.2.2.1
Auftragsvergabe

Bei der Fa. DigiTask wurde, jeweils bezogen auf die Inhalte der richterlichen Anordnung, eine speziell zugeschnittene Software samt benötigter Hardware bestellt.

Von DigiTask wurde jeweils auch ein Server bezogen, auf dem die ausgeleiteten Daten gespeichert wurden. Nach Beendigung der Maßnahme gingen die Server zurück an DigiTask. Vorher wurden die Festplatten mit den gespeicherten Daten ausgebaut, da sie Eigentum der Polizei waren. Formal sind sie Teil der Ermittlungsakte, da sie Beweismittel im Verfahren sind.

Der schriftliche Auftrag gab die Abläufe und Leistungen nur unzureichend wieder.

3.3.2.1.2.2.2
Abnahme

Vor dem Einsatz der Software erfolgte eine Abnahme in den Räumen der Fa. DigiTask. Dabei wurde von der Fa. DigiTask jeweils die Funktionalität nur vorgeführt. Es gibt keine Abnahmeprotokolle.

Nach Auskunft der Mitarbeiter beim LKA wurde bei dieser Abnahme nur geprüft, ob die Software die in der Anordnung genannten Funktionen der Quellen-TKÜ erfüllt. Eine Überprüfung, ob auch andere eventuell unzulässige Funktionalitäten vorhanden sind, erfolgte nicht. Dies sei auch nur durch umfangreiche Tests, eine (aufwändige) Quellcodeanalyse oder, soweit man konkrete Anhaltspunkte habe, durch gezielte Tests möglich.

Vor diesem Hintergrund hat das LKA auf eine erweiterte Abnahme verzichtet. Den Quellcode wollte die Fa. DigiTask nicht herausgeben. Das LKA hat nicht versucht, sich vertraglich erforderlichenfalls den Zugriff auf den Quellcode zusichern zu lassen.

Ob die Software gleichzeitig die Ausleitung einzelner Daten auch an andere Stellen als an die Polizei ermöglichte, könnte ebenfalls nur durch die o. g. aufwändigen Analysen festgestellt werden.

Die Abnahme selbst und deren Dokumentation sind unzureichend.

3.3.2.1.2.2.3
Überwachung und wesentliche Funktionalitäten

Durch das LKA wurden mir einzelne Funktionalitäten des durch DigiTask erstellten Angebots bzw. der bestellten Software näher erläutert. Dabei handelte es sich um „Application-Screenshots“, d. h. Bilder des Browserfensters, in dem kommuniziert wird, und um einen prozessbasierten Keylogger, der nur solche Eingaben aufzeichnet, die im Rahmen der Kommunikation erfolgen.

Eine Dokumentation der Abläufe der Überwachungen selbst konnte mir durch das LKA nicht vorgelegt werden.

3.3.2.1.2.2.4
Weitere Leistungen der Fa. DigiTask

Mit der Fa. DigiTask wurde je Auftrag auch ein Vertrag über einen Support geschlossen. Dieser beinhaltet eine Unterstützung bei der Fehlersuche. Dafür erhielt die Fa. jedoch nach Aussagen des LKA keinen Zugriff auf das System zur Quellen-TKÜ, sondern es erfolgte eine Beratung, wo bzw. wie nach

der Ursache für einen Fehler gesucht werden kann. Soweit notwendig würde dann nicht auf die vorhandene Software zugegriffen, sondern durch DigiTask ein angepasstes Modul der Polizei zur Verfügung gestellt, das diese einspielt (hierzu wird nach den Aussagen der Polizei die „Nachladefunktion“ genutzt).

Nach den mir gegebenen Erläuterungen gehe ich davon aus, dass die aktive Beteiligung der Fa. DigiTask bei der Konfiguration der Systeme beendet war, bevor die Software auf dem Zielrechner eingebracht wurde. Dazu wurden durch eine entsprechende Konfiguration rechtzeitig Zugriffsmöglichkeiten von DigiTask gelöscht. Nach meinem Verständnis hat die Fa. DigiTask im Betrieb keinen Zugriff auf die notwendigen Rechner/Komponenten gehabt.

3.3.2.1.2.2.5
Fazit

Für die Organisation des Einsatzes ist festzustellen:

Es gibt keine dezidierte Beschreibung der Anforderungen und der erfolgten Lieferung, die über eine rudimentäre Bezeichnung in der von der Fa. gestellten Rechnung hinausgeht.

Die Abnahmen wurden nicht dokumentiert. Die Vereinbarungen mit der Fa. DigiTask sind nur pauschal und lückenhaft dokumentiert.

Der Einsatz selbst ist nur in dem Rahmen dokumentiert, der sich aus den Ermittlungsakten ergibt. Diese liegen mir aber nicht vor.

Da der Quellcode bei der Fa. DigiTask verblieb, ist auch eine nachträgliche Kontrolle, was die Software im einzelnen leisten konnte bzw. ob mit ihr auch andere Aktionen in den betroffenen Computern hätten angestoßen werden können bzw. auch gespeicherte Daten ausgeleitet werden können oder auch andere als die von der Polizei eingesetzten Empfangsgeräte hätten Zugriff haben können, nicht möglich.

Selbst wenn jetzt ein Quellcode der Firma analysiert wird, gibt es keine Garantie, dass dieser der jeweils gelieferten Software entspricht, so dass allenfalls eine allgemeine Überprüfung der Funktionalität dieser Software möglich wäre.

Ich gehe davon aus, dass die Fa. DigiTask den Programmcode nicht immer neu erstellt hat, sondern für die Aufträge der verschiedenen Polizeidienststellen auf vorhandene Bausteine aufgesetzt hat. Eine Analyse des Quellcodes war sowohl vom Bundesbeauftragten für den Datenschutz als auch von den Bayrischen Kollegen beabsichtigt, konnte allerdings nicht durch-

geführt werden, da die dafür von der Firma DigiTask geforderten Rahmenbedingungen – u. a. eine ausdrückliche Verschwiegenheitsverpflichtung – für eine Überprüfung durch unabhängige Datenschutzbeauftragte nicht akzeptabel waren.

3.3.2.1.2.3
Überprüfung der ausgeleiteten Daten

Zu den Fällen 1, 3 und 4 habe ich Kopien von Datenträgern erhalten, auf denen die ausgeleiteten Daten gespeichert sind. Im Fall 2 waren auf Anordnung der zuständigen Staatsanwaltschaft entsprechend den gesetzlichen Vorgaben die Daten schon gelöscht. Meine Kontrolle habe ich auf die Ausdrucke/Abbildungen der sog. Screenshots beschränkt. Die konkrete Überprüfung der mitgeschnittenen verschlüsselten Telefonie z. B. über Skype habe ich in diesem Kontext nicht für vordringlich gehalten, da insoweit – mit Ausnahme der Problematik der vom Kernbereich betroffenen Gespräche – keine Besonderheiten im Vergleich zur herkömmlichen Telefonie gegeben sind.

Soweit die Ausdrucke/Abbildungen dies erkennen lassen, sind zwar bei den sog. Application-Screenshots „nur“ jeweils die Fenster mit den Browsern ausgeleitet. Allerdings ist nicht sichergestellt, dass dabei in diesen Fenstern jeweils Daten aus einer gerade stattfindenden Telekommunikation enthalten waren. Bei einer der Maßnahmen finden sich wiederholt Screenshots mit der Startseite zum Zugriff auf das Firmen-Intranet. Weiterhin ist nicht immer sicher, ob nicht mit dem Browser auch Dateien betrachtet worden sind, die nicht Teil eines aktiven Telekommunikationsvorgangs sind. Denn der Browser wird auch benötigt, um Dateien im HTML-Format einzusehen, die bei einer früheren Kommunikationsverbindung auf dem Rechner gespeichert worden sind.

Die Screenshots werden offensichtlich in einem bestimmten zeitlichen Abstand (mehrmals pro Minute) erstellt, soweit gerade eine aktive Internetverbindung besteht. Es ist nicht eindeutig festzustellen, ob gerade der Inhalt der abgelichteten Browseranzeige zu diesem Telekommunikationsvorgang gehört.

Aus den vorliegenden Unterlagen ist weiterhin nicht ersichtlich, inwieweit bei der Durchführung der Maßnahme bzw. bei der weiteren Behandlung der ausgeleiteten Daten dem Kernbereichsschutz, insbesondere der unverzüglichen Löschung der betroffenen Kommunikationsdaten, Rechnung getragen worden ist. Aus vergleichbaren Prüfungen der Kollegen ist mir bekannt, dass es bei den über Skype geführten Gesprächen schwierig bis unmöglich war, die durch die Software der Fa. DigiTask ausgeleiteten Daten so zu bearbeiten, dass die entsprechenden Daten gelöscht werden konnten.

Das Problem des Kernbereichs stellt sich auch für die Application Screenshots. In einem Fall finden sich wiederholt Abbildungen von chats im Rahmen von Partnervermittlungen, bei denen nicht unbedingt davon auszugehen ist, dass hier „nur“ getarnte Gespräche geführt wurden.

Ob der eingesetzte Keylogger nur im Rahmen aktiver Telekommunikationsverbindung Daten aufgezeichnet hat, konnte ich nicht überprüfen.

Hier wäre zumindest zu klären, wie beim Einsatz einer solchen Funktionalität bei einer aktiven Telekommunikationsverbindung unterschieden werden kann, ob die jeweilige Eingabe Teil des Kommunikationsvorgangs ist oder nur im Rahmen einer parallel gleichzeitig genutzten Anwendung erfolgt.

3.3.2.1.3
Bewertung der Ergebnisse

Die konkrete Durchführung der Maßnahmen zur Quellen-TKÜ war nicht mit den Anforderungen an eine ordnungsgemäße Datenverarbeitung zu vereinbaren.

Der seit 2010 geltende § 15b HSOG benennt zumindest einige Anforderungen an die Dokumentation bzw. Protokollierung des konkreten Einsatzes. Dieser gilt zwar nur für Maßnahmen dieser Art im präventiven Bereich. Doch hätte zumindest das Inkrafttreten dieser Norm Anlass sein müssen, die Rahmenbedingungen für den Einsatz auch für Ermittlungsverfahren auf Grundlage der StPO vergleichbar zu gestalten.

Die festgestellten organisatorischen Mängel erfüllten nach meiner Einschätzung grundsätzlich die Voraussetzungen, die eine formale Beanstandung gem. § 27 HDSG rechtfertigen würden. Von einer solchen habe ich jedoch aus folgenden Gründen abgesehen:

Ein weiterer Einsatz dieser Software war nicht mehr vorgesehen. Zudem sind die dargestellten Defizite der Hessischen Polizei bewusst. Sie hat sich daher entschlossen, zukünftig die Software für eine Quellen-TKÜ in Kooperation mit anderen Polizeien selbst zu entwickeln oder eine kommerzielle Lösung tiefgreifend zu analysieren und ggf. zu zertifizieren.

3.3.2.1.4
Anforderungen an einzusetzende Software

Die festgestellten Mängel dürfen bei einer zukünftigen Nutzung nicht erneut auftreten. Daher ergeben sich eine Reihe von Anforderungen an den tech-

nischen und organisatorischen Rahmen der Entwicklung, die technischen Funktionen und den Betrieb einer Quellen-TKÜ-Software.

Die Programmentwicklung muss auf den richterlichen Beschlüssen fußen. Es muss dokumentiert werden, welche Funktionen beauftragt und programmiert wurden. Durch die Programmierung begleitende qualitätssichernde Maßnahmen und Abnahmetests muss sichergestellt werden, dass die Software die rechtlichen Vorgaben einhält. Für eine tiefergehende Analyse muss der Quellcode zur Verfügung stehen.

Durch technische Sicherungen muss die Software mit ihren Komponenten gewährleisten, dass Unbefugte das Programm nicht nutzen können und übertragene Daten nicht zur Kenntnis genommen werden können. Änderungen auf dem überwachten Rechner müssen sich auf das unbedingt erforderliche Maß beschränken. Ferner muss durch eine revisionssichere Protokollierung die Dokumentation der Quellen-TKÜ-Maßnahme unterstützt werden.

Der Betrieb muss so dokumentiert werden, dass nachträglich alle wichtigen Schritte nachvollziehbar sind. Dazu müssen die handelnden Personen ihre Tätigkeiten dokumentieren und mit der o. g. Protokollierung der zugehörigen technischen Abläufe ist diese zu ergänzen.

Wenn dieser Rahmen passend umgesetzt wird, ist eine rechtskonforme Quellen-TKÜ denkbar.

3.3.2.2
Recherche der Polizei in sozialen Netzen

Mit zunehmender Nutzung sozialer Netzwerke durch Bürgerinnen und Bürger wächst auch bei der Polizei das Interesse an den dort vorhandenen Informationen. Nicht jegliche Recherche ist im Rahmen der geltenden Rechtsgrundlagen zulässig.

Mit wenig Aufwand, meist schon durch einen Blick auf das Profil, können Behörden eine ganze Reihe von Informationen über Betroffene erlangen. Fotos, aber auch Informationen zu Beziehungen zu Freunden, Bekannten oder Geschäftspartnern sowie die Dialoge der Nutzer untereinander können für Ermittlungsbehörden interessant sein.

Will die Polizei Daten über einzelne Bürger erheben, muss sie sich dazu auf eine Erlaubnisnorm stützen. Ob dazu eine allgemeine Befugnisnorm ausreicht oder eine spezifische Rechtsgrundlage notwendig ist, hängt davon ab, wie intensiv die Datenerhebung in Grundrechte eingreift. Grundsätzlich liegt kein Eingriff in Grundrechte vor, wenn eine Ermittlungsbehörde allgemein zugängliche Inhalte – wie jeder Dritte auch – zur Kenntnis nimmt.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt jedoch dann vor, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeitsrechte von Betroffenen ergibt. Für die Einordnung solcher Recherchen hat das Bundesverfassungsgericht (Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07) zudem darauf abgestellt, ob dabei ein schutzwürdiges Vertrauen Betroffener ausgenutzt wird. Ein Eingriff in das Recht auf informationelle Selbstbestimmung liege nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt, wohl aber wenn sie dabei ein schutzwürdiges Vertrauen in die Identität und die Motivation seines Kommunikationspartners ausnutze, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde.

Es kommt daher entscheidend darauf an, inwieweit die Nutzenden eines sozialen Netzwerks auf die Vertraulichkeit der Eintragungen und/oder die Identität ihrer Kommunikationspartner vertrauen können, beziehungsweise ob eingestellte Informationen als öffentlich zugänglich zu bewerten sind. Dies ist bei der Ausgestaltung der sozialen Netze nicht immer einfach zu beantworten, zumal in der Regel keine Überprüfung der Identität von Personen, die sich anmelden, erfolgt.

Zumindest dann, wenn der Zugriff auf einzelne Einträge eingeschränkt ist und überprüft wird (z. B. durch den Nutzer selbst, indem er bestimmt, welchen Personen er als „Freunden“ Zugriff auf Daten gewährt, durch einen Gruppenmoderator, der über die Aufnahme von Nutzern in geschlossene Gruppen entscheidet oder durch Nutzungsbeschränkungen für ein soziales Netzwerk, für das besondere Teilnahmebedingungen erfüllt werden müssen), können diese nicht als allgemein zugängliche Daten eingestuft werden. Ein Vertrauen in die Identität des Kommunikationspartners kann dann entstehen, wenn dieser eindeutig vor der Anmeldung verifiziert wird. Allein die Forderung nach Nennung eines Klarnamens und Angabe einer E-Mail Adresse reicht dazu nicht aus. Das Beitreten zu einer Gruppe auf ausdrückliche Einladung kann dann Vertrauen schützen, wenn sichergestellt ist, dass Einladungen zur zukünftigen Nutzung nur an solche Personen ergehen, deren Identität dem Einlader eindeutig bekannt ist.

Sind Einträge nicht durch solche Einstellungen/Nutzungsbedingungen geschützt, sind sie genauso allgemein zugänglich wie andere im Internet einsehbare Daten. Ein Indiz dafür ist die Möglichkeit des Erschließens dieser Inhalte durch die gängigen Suchmaschinen. Damit bringt der Betroffene

zum Ausdruck, dass er für diese Daten kein Interesse daran hat, diese nur bestimmten Personen zugänglich zu machen.

Für die Ermittlungsbehörden bedeutet dies, dass dann die Generalbefugnisse aus dem HSOG oder aus der StPO als Rechtsgrundlage in der Regel ausreichen. Voraussetzung ist hiernach, dass die Kenntnis der Daten für die Durchführung eines strafrechtlichen Ermittlungsverfahrens oder zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Solche Erhebungen müssen nicht zwingend offen erfolgen. Daher ist es auch zulässig, dass die ermittelnden Beamten sich unter einem Pseudonym in dem sozialen Netzwerk bewegen. Ein schutzwürdiges Vertrauen wird in dieser Konstellation nicht ausgenutzt. Andererseits verhindert ein Pseudonym, dass der Betreiber des sozialen Netzes erkennen kann, dass die Polizei an den Aktivitäten bestimmter Nutzer interessiert ist.

Speziellere Grundlagen sind jedoch immer dann erforderlich, wenn die Polizei in geschützten Bereichen recherchieren will. Im Prinzip gibt es dabei Ähnlichkeiten zum Einsatz verdeckter Ermittler, wie er z. B. in § 110a StPO geregelt ist.

§ 110a StPO

(1) Verdeckte Ermittler dürfen zur Aufklärung von Straftaten eingesetzt werden, wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat von erheblicher Bedeutung

1. *auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,*
2. *auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes),*
3. *gewerbs- oder gewohnheitsmäßig oder*
4. *von einem Bandenmitglied oder in anderer Weise organisiert*

begangen worden ist. Zur Aufklärung von Verbrechen dürfen Verdeckte Ermittler auch eingesetzt werden, soweit auf Grund bestimmter Tatsachen die Gefahr der Wiederholung besteht. Der Einsatz ist nur zulässig, soweit die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Zur Aufklärung von Verbrechen dürfen Verdeckte Ermittler außerdem eingesetzt werden, wenn die besondere Bedeutung der Tat den Einsatz gebietet und andere Maßnahmen aussichtslos wären.

(2) Verdeckte Ermittler sind Beamte des Polizeidienstes, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln. Sie dürfen unter der Legende am Rechtsverkehr teilnehmen.

(3) Soweit es für den Aufbau oder die Aufrechterhaltung der Legende unerlässlich ist, dürfen entsprechende Urkunden hergestellt, verändert und gebraucht werden.

Ein Pseudonym bei der Anmeldung im sozialen Netz ist aber nicht unbedingt mit einer Legende im Sinne dieser Norm gleichzusetzen. Insbesondere wird mit einem Pseudonym regelmäßig keine auf Dauer angelegte, veränderte Identität angenommen.

Auch über den Weg des § 100a StPO, die Möglichkeiten der Telekommunikationsüberwachung, wird in der Regel ein solches Surfen unter einem Pseudonym nicht abzusichern sein.

§ 100a Abs. 1 StPO

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. *bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Abs. 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,*
2. *die Tat auch im Einzelfall schwer wiegt und*
3. *die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.*

Diese Regelung ist schon deshalb nicht einschlägig, da kein Eingriff in das Telekommunikationsgeheimnis vorliegt, denn dieses schützt die Kommunikation nach außen aber nicht zwischen den Kommunikationsteilnehmern. Darüber hinaus ist das Auslesen/Auswerten von Inhalten, die eine Person im Netz eingestellt hat, nicht mit der Kommunikation mit dieser Person gleichzusetzen. Das Telekommunikationsgeheimnis greift nicht mehr, nachdem der jeweilige Teilnehmer (erstmals) Gelegenheit hatte, den Inhalt zur Kenntnis zu nehmen. Sinn der Nachrichten in sozialen Netzen ist ja aber auch, dass Aussagen längerfristig gepostet werden sollen.

Auch § 100a StPO kann in der Regel nicht als Grundlage für den verdeckten Einsatz in geschützten Bereichen zu Grunde gelegt werden. Da der recherchierende Beamte an der Telekommunikation beteiligt ist, greift das Telekommunikationsgeheimnis nicht.

Rechtssicherheit für solche Recherchen in geschützten Bereichen kann daher nur dann hergestellt werden, wenn dazu spezielle Rechtsgrundlagen geschaffen werden. Wenn solche rechtspolitisch gewünscht werden, wird zudem das Problem zu lösen sein, wie der Schutz des Kernbereichs privater Lebensführung sichergestellt werden kann.

3.3.3
Schulen, Schulverwaltung, Hochschulen, Archive

3.3.3.1
Gesetz zur Neuregelung des Archivwesens und des Pflichtexemplarrechts

Die Hessische Landesregierung hat eine Neufassung des Hessischen Archivgesetzes vorgelegt. Gegenüber dem Ausschuss für Wissenschaft und Kunst des Hessischen Landtags, zuvor gegenüber dem Hessischen Minis-

terium für Wissenschaft und Kunst, habe ich zu der Neufassung Stellung genommen. Gegen die zuletzt vorgelegte Fassung (LTDrucks. 18/6067) hatte ich keine datenschutzrechtlichen Bedenken erhoben. Erhebliche datenschutzrechtliche Bedenken bestehen allerdings gegen die dann tatsächlich beschlossene Fassung des Gesetzes.

Neben einer Reform der Archivverwaltung und der gesetzlichen Verankerung der Archivschule Marburg und des Hessischen Landesamtes für geschichtliche Landeskunde, bezweckt das inzwischen in Kraft getretene Archivgesetz eine Fortentwicklung des Archivrechts aufgrund der Entwicklung in der Schriftgutverwaltung sowie der Archivierung und Nutzung des Archivgutes.

§ 8 des Gesetzes unterwirft alle Unterlagen, die von den öffentlichen Stellen in Hessen zur Erfüllung ihrer Aufgaben nicht mehr benötigt werden und deren Aufbewahrungsfristen abgelaufen sind, der Anbietungspflicht an das zuständige Archiv. Bejaht das Archiv binnen sechs Monaten die Archivwürdigkeit, werden die Unterlagen mit ihrer Übernahme zum Archivgut. Ansonsten erfolgt die Löschung bzw. die Vernichtung.

§ 8 HArchivG

(1) 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. Dies hat spätestens 30 Jahre nach Entstehung der Unterlagen zu erfolgen, soweit nicht Rechtsvorschriften andere Aufbewahrungsfristen bestimmen. Das zuständige Archiv hat binnen sechs Monaten über die Archivwürdigkeit angebotener Unterlagen zu entscheiden.

(2) Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder des Datenschutzes unterworfen sind oder die aufgrund besonderer Vorschriften hätten gelöscht oder vernichtet werden müssen.

(3) Die in § 2 Abs. 3 und 6 genannten Stellen dürfen nach Ablauf der Aufbewahrungsfristen Unterlagen nur vernichten oder Daten nur löschen, die das zuständige Archiv zur Vernichtung oder Löschung freigegeben hat oder wenn es nicht binnen sechs Monaten über die Archivwürdigkeit angebotener Unterlagen entschieden hat, und sofern kein Grund zur Annahme besteht, dass durch die Vernichtung oder Löschung schutzwürdige Belange von Betroffenen beeinträchtigt werden.

(4) Auf die Anbietung von offensichtlich nicht archivwürdigen Unterlagen und Daten wird im Einvernehmen mit dem zuständigen Archiv verzichtet.

(5) Die in § 2 Abs. 3 und 6 genannten Stellen bieten jeweils ein Exemplar der von ihnen herausgegebenen Veröffentlichungen, auch solcher in elektronischer Form, dem zuständigen Archiv zur Übernahme an.

(6) Die in § 2 Abs. 3 und 6 genannten Stellen können Unterlagen einem anderen öffentlichen Archiv anstelle des zuständigen Archivs mit dessen Einvernehmen zur Archivierung anbieten, wenn es im öffentlichen Interesse liegt.

§ 2 HArchivG

...

(3) Öffentliches Archivgut sind alle archivwürdigen Unterlagen der Verfassungsorgane, Behörden, Gerichte, des Landtags und der sonstigen öffentlichen Stellen des Landes, der Städte, Gemeinden, Landkreise und kommunalen Verbände, ihrer Rechts- und Funktionsvorgänger sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihrer Vereinigungen einschließlich der Hochschulen, die zur dauernden Aufbewahrung von einem öffentlichen Archiv übernommen werden.

...

(6) Als öffentliche Stellen des Landes gelten auch:

1. *Stiftungen des Privatrechts, wenn das Land oder ein Rechtsvorgänger überwiegend das Stiftungsvermögen bereitgestellt hat, und*
2. *andere juristische Personen des Privatrechts, wenn sie nicht am wirtschaftlichen Wettbewerb teilnehmen und dem Land mehr als die Hälfte der Anteile oder der Stimmen zusteht.*

Das Archivgesetz verfolgt das Ziel, Archivgut der Allgemeinheit und der Forschung zur Verfügung zu stellen. Dies umfasst auch archivwürdiges Material, das personenbezogene Daten enthält, die datenschutzrechtlich zu löschen wären. Zutreffend ist in der Gesetzesbegründung ausgeführt, dass es im Hinblick auf die Bestimmungen des Datenschutzes spezialgesetzlicher Vorschriften über die Verarbeitung und Nutzung personenbezogenen Archivgutes durch die Archive bedarf. Das Archivgesetz legt die rechtlichen Rahmenbedingungen fest, unter denen in den Archiven enthaltene personenbezogene Daten gespeichert und zugänglich gemacht werden, damit sie für Forschungszwecke und für die Wahrnehmung berechtigter Belange von Bürgerinnen und Bürgern und Verwaltung genutzt werden dürfen.

Ziel dieser Regelungen ist ein möglichst weitgehender Ausgleich zwischen den widerstreitenden Schutzgütern der Wissenschaftsfreiheit (Art. 5 GG) und dem Recht auf informationelle Selbstbestimmung (Art. 2 i. V. m. Art. 1 GG) im Sinne einer praktischen Konkordanz. Die Abwägung erfolgt in folgender Weise: Behörden müssen Akten und Dokumente, für die die Aufbewahrungsfristen abgelaufen sind, dem zuständigen Archiv anbieten. Nur dasjenige, was das Archiv nicht für archivwürdig eingestuft hat, darf vernichtet werden. Das gilt auch für personenbezogene Daten, die aufgrund datenschutzrechtlicher Bestimmungen zu löschen oder zu vernichten wären. Für sie sieht das Archivgesetz eine Schutzfrist von 60 Jahren nach ihrer Entstehung vor (§ 13 Abs. 1). Während der Schutzfrist unterscheidet das Gesetz u. a. zwischen der Nutzung und der Veröffentlichung des personenbezogenen Archivgutes.

Einem Antrag auf Nutzung vor Ablauf der Schutzfrist darf nur stattgegeben werden,

1. wenn die Nutzung für ein bestimmtes Forschungsvorhaben erforderlich ist und schutzwürdige Belange der betroffenen Personen oder Dritter nicht beeinträchtigt werden oder
2. das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange erheblich überwiegt oder
3. die Nutzung der Wahrnehmung berechtigter Belange im überwiegenden Interesse einer anderen Person oder Stelle unerlässlich ist und eine Beeinträchtigung schutzwürdiger Belange durch angemessene Maßnahmen ausgeschlossen wird.

Eine Veröffentlichung der personenbezogenen Daten darf nur erfolgen, wenn die betroffene Person, im Falle des Todes der überlebende Ehegatte oder eingetragene Lebenspartner, im Falle auch deren Todes die Kinder, eingewilligt hat oder dies für die Darstellung des bestimmten Forschungsvorhabens unerlässlich ist. Weitere Ausnahmen gelten für Amtspersonen in Ausübung ihres Amtes und Personen der Zeitgeschichte.

Davon unbeschadet darf Archivgut, das sich auf eine natürliche Person bezieht, im Regelfall erst zehn Jahre nach dem Tod der betreffenden Person durch Dritte genutzt werden. Ist der Todestag nicht festzustellen, endet die Schutzfrist 100 Jahre nach der Geburt der betroffenen Person.

Mit der Übergabe des Archivgutes an das zuständige Archiv geht auch die Verantwortung dafür, das Recht auf informationelle Selbstbestimmung zu sichern, auf das Archiv über. Dies ist aus datenschutzrechtlicher Sicht akzeptabel. Mit den im Gesetz enthaltenen Schutzfristen und weiteren Elementen des Datenschutzes – wie weiteren Nutzungseinschränkungen im Einzelfall (§ 14) und einem Auskunfts- und Berichtigungsrecht (§ 15) – ist dem Recht auf informationelle Selbstbestimmung – auch in der Abwägung zur Wissenschaftsfreiheit gerade noch hinreichend Rechnung getragen. Gegen den Gesetzentwurf – LTDrucks. 18/6067 – habe ich deshalb insoweit keine Bedenken erhoben.

Das HMWK hatte mich bereits im Rahmen der Ressortanhörung an dem Gesetzentwurf beteiligt. Im Zuge dieser Beteiligung hat das Ministerium von einer früheren Fassung, die vorsah, auch unzulässig erhobene Daten zu archivieren, auf meine Empfehlung hin abgesehen.

Diese Korrektur hat der Hessische Landtag in seiner Sitzung am 22. November 2012 rückgängig gemacht. Am 20. November 2012 legten die Regierungsfraktionen einen in der letzten Sitzung des Ausschusses für Wissenschaft und Kunst angekündigten aber nicht näher beschriebenen Änderungsantrag vor. In diesem Änderungsantrag wurden u. a. in § 8 Abs. 2 die Wörter „sofern diese nicht unzulässig erhoben oder verarbeitet wurden“ gestrichen. Die Vorschrift lautete zuvor:

§ 8 Abs. 2 HArchivG – Fassung LTDrucks. 18/6067

Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder des Datenschutzes unterworfen sind oder aufgrund besonderer Vorschriften hätten gelöscht oder vernichtet werden müssen, sofern diese nicht unzulässig erhoben oder verarbeitet wurden.

Die Begründung für diese Änderung lautete: „Die Änderung ermöglicht, dass die Anbietungspflicht auch für solche Unterlagen gilt, die unzulässig erhobene oder gespeicherte Daten enthalten. Auch Unterlagen mit rechtswidrig gespeicherten Daten müssen archiviert werden können. Der besondere historische Wert solcher Unterlagen kann gerade in der rechtswidrigen Datenspeicherung liegen."

Der Hessische Landtag beschloss diese Änderung, ohne sich mit der datenschutzrechtlichen Problematik auseinanderzusetzen, kurz vor Schluss der Nachmittagssitzung am 22. November 2012 – s. PlPr 18/122 – 22. November 2012.

Damit wird der Vorrang der Forschungsfreiheit vor dem Datenschutzrecht in unverhältnismäßigem Umfang ausgeweitet. Die bereits vorhandene Vorrangstellung in der Form, dass Akten und Unterlagen, die von der Verwaltung nicht mehr benötigt werden und deren Aufbewahrungsfristen abgelaufen sind, nicht gelöscht, sondern über das Archivrecht der Forschung zur Verfügung gestellt werden, ist aus datenschutzrechtlicher Sicht gerade noch akzeptabel. Die vorhandenen Schutzfristen und weitere Elemente des Datenschutzes fanden im Archivrecht hinreichend Berücksichtigung. Ausgenommen waren bislang diejenigen Daten und Unterlagen, welche aufgrund gesetzlicher Vorschriften zu löschen oder zu vernichten waren oder die unzulässig erhoben oder verarbeitet wurden.

Dies ist jetzt entfallen. Dadurch treten datenschutzrechtliche Elemente wie der Anspruch auf das Vergessen einer einst belastenden Information, Resozialisierungsgründe, aber auch der Anspruch auf die Korrektur eindeutig falscher Daten und der Anspruch auf Löschung unzulässig erhobener und verarbeiteter Daten völlig zurück. Eine rechtswidrige Datenspeicherung durch eine Behörde bedeutet einen nicht gerechtfertigten Eingriff in das verfassungsrechtlich verbürgte informationelle Selbstbestimmungsrecht des Bürgers. Wenn dieses Grundrecht, das eigentlich ein (vorbeugendes) Abwehrrecht gegen Eingriffe ist, verletzt wird, „wandelt" es sich quasi zu einem Folgenbeseitigungsanspruch um: Der Staat hat nun alles zu tun, um die eigentlich zu vermeidende Rechtsverletzung wieder rückgängig zu machen. Eine Archivierung durch das Staatsarchiv würde aber eine Perpetuierung der Rechtsverletzung bedeuten. Eine solche Aufrechterhaltung einer

bestehenden Rechtsverletzung – und dies auch noch für unabsehbare Zeit – ist verfassungsrechtlich inakzeptabel.

3.3.3.2
Hessisches BAföG/AFBG-Verfahren

Die Einführung eines neuen Verfahrens zur Durchführung des Bundesgesetzes über individuelle Förderung der Ausbildung und des Bundesgesetzes zur Förderung der beruflichen Aufstiegsfortbildung in Hessen war komplex, insbesondere galt es eine Vielzahl datenschutzrechtlicher Probleme zu bewältigen. In das Verfahren war ich frühzeitig eingebunden, so dass die datenschutzrechtliche Beratung und die antizipierende Kontrolle ineinander flossen.

3.3.3.2.1
Einführung

In Hessen wird das Gesetz über individuelle Förderung der Ausbildung – Bundesausbildungsförderungsgesetz – (BAföG) von 26 kommunalen Ämtern für Ausbildungsförderung und fünf Studentenwerken ausgeführt. Das HMWK hatte bereits im Jahr 2007 beschlossen, das bislang dafür bei der HZD eingesetzte Großrechnerverfahren durch ein neues, modernes client-/serverbasiertes IT-Verfahren zu ersetzen. Durch stetige Verzögerungen im zunächst verfolgten Länderverbundprojekt „BAföG21/Dialog21/Kasse21“ wurde vom HMWK nach Alternativen gesucht, um das veraltete, aus den 1970er Jahren stammende Verfahren baldmöglichst abzulösen. Nach einer Vorstudie und Markterhebung in den Jahren 2008/2009 stellte sich heraus, dass die auf dem freien Markt erhältliche Software der Firma DATAGROUP eine solche geeignete Alternative sein könnte. Vor der Entscheidung mussten aber noch rechtliche und technische Fragen geklärt werden.

3.3.3.2.1.1
Sachstand altes Verfahren

Die BAföG-Anträge wurden vor Ort in den Studentenwerken und in den Kommunen von Beschäftigten bearbeitet, die über eine entsprechende Infrastruktur mit einem Zentralrechner und einer zentralen Datenbank verbunden waren. Die zentrale Datenverarbeitung fand in der HZD statt. Die eigentliche Antragsstellung und Aktenführung verblieb in den Studentenwerken und Kommunen.

3.3.3.2.1.2
Sachstand neues Verfahren

Geplant ist, künftig die zentrale Datenverarbeitung der BAföG- und AFBG-Daten der Firma DATAGROUP zu übertragen, die hierfür ihr Rechenzentrum in Bremen nutzen wird. Hierfür ist es erforderlich, dass sämtliche im derzeitigen Großrechnerverfahren gespeicherten BAföG- und AFBG-Daten an DATAGROUP übermittelt und bei DATAGROUP gespeichert werden.

3.3.3.2.2
Rechtliche Bewertung

3.3.3.2.2.1
§ 80 Abs. 5 SGB X

Im Rahmen des formellen Vergabeverfahrens stellte sich die Frage, inwieweit Softwarebeschaffung und gleichzeitiger Betrieb des Verfahrens aus einer Hand im Rahmen der Auftragsdatenverarbeitung zulässig ist.

Zu prüfen war, ob das geplante Vorgehen mit § 80 Abs. 5 SGB X in Einklang zu bringen ist

> *§ 80 Abs. 5 SGB X*
>
> *Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen ist nur zulässig, wenn*
> 1. *beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder*
> 2. *die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben.*

Bei der Ausgestaltung des Verfahrens wurden vor diesem rechtlichen Hintergrund zwei Optionen erörtert.

Option Nr. 1
Speicherung der BAföG-Daten und AFBG-Daten auf einem Rechner in einem Rechenzentrum der DATAGROUP.

Die Beauftragung nicht öffentlicher Stellen mit der Verarbeitung von Sozialdaten ist grundsätzlich nachrangig gegenüber der Verarbeitung durch eine öffentliche Stelle. Für sie gelten die erschwerten Bedingungen, die im oben

zitierten § 80 Abs. 5 SGB X aufgelistet sind. Die Gefahr, dass beim Auftraggeber sonst Störungen im Betriebsablauf auftreten könnten, wurde mangels praktischer Bedeutung verneint (§ 80 Abs. 5 Nr. 1 SGB X).

Voraussetzung für die Aufgabenerledigung durch eine nicht-öffentliche Stelle ist nach § 80 Abs. 5 Nr. 2 SGB X, dass die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können. Das HMWK hat dies nachvollziehbar bejaht. Bei dem Kostenvergleich sind neben der hauseigenen Verarbeitung durch den Sozialleistungsträger selbst auch die Auftragsdatenverarbeitung durch andere Sozialleistungsträger bzw. sonstige öffentliche Stellen zu berücksichtigen.

Daneben ist Voraussetzung, dass der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer gibt, verbleiben. Lediglich die Speicherung von Daten darf sich nicht auf den gesamten oder überwiegenden Datenbestand beziehen. Im Übrigen – also soweit sie keine Speicherung ist – kann die Datenverarbeitung durch den beauftragten Privaten den gesamten Datenbestand betreffen. Eine Speicherung des gesamten Datenbestandes ist bei dem Projekt jedoch erforderlich. Es würden nämlich sämtliche Daten, die bei diesem Projekt verarbeitet werden, an DATAGROUP übergeben werden, sodass keinerlei BAföG- und AFBG-Daten beim Auftraggeber verblieben. Daher ist die Option Nr. 1 als rechtliche Möglichkeit ausgeschieden.

Option Nr. 2

Das HMWK wird eine Parzelle in einem externen Rechenzentrum, das den sonstigen Anforderungen – BSI-Grundschutz – erfüllt, anmieten und dort eine eigens gekaufte bzw. geleaste Hardware aufbauen. Die Administration erfolgt durch eine Fremdfirma (DATAGROUP):

Rechtlich bedeutet dies, dass die Speicherung der Daten nicht beim Auftragnehmer erfolgt und somit ein Verstoß gegen § 80 Abs. 5 Nr. 2 SGB X ausscheidet.

3.3.3.2.2.2
Vorabkontrolle und Verfahrensverzeichnisse (§§ 7, 15 HDSG)

§ 7 Abs. 6 HDSG verlangt für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung eine gutachtliche

Bewertung der einzelnen Gefahren für das informationelle Selbstbestimmungsrecht unter den Aspekten der rechtlichen Zulässigkeit sowie der technischen und organisatorischen Datensicherheit (Vorabkontrolle). Durchzuführen ist die Vorabkontrolle von demjenigen, der für den Einsatz oder die wesentliche Änderung des Verfahrens zuständig ist. Das hessische BAföG/AFBG-Verfahren (HeBaV) wird landeseinheitlich eingeführt werden. Die Konzeption, die Gesamtsteuerung und die Federführung liegen beim HMWK. Gleichwohl bleiben die kommunalen Ämter für Ausbildungsförderung und die Studentenwerke aber für ihren Bereich die nach dem Hessischen Datenschutzgesetz verantwortlichen Daten verarbeitenden Stellen.

Da das HMWK zentrale Vorgaben für den Einsatz des Verfahrens macht, hat es folglich insoweit auch die Vorabkontrolle zu erstellen. Weil es sich um ein gemeinsames Verfahren nach § 15 HDSG handelt, trifft das HMWK als Federführer ohnehin hier diese Pflicht.

Das Verfahrensverzeichnis nach § 15 HDSG und das Muster- Verfahrensverzeichnis nach § 6 HDSG wurden vom HMWK mit meiner Unterstützung erarbeitet. Das HMWK hat den Studentenwerken und kommunalen Ämtern das Muster-Verfahrensverzeichnis zur Vervollständigung zur Verfügung gestellt.

Das HMWK führt das Verfahrensverzeichnis nach § 15 HDSG und die Verfahrensverzeichnisse aller beteiligten Stellen. Diese liegen seit Anfang September 2012 vor.

3.3.3.2.3
Technische Ausgestaltung

Bei den zu verarbeitenden BAföG- und AFBG-Daten handelt es sich um Daten mit hohem Schutzbedarf. Neben Verfügbarkeit und Integrität muss deshalb insbesondere die Vertraulichkeit der Daten gewährleistet werden. Bei der Auswahl und der Gestaltung des Verfahrens wurde hierauf besonderes Augenmerk gelegt.

3.3.3.2.3.1
Aktueller Sachstand

Mit Hilfe des neuen Verfahrens werden alle notwendigen Prozesse zur Antragstellung, Berechnung, Bescheiderstellung, Zahlung und Rückforderung im Rahmen der Förderung von Schülerinnen, Schülern und Studierenden sowie der beruflichen Aufstiegsförderung abgewickelt. Monatlich werden Zahlungen an ca. 35.000 Antragsteller durchgeführt sowie ca. 8.500 Bescheide ausgedruckt. Derzeit wird das Altverfahren durch ein voll integrier-

tes Verfahren der Firma DATAGROUP ersetzt. Basierend auf den gesetzlichen Vorgaben des BAföG/AFBG kann mit der Software Studierenden-, Schüler- und Auslands- sowie Meister-BAföG abgewickelt werden. Dabei steht die Erleichterung der Arbeit für den Sachbearbeiter im Mittelpunkt. Leistungsmerkmale sind u. a. sofortiger Ausdruck des Bescheides bereits am Sachbearbeiterplatz, elektronische Aktenführung mit Wiedervorlagefunktion, E-Mail-Integration zur schnellen und einfachen Kommunikation mit den Personen, die die Förderung beantragen, Möglichkeit von Zukunftseingaben und Zukunftsbescheiden, MICROSOFT-WORD-Schnittstelle zur komfortablen Erzeugung von Dokumenten, automatische Protokollierung aller Änderungen, vollständige Plausibilisierung, Vergleichsberechnung für Aktualisierungsanträge, Vieraugenprinzip oder Sammelfreigabe, Serviceberechnung für Beratungsgespräche, umfangreiche Such- und statistische Auswertungsmöglichkeiten, Kassenverfahren und Schnittstellen zur elektronischen Datenübermittlung. Die Software beinhaltet darüber hinaus die Möglichkeit der Onlinebeantragung von Förderleistungen. Bei diesen komplexen Anforderungen muss großer Wert auf die IT-Sicherheit gelegt werden.

3.3.3.2.3.2
Technische Umsetzung

3.3.3.2.3.2.1
Rechenzentrum

Der Betrieb des gesamten Verfahrens erfolgt in einem durch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) zertifizierten Datacenter. In diesem wurde Stellfläche für ein verschließbares Rack angemietet. Das Rack verfügt über ein Remote-Schließsystem. Der „Masterkey“ zum Schließsystem liegt beim HMWK, sodass auch aus der Ferne der physikalische Zugang zum System kontrolliert und bei Bedarf unterbunden werden kann.

3.3.3.2.3.2.2
Monitoring

Im Rahmen des Betriebs erfolgt ein umfangreiches Monitoring. Eine regelmäßige Überwachung, insbesondere der Infrastruktur mit einer speziellen Software (Nagios) und Videoüberwachungssystem, der Zugangskontrollmechanismen und eine Dokumentation von Vorkommnissen und durchgeführten Maßnahmen sorgt für Sicherheit.

3.3.3.2.3.2.3
Hardware

Das gesamte Verfahren wird auf vier identisch ausgestatteten Serversystemen unter dem Einsatz von VMware-Virtualisierungstechnologie betrieben. Das System ist ausfallsicher ausgelegt. Dabei sind die wichtigsten Elemente (z. B. Stromversorgung, Netzschnittstellen, Festplattenspeichersystem) redundant vorhanden.

3.3.3.2.3.2.4
Firewall-Systeme und Netzanbindung

Das Rechenzentrum nutzt zur Anbindung an das Internet das Routingprotokoll BGP4 und ist über zwei Provider – ebenfalls, um eine hohe Verfügbarkeit zu gewährleisten – redundant angebunden. Dieses Multi-WAN-Konzept und der ISP-Failover (ungeplanter Wechsel zwischen den Providern bei einseitigem Ausfall) steigern die Zuverlässigkeit und den Schutz gegen Internetausfälle. Das BAföG/AFBG-System wird über VPN-Tunnel zu den Standorten angebunden. Diese VPN-Tunnel bedingen eine Firewall/einen Router am Standort der Benutzer und im Datacenter, der mit der Verschlüsselung AES oder Triple-DES und der Authentifizierung SHA1 oder MD5 verschlüsselte Verbindungen aufbauen kann. Das HMWK stellt die komplette VPN-Hardware zur Verfügung. Das Datacenter betreibt zudem ein modernes, zentrales und redundantes Firewall-System. Der gesamte Datenverkehr aller angeschlossenen Nutzer wird über diese Firewall zentral weitervermittelt. Dieses Firewall-System garantiert, dass nur die im Rahmen der Sicherheitsrichtlinie zugelassenen netzübergreifenden Aktivitäten möglich sind. Damit ist ein einheitliches Sicherheitsniveau erreicht. Zusätzlich wird für das HMWK eine dedizierte Firewall bereitgestellt, um ein erhöhtes Sicherheitsniveau und eine höhere Flexibilität für die Konfiguration der Zugriffe zu erreichen. Diese Firewall ist redundant ausgelegt. Über dieses mehrstufige Firewall-Konzept wird die Anbindung an den internen LAN-Backbone gegen unberechtigte Nutzer abgesichert. Auch eine Absicherung gegen Viren ist im Service-Paket enthalten.

3.3.3.2.3.2.5
Systemsoftware

Der Auftragnehmer betreibt für das BAföG/AFBG-Verfahren ein komplett eigenständiges System, das keine Verbindungen zu anderen Systemen hat. Dieses eigenständige System besteht aus vier Hochleistungsservern, auf denen etwa 20 virtuelle Server installiert werden. Einer dieser virtuellen Server wird für die Datenbank genutzt.

In einer auf Terminalserverarchitektur basierenden Installation erfolgt die Kommunikation zwischen den Arbeitsplatzrechnern der Sachbearbeiter und den zentralen Terminalservern über VPN, das verschlüsselt genutzt wird. Die Systeme werden auf VMware vSphere virtualisiert. Der Vorteil dieser Bare-Metal-Virtualisierungslösung liegt in der Skalierbarkeit und der optimalen Auslastung der Hardware-Ressourcen bei gleichzeitig sehr hoher Verfügbarkeit und Datensicherheit.

Netzwerkseitig sind die virtuellen Maschinen an dedizierte Netzwerkanschlüsse gebunden, sodass die Netze logisch getrennt werden. Somit wird verhindert, dass DMZ und internes Netz unter Umgehung des Firewall-Systems miteinander kommunizieren können.

Die MICROSOFT-Active-Directory-Dienste sind auf zwei virtuellen Servern installiert, um den Ausfall eines Servers kompensieren zu können. Die komplette MICROSOFT-Windows-Umgebung ist durch Trend-Micro-Virenscanner abgesichert.

Das Active Directory setzt für die Benutzerauthentifizierung das Protokoll Kerberos ein, somit sind die Anmeldetoken an keiner Stelle klar lesbar.

Über das Active Directory werden im Übrigen Gruppenmitgliedschaften und Berechtigungen der einzelnen Benutzer definiert. Ein begrenzter Benutzerkreis (Administration) kann diese Berechtigungen steuern und ein Benutzer hat hierauf keinen Einfluss. Alle Änderungen können über die Systemprotokollierung transparent nachvollzogen werden.

3.3.3.2.3.2.5.1
Terminaldienste

Es sind mehrere Terminalserver installiert. Die Applikationen werden über Citrix XenApp-Terminalserver den Anwendern zur Verfügung gestellt. Diese sind so konfiguriert, dass eine automatische Lastverteilung stattfindet. Für die Benutzer, die nicht über einen VPN-Tunnel angebunden sind, werden die Citrix-Dienste über ein separates Webinterface mit Zwei-Faktor-Authentifizierung zur Verfügung gestellt. Das Webinterface ist per https mit einem RSA-Schlüssel mit 2048 Bit auf einem separaten DMZ-Netz veröffentlicht. Somit ist die Verbindung im Internet verschlüsselt. Um den erhöhten Schutzbedarf sicherzustellen und insbesondere den Zugriff durch Unbefugte zu verhindern, werden für diesen Benutzerkreis Einmalkennwort-Generatoren von VASCO eingesetzt. Der Anwender benötigt daher für den Zugriff seinen Benutzernamen, sein WINDOWS-Active-Directory-Kennwort, eine Ziffernfolge des Einmalkennwort-Generators sowie eine PIN. Die Si-

cherheitsanforderung, den Zugriff an die Faktoren Besitz und Wissen zu knüpfen, ist dadurch erfüllt.

3.3.3.2.3.2.5.2
Datenbank

Die Ablage der Daten erfolgt verschlüsselt im Datenbanksystem Caché 2010 (Intersystems). Es handelt sich um eine objektrelationale Datenbank.

3.3.3.2.3.2.5.3
Protokollierung

Die An- und Abmeldung von Benutzern wird vom Betriebssystem gespeichert. Jede Dateneingabe/-änderung wird im Fachverfahren mit Datum, dem alten und dem neuen Wert sowie dem Sachbearbeiter, der die Änderung eingegeben hat, protokolliert. Zusätzlich wird im Verfahren der Zugriff auf Datensätze protokolliert. Dabei wird festgehalten, wer wann welchen Datensatz aufgerufen hat und dabei unterschieden, ob der Datenzugriff schreibend oder löschend war. Auch eine Dokumentation von nur lesenden Zugriffen ist möglich. Mit Administrationsrechten ist das Protokoll einsehbar und nach den Kriterien in den Spalten sortier- und filterbar.

3.3.3.2.3.2.5.4
Backup

Zur Durchführung der regelmäßigen Datensicherung werden ein geeigneter Sicherungsplan sowie eine umfassende Sicherungsprozedur erstellt. Zudem werden regelmäßige Wiederherstellungstests zur Sicherstellung der Wiederherstellungsfähigkeit durchgeführt.

Nach einem Schadensfall kann die Wiederherstellung des uneingeschränkt lauffähigen Systems innerhalb kurzer Zeit gewährleistet werden. Die Wiederherstellung wird in einem Wiederherstellungsjournal gespeichert und ist somit verifizierbar. Eine (Teil-)Wiederherstellung ist auch im laufenden Betrieb möglich. Die Datensicherung beinhaltet alle Produktivdaten. Zu Archivierungszwecken können die Daten auf WORM-Bänder gesichert werden. Die Datensicherung erfolgt verschlüsselt (z. B. 256 Bit AES).

3.3.3.2.3.2.6
Anwendungssoftware

BAFSYS der Firma DATAGROUP ist ein Fachverfahren, um BAföG- und AFBG Anträge in Ämtern für Ausbildungsförderung zu bearbeiten, zu bescheiden und die Förderakten weitgehend elektronisch zu führen. Es beinhaltet u. a. folgende Module:

Das **Hauptsystem** dient dazu, Daten der Personen, die die Förderung beantragen sowie ihrer Anträge zu verwalten und die Anträge zu bearbeiten. Hier werden die Stammdaten dieser Personen erfasst und die Antragsdaten eingegeben oder aus dem Online-Antrag übernommen. Aus dem Hauptsystem heraus können Dokumente erstellt werden wie z. B. Schreiben, mit denen fehlende Unterlagen angefordert werden. Außerdem kann von hier aus das Rückforderungsmanagement aufgerufen und Einsicht in die jeweilige Kassenakte genommen werden.

Mit dem **Benutzerrollenkonzept** kann die Administration beliebig viele Rollen anlegen. Sie kann jeder mit der Sachbearbeitung betrauten Person eine der vorher erstellten Rollen zuweisen. Für jede Rolle können die Zugriffsrechte auf jeden vorhandenen Menü-Eintrag festgelegt werden. Jeder Sachbearbeiter bzw. jede Sachbearbeiterin wird einem Mandanten zugeordnet. In der Mandantenverwaltung können durch den Administrator jedem Mandanten mehrere Amtsnummern (Kurzbezeichnungen) zugeordnet werden. Der Zugriff auf die Fälle innerhalb eines Mandanten (Amts) kann für jede für die Sachbearbeitung zuständige Person durch den dezentralen Administrator nach Buchstabenbereichen der Nachnamen der den Antrag stellenden Personen festgelegt werden. Dabei ist sichergestellt, dass jeder dezentrale Administrator nur die Zugriffsberechtigungen derjenigen Beschäftigten verwalten kann, die dem gleichen Mandanten zugeordnet sind, wie er selbst.

Das Verfahren bietet die Möglichkeit des **Online-Antrags**, d. h. Personen, die einen Förderantrag stellen wollen, können ihre Daten künftig online eingeben. Die Daten werden auf Format und Vollständigkeit geprüft und soweit wie möglich plausibilisiert, z. B. auch Post- und Bankleitzahlen. Außerdem erhält jede Person, die einen Antrag stellt, eine individuelle Liste mit einzureichenden Unterlagen. Sie kann anschließend den Antrag ausdrucken, unterzeichnen und im Amt abgeben (oder diesem zuschicken). Die jeweils für die Sachbearbeitung zuständige Person kann nach Eingang des Antrages über die aufgedruckte Telenummer die Daten abrufen und sie so medienbruchfrei in das Verfahren übernehmen. Beim Online-Antrag haben Antragstellende die Möglichkeit, die eingegebenen Daten in einer Datei lokal auf ihrem Rechner abzuspeichern. Die Dateien besitzen ein eigenes Format

und können wieder in das entsprechende Online-Formular geladen werden. Beim Speichern der Daten besteht die Möglichkeit, die Datei mit einem eigenen Passwort zu verschlüsseln. Wird die Datei ohne eigenes Passwort gespeichert, so wird sie trotzdem mit einem Standardpasswort verschlüsselt.

Mit Hilfe des **Informationsportals** kann das zuständige Ministerium die gesamte Information aller Ämter für Ausbildungsförderung zu neuen Erlassen und Urteilen sicherstellen.

Es existiert ein **Service-Desk** des Softwareanbieters. Dieser gilt als Single Point of Contact für alle Probleme rund um das gesamte Verfahren.

3.3.3.2.4
Zusammenfassung

Das gesamte Projekt habe ich datenschutzrechtlich begleitet. Es lief in folgenden wesentlichen Verfahrensschritten ab:

- Klärung der rechtlichen Rahmenbedingungen
- Analyse der hessenspezifischen Anforderungen
- Customizing der Software und Umsetzung der spezifischen Anpassungen
- Einrichtung des Systems beim Betreiber
- Einrichtung der Berechtigungen
- Tests (Funktionstest, Integrationstest, Lasttest, GUI-Test, Penetrationstest)
- Schulung der Anwender und Administration
- Migration der Altdaten
- Parallelbetrieb
- Erstellung Betriebskonzept
- Erstellung Vorabkontrolle und Verfahrensverzeichnisse
- Erstellung Sicherheitskonzept
- Erstellung Administrationskonzept
- Abnahme durch den Auftraggeber
- Produktivsetzung

Diese wurden jeweils mit mir abgestimmt. Die beschriebenen Unterlagen und Konzepte habe ich während der Projektphase zur Prüfung vorgelegt bekommen, sodass jederzeit Datenschutzaspekte berücksichtigt wurden. Gegen den Einsatz des Verfahrens bestehen keine datenschutzrechtlichen Bedenken.

3.3.3.3
Videoüberwachung in Schulen

Regelmäßig fragen Schulen, unter welchen Bedingungen sie Videoaufzeichnungen anfertigen dürfen. Mal geht es um Graffitis an den Gebäuden, mal um Diebstähle am Fahrradständer, Vandalismus in den Schultoiletten oder Rauschgifthandel auf den Schulhöfen.

Der Einsatz von Videotechnik stellt eine automatisierte Verarbeitung personenbezogener Daten dar. Als Rechtsgrundlage kommt § 14 Abs. 4 Nr. 2 HSOG in Frage.

§ 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 Hausrechtes. Abs. 1 Satz 2 und 3, Abs. 3 Satz 2 und 3 sowie § 15 des Hessischen Datenschutzgesetzes gelten entsprechend.

§ 14 Abs. 4 Nr. 2 HSOG erlaubt die Videoüberwachung zum Schutz einer besonders gefährdeten öffentlichen Einrichtung. Schulen sind nicht per se besonders gefährdete öffentliche Einrichtungen. Es reicht deshalb nicht aus, dass die Schule mit der Videoanlage (nur) ihre allgemeine Aufsichts-

pflicht unterstützen will oder einmal eine Rangelei auf dem Schulhof nicht aufklären konnte, die ansonsten mittels der Videotechnik hätte aufgeklärt werden können. Es müssen schon so schwerwiegende Beeinträchtigungen vorliegen, dass der Einsatz von Videotechnik zum Schutz der Einrichtung erforderlich und in Abwägung mit dem Rechtseingriff bei den Personen, deren Verhalten aufgezeichnet wird, verhältnismäßig ist.

Der Einsatz kommt in Betracht, wenn in der Vergangenheit schwere Sachbeschädigungen in dem zur Überwachung vorgesehenen Bereich aufgetreten sind oder wenn besonders schweren oder häufigen Straftaten oder Bedrohungen entgegengewirkt werden soll (BVerwG Urteil vom 25. Januar 2012, BVerwGE 141, 329). Für die Beurteilung der Verhältnismäßigkeit spielt die Eingriffstiefe der Maßnahme eine Rolle. Der Rechtseingriff ist gering, wenn es sich um eine Einbruchssicherung handelt und die Kameras nur außerhalb des Schulbetriebes, in den Ferien oder nur nachts in Betrieb genommen werden. Anders zu beurteilen sind Anlagen, die regelmäßig Schüler und Lehrer aufzeichnen.

§ 14 Abs. 4 HSOG erlaubt den Videoeinsatz den Gefahrenabwehrbehörden. Nach Satz 2 zählt dazu auch der Inhaber des Hausrechts. Bei Schulen ist das der Schulträger. Er muss abwägen, ob die Umstände die Annahme einer besonders gefährdeten Einrichtung rechtfertigen, der Einsatz im konkreten Fall verhältnismäßig ist und er ist verantwortlich für die Erstellung eines Verfahrensverzeichnisses nach § 28 Abs. 1 HSOG. Er kann nicht das Hausrecht, aber das Betreiben der Anlage auf die Schulleitung übertragen. Wegen der Geltung des Polizeirechts statt des allgemeinen Datenschutzrechtes findet keine förmliche Vorabkontrolle nach § 7 Abs. 6 HDSG statt. An die Stelle des Verfahrensverzeichnisses nach § 6 HDSG tritt das Verfahrensverzeichnis nach § 28 HSOG. Es ist dem schulischen Datenschutzbeauftragten vorzulegen und kann dort grundsätzlich von jeder Person eingesehen werden.

Der Schulträger hat nach § 14 Abs. 4 Satz 3 i. V. m. Abs. 3 Satz 3 HSOG spätestens alle zwei Jahre zu prüfen, ob die Voraussetzungen immer noch vorliegen, die den Einsatz einer fest installierten Videoanlage ursprünglich gerechtfertigt haben. Außerdem hat er den Umstand der Überwachung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen (§ 14 Abs. 4 Satz 3 i. V. m. Abs. 3 Satz 2 HSOG).

Werden auch die Daten von Beschäftigten aufgenommen, ist zusätzlich § 34 HDSG zu beachten. Nach § 34 Abs. 5 HDSG ist der Personalvertretung das Verfahrensverzeichnis vorzulegen, wobei gem. § 28 Abs. 3 HSOG an die Stelle des in § 34 Abs. 5 HDSG genannten Verfahrensverzeichnisses nach § 6 HDSG das Verfahrensverzeichnis nach § 28 Abs. 1 HSOG tritt. Die

Personalvertretung muss darauf hingewiesen werden, dass sie eine Stellungnahme des Hessischen Datenschutzbeauftragten fordern kann.

Um Gefährdungen für die Persönlichkeitsrechte der Betroffenen zu minimieren, sind Vorkehrungen zu treffen, die den Zugang zu den Aufzeichnungen regeln. Die Aufzeichnungen dürfen nur zweckgebunden verarbeitet werden, also zur Abwehr einer Gefahr, zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung. Der Zugang zu den Aufzeichnungen sollte passwortgeschützt sein und nur bestimmten einzelnen Funktionsträgern eingeräumt werden. Zugriffe sind zu protokollieren.

Keine Einwände hatte ich gegen die Einrichtung je einer Videoüberwachung an zwei Schulen des Landkreises Limburg-Weilburg, deren Ziel es ist, das jeweilige Objekt vor Schäden außerhalb der üblichen Betriebszeiten zu schützen und im Falle eines Schadens die Verantwortlichen zu ermitteln bzw. die Strafverfolgung zu unterstützen. Das Verfahren war vorbildlich und ausführlich beschrieben. Detailliert waren die aufgetretenen Schäden durch schwere Diebstähle, Schäden an Fenstern und Türen, ein Diebstahl aus Lagerräumen sowie Graffiti-Schäden aufgezeigt. Die Videodaten werden nur wenige Tage vorgehalten. Es sind Schilder mit Piktogrammen, den Überwachungszeiten und Angabe des Betreibers aufgestellt. Der Zugang zu den Aufzeichnungen muss von einer autorisierten Person freigeschaltet werden. Der Datenschutzbeauftragte des Landkreises ist beim Zugriff auf die Aufzeichnungen zu beteiligen, und jeder Datenzugriff wird dokumentiert.

Einwände hatte ich allerdings gegen eine Videoanlage einer berufsbildenden Schule. Aufgezeichnet wurden die Zugänge zu den Toilettenanlagen während des Schulbetriebes. Außerdem sollte eine Kamera eine Ledercouch, die im Aufenthaltsraum der Schüler aufgestellt war, vor Beschädigungen schützen. Die Einstufung des Objektes als eine besonders gefährdete öffentliche Einrichtung konnte ich nicht teilen. Die Anlage wurde abgebaut.

3.3.3.4
Einverständniserklärung zur Veröffentlichung von Schülerdaten im Internet

Die Veröffentlichung von Fotos von Schülerinnen und Schülern z. B. im Internet durch Schulen ist nicht vom Bildungs- und Erziehungsauftrag der Schulen gedeckt. Deshalb müssen Schülerinnen und Schüler bzw. deren Erziehungsberechtigte in die Veröffentlichung einwilligen. Der Beitrag enthält ein Beispiel für eine Einverständniserklärung, die alle gesetzlich vorgeschriebenen Elemente berücksichtigt.

Schulen werben öffentlich um Anerkennung und Sympathie und gehen dazu über, ihren Schulalltag im Internet öffentlich zu machen. Es werden z. B. Klassenbilder veröffentlicht und über Klassenfahrten oder Schulprojekte oder besondere Leistungen und Auszeichnungen einzelner Schüler berichtet. Diese Veröffentlichung personenbezogener Daten zum Zwecke der Selbstdarstellung der Schulen kann aber nicht mehr dem allgemeinen Bildungs- und Erziehungsauftrag nach § 83 Abs. 1 des Hessischen Schulgesetzes zugeordnet werden. Auch die nach derselben Vorschrift noch zulässige Datenverarbeitung zum Zwecke schulorganisatorischer Maßnahmen liegt nicht vor.

Eine solche Datenübermittlung ist nur zulässig, wenn der Betroffene in die Datenverarbeitung eingewilligt hat. Damit diese Einwilligung auch gültig ist, muss sie schriftlich, freiwillig und informiert erfolgen (§ 7 Abs. 2 HDSG).

Bei der Veröffentlichung von Lichtbildern im Internet ist es wegen der Schwere und Dauer der Auswirkungen auf das Persönlichkeitsrecht geboten, von der allgemein vorgegebenen Schriftform nicht abzuweichen. Die Betroffenen sind unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und auch jederzeit mit Wirkung für die Zukunft widerrufen können. Zur „Informiertheit“ gehört, dass die vorgesehene Veröffentlichung so konkret wie möglich in Bezug auf den Umfang (Lichtbild, Klasse, Namen und weiteres) als auch auf den vorgesehenen Verbreitungsgrad (z. B. Internet, passwortgeschützter Teil der Homepage, Tageszeitung) beschrieben wird. Bei einer Veröffentlichung im Internet ist es geboten, auf die Gefahr des Kopierens und Verfälschens des Lichtbildes hinzuweisen.

Bei Grundschülern genügt die Einwilligung eines Erziehungsberechtigten. Die Thematik, dass ab einem bestimmten Grad der Einsichtsfähigkeit die jugendlichen Schülerinnen und Schüler ebenfalls einwilligen müssen, habe ich bereits in meinem 40. Tätigkeitsbericht (Ziff. 3.6.4) behandelt.

Das nachstehende Beispiel einer Einwilligungserklärung enthält alle gesetzlich vorgegebenen Elemente einer gültigen Einwilligung. Der Text der Erklärung ist auf das tatsächliche Vorhaben anzupassen.

Veröffentlichung von Fotos und anderen personenbezogenen Daten

Information

Die XY-Schule beabsichtigt, Fotos von ihren Schülerinnen und Schülern zu erstellen und auf ihrer Homepage www.xyschule.de zu veröffentlichen. Dies kann auch schulische Leistungsprodukte (z. B.: Zeichnungen) und andere personenbezogene Daten der Schülerinnen und Schüler (z. B.: Name, Klasse) betreffen. Zweck hierfür ist eine öffentlichkeitswirksame Darstellung der Schule und das Betreiben einer Kommunikationsplattform für die Schule und ihre Schülerinnen und Schüler.

Dies ist eine Erhebung, Speicherung und Übermittlung von personenbezogenen Daten gemäß § 2 Abs. 2 Nr. 1-3 HDSG. Eine solche Datenverarbeitung bezüglich der Abbildung von Schülern zählt weder zu den Schulverwaltungsaufgaben, noch ist sie durch den Bildungs- und Erziehungsauftrag gedeckt. Daher ist eine schriftliche Einwilligung des Betroffenen bzw. seiner Erziehungsberechtigten einzuholen (§ 7 Abs. 1 HDSG).

Die Einwilligung ist freiwillig. Eine Ablehnung führt zu keinen Nachteilen. Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft nach § 7 Abs. 2 HDSG widerrufen werden. Des Weiteren kann die Einwilligung unter Bedingungen oder Auflagen erteilt werden.

Spätestens nach Eintritt der Volljährigkeit ist die Einwilligung der Betroffenen selbst einzuholen. Frühestens kann dies nach Vollendung des 14. Lebensjahres und einer ausreichenden Einsichtsfähigkeit des Kindes erfolgen.

Auf die speziellen Gefahren des Internets wird hingewiesen. Das Internet ermöglicht weltweit jedermann Zugriff auf die eingestellten Inhalte. Diese können weiterverarbeitet werden und sind auch der Gefahr des Missbrauchs ausgesetzt. So können z. B. Daten zur Person mit anderen Daten beliebig verknüpft werden. Auch nach einer Löschung der Daten in der Originalquelle können diese immer noch im Internet an anderer Stelle auffindbar sein.

Einwilligung

Name der Schülerin / des Schülers: ……..

Klasse: ……

Ich erkläre mich mit der Erstellung von Fotos und deren Veröffentlichung auf der Homepage der XY-Schule einverstanden. Auch mein Name und die von mir besuchte Klasse der Schule darf dabei genannt werden.

Bedingungen oder Auflagen:

……..

……..

Unterschrift

……..

Ort, Datum *Schüler*

……..

Ort, Datum *Erziehungsberechtigter*

3.3.4
Statistik

3.3.4.1
Zensus 2011 – Abschluss der Erhebung und Erfassung der Daten

Der Zensus (Volkszählung) 2011 wurde im vergangen Jahr hinsichtlich der Datenerhebung und deren Aufbereitung weitgehend abgeschlossen. Datenschutzrechtlich von Bedeutung war in dieser zweiten Phase die Schließung der 33 hessischen Erhebungsstellen, die Befragung zur Klärung von Unstimmigkeiten, die Löschung der personenbezogenen Daten bei den externen Dienstleistern, die Vernichtung aller dort verwendeten Datenträger sowie die Überprüfung der Erhebungsstelle des Statistischen Landesamtes.

3.3.4.1.1
Erhebungsstellen

3.3.4.1.1.1
Erhebungsstelle des HSL

Vor der Einrichtung seiner Erhebungsstelle ist das HSL an mich herangetreten, um die Anforderungen an die räumlich-organisatorische Trennung in dem dafür vorgesehenen Gebäudekomplex im notwendigen Umfang abzustimmen. Neben den Maßnahmen zur Zugangskontrolle, wie der Sicherung aller Türen durch eine Alarmanlage, der Überwachung des Innenhofs durch eine Kamera, einer besetzten Pforte sowie der Zusatzsicherung an „gefährdeten“ Fenstern, war es unvermeidlich, dass allen Beschäftigten anderer Institutionen, die bis dahin in diesen Gebäuden ihren Arbeitsplatz hatten, andere Büroräume zugewiesen wurden.

Im Ergebnis standen die Räumlichkeiten exklusiv nur für die Arbeit der Erhebungsstelle zur Verfügung, ein Zutritt durch Unbefugte war durch die technischen Maßnahmen und organisatorischen Rahmenbedingungen hinreichend ausgeschlossen.

Bei einer Prüfung im Laufe des vergangenen Jahres konnten sich meine Mitarbeiter davon überzeugen, dass die technische Umsetzung zur „Abschottung“ der Statistikstelle den konzeptionellen Anforderungen, die das HSL auch für die kommunalen Erhebungsstellen entwickelt hatte, entsprach.

In dem Gebäude wurde ein geschütztes DV-Subnetz nur für die Erhebungsstelle eingerichtet. Alle Arbeitsplätze wurden als sogenannte laufwerkslose Thin-Clients realisiert, an deren USB-Ports nur die durch eine Kontrollsoftware zugelassenen Komponenten erfolgreich angeschlossen

werden konnten. Zwischenergebnisse wurden nur auf einem gesonderten Erhebungsstellen-Server in den durch Profile vorgegebenen Verzeichnissen abgelegt. Die Mitarbeiter der Erhebungsstelle waren in eingeschränktem Umfang an das Mail-System des HSL angebunden, so dass ihnen nur ein definierter Empfängerkreis im HSL zur Verfügung stand.

Alle Datenflüsse von oder zur Erhebungsstelle waren über ein Firewall-Regelwerk abgesichert. Darüber wurde auch der exklusive Zugriff der Erhebungsstellen-Arbeitsplätze auf das zentrale Portal des Zensus in Nordrhein-Westfalen gesteuert. Zugriffe von anderen Arbeitsplätzen des HSL auf dieses Portal waren bis auf einen notwendigen Administratorenzugang nicht möglich.

Damit auch in der Erhebungsstelle Einzelfragen über eine Internetrecherche geklärt werden konnten, standen einzelne separate Rechner mit sicherem Internetzugang in der Erhebungsstelle zur Verfügung, die vom Erhebungsstellen-Netz getrennt waren.

3.3.4.1.1.2
Schließung der Erhebungsstellen

Nach den Vorgaben des Zensusgesetzes sollten alle hessischen Erhebungsstellen in den Städten und Landkreisen zum 31. Mai vergangenen Jahres ihre Tätigkeit beendet und die Einrichtung aufgelöst haben. Nur wenige Stellen konnten die zeitliche Vorgabe einhalten. Die meisten Organisationseinheiten beendeten im Juni ihre Tätigkeit. Nur ein Kreis konnte seine Stelle erst im Juli vergangenen Jahres schließen. Trotz dieser – nicht unerheblichen – zeitlichen Verzögerung verlief dieser Prozess geordnet und in der Regel planmäßig. An mich herangetragen wurden zu diesem Komplex keine Beschwerden. Das mag auch daran gelegen haben, dass die zuständigen Mitarbeiter meiner Behörde im Jahr 2011 mit der datenschutzrechtlichen Prüfung aller Erhebungsstellen in Hessen möglichen Unzulänglichkeiten von vorneherein die Grundlage entzogen. Alle schriftlichen Unterlagen wurden entweder vor Ort vernichtet oder zum HSL transportiert.

3.3.4.1.2
Einzelstatistische Erhebungen

3.3.4.1.2.1
Befragung zur Klärung von Unstimmigkeiten

Für diese Befragung, die Bestandteil der sog. Haushaltsstichprobe war, die den Umfang von 10 % der hessischen Bevölkerung hatte, waren etwas über

22.000 Anschriften ausgewählt worden. Fast 68.000 Fragebogen wurden von den auskunftspflichtigen Personen ausgefüllt. Ziel dieses Erhebungsteils war es, Unstimmigkeiten zwischen den vorgefundenen, tatsächlichen Verhältnissen und dem Melderegistereintrag einer Anschrift aufzuklären. Dieses Vorhaben verlief datenschutzrechtlich weitgehend geräuschlos. Nur in wenigen Fällen musste ich irritierte Bürgerinnen und Bürger aufklären und die Rechtmäßigkeit der vom Statistischen Landesamt organisierten und den Erhebungsstellen durchgeführten Maßnahme bestätigen.

3.3.4.1.2.2
Wiederholungsbefragung

Die sogenannte Wiederholungsbefragung, bei der etwa 8.000 Anschriften gezogen und die dort lebenden Haushalte einer weiteren Befragung unterzogen wurden, hat nur in Einzelfällen dazu geführt, dass betroffene Bürgerinnen und Bürger bei meiner Dienststelle Rückfragen stellten bzw. Beschwerden formulierten. Die Erhebung, welche der Qualitätskontrolle der Haushaltsstichprobe diente, wurde mit nicht unerheblichem Aufwand betrieben. So waren nochmals mehr als 300 Erhebungsbeauftragte hessenweit unterwegs, die einen Rücklauf von fast 30.000 Erhebungsbogen initiierten.

3.3.4.1.2.3
Gebäude- und Wohnungszählung

Die Hauptphase dieser Totalerhebung aller Gebäude- und Wohnungseigentümer war bis Herbst 2011 beendet. Im Nachgang und damit bis in das Frühjahr 2012 hinein wurden durch das Hessische Statistische Landesamt etwa 12.000 Zwangsgeldverfahren eingeleitet. Mit dieser Maßnahme wurden 75 % der Betroffenen veranlasst, den Bogen auszufüllen. Die verbliebenen 3.000 Eigentümer wurden auf ihre Verhältnisse hin geschätzt. Damit haben die Statistiker eine Erfassungsquote von 99,93 % erreicht. Die Beschwerden im Rahmen der heißen Phase der Gebäude- und Wohnungszählung hielten sich in Grenzen. Dies betrifft auch die eingeleiteten Zwangsgeldverfahren. In allen Fällen, die an mich herangetragen wurden, konnte ich den Betroffenen den Auskunftsanspruch der amtlichen Statistik vermitteln.

3.3.4.1.3
Vernichtung und Löschung personenbezogener Daten bei externen Dienstleistern

Hinsichtlich der geplanten und Ende des Jahres 2011 teilweise eingeleiteten Vernichtungs- und Löschungsprozeduren bei externen Dienstleistern

habe ich mich bereits im 40. Tätigkeitsbericht (Ziff. 3.7.2.2.3) geäußert. Gegen Ende des Jahres 2012 war ein großer Teil der Belege vernichtet, die Datenträger (Festplatten) durch Fachbetriebe datenschutzgerecht entsorgt worden.

3.3.4.1.3.1
Dienstleistung Versand der Unterlagen und Mahnverfahren

Für diesen Teil der Ablauforganisation hatten einige Statistische Landesämter (Sachsen, Sachsen-Anhalt, Thüringen, Rheinland-Pfalz und Hessen) ein Tochterunternehmen der Deutschen Post beauftragt. Millionen von Personendatensätzen wurden von den Landesämtern in ein Rechen- und Druckzentrum nach Einbeck in Niedersachsen übermittelt, um dort die Erhebungsbogen zur Gebäude- und Wohnungszählung zu personalisieren und zu versenden. Auch das Mahnverfahren, also auch der nochmalige Versand von Fragebogen, wurde hier abgewickelt. Gespeichert wurden die Daten der Gebäude- und Wohnungseigentümer auf für jedes Bundesland separat eingerichteten Festplatten (s. hierzu auch 40. Tätigkeitsbericht, Ziff. 3.7.2.2.1). Nach dem Abschluss des Mahnverfahrens wurden die Festplatten sowie alle Sicherungskopien unter der Aufsicht der Mitarbeiter eines Statistischen Landesamtes von einem Fachbetrieb zerstört. Sämtliche, im Produktionsprozess temporär gespeicherten Daten wurden gelöscht. Der Auftragnehmer bestätigte den Statistischen Landesämtern in einer schriftlichen Erklärung, dass nach der Löschung der Daten bzw. der Vernichtung der Datenträger keine Daten aus der Produktion „Zensus“ auf dessen Systemen mehr gespeichert waren.

3.3.4.1.3.2
Dienstleistung Erfassung der Bogen der Gebäude- und Wohnungszählung und der Hauhaltsbefragung

Millionen von Fragebogen der Gebäude- und Wohnungszählung, aber auch der 10 %-Stichprobe der Hauhaltsbefragung, wurden von einem Unternehmen in Hallstadt bei Bamberg erfasst (s. a. 40. Tätigkeitsbericht, Ziff. 3.7.2.2.2). Zur Lagerung der Bogen, aber auch zu Spitzenzeiten der Erfassung wurden Partnerunternehmen im Konzernverbund mit eingeschaltet. Diese Unternehmen verarbeiteten die Daten allerdings auf Geräten, welche der Hauptauftragnehmer zur Verfügung stellte oder die Daten wurden, wie bei dem zweiten involvierten Unternehmen geschehen, mittels einer Terminalserver-Emulation bearbeitet. Das hatte zur Konsequenz, dass diese Unternehmen keine Zensus-Daten auf eigenen Medien bearbeiten mussten und sich somit eine (auch temporäre) Speicherung von Zensus-Daten nicht

ergab. Die Bogen lagerten nach der Erfassung in Bamberg selbst bei einem der Partnerunternehmen. Nach ausdrücklicher Freigabe durch die Statistischen Landesämter begann die Vernichtung der Bogen im Frühjahr 2012 und endete im Dezember 2012. Neben den physischen Belegen waren auch alle Datenträger, die für den Produktionsprozess „Zensus“ eingesetzt wurden, datenschutzgerecht zu entsorgen. In Anwesenheit von Mitarbeitern der Statistischen Landesämter wurde dieser abschließende Arbeitsschritt vollzogen. Den Auftraggebern wurde auch für diese Arbeitsphase eine schriftliche Bestätigung über die Vernichtung und Löschung aller erhaltenen bzw. verarbeiteten Daten sowie Datenträger ausgehändigt.

3.3.4.1.3.3
Anmerkungen zur Einschaltung externer Dienstleister

Die Frage nach der rechtlichen Zulässigkeit einer externen Verarbeitung von Volkszählungsdaten wurde unter den Datenschutzbeauftragten von Bund und Ländern wiederholt kontrovers diskutiert. Ich hatte mich im Vorfeld des Zensus hierzu frühzeitig geäußert und meine Rechtsauffassung, wonach eine derartige Verarbeitung ohne Verletzung der Statistikgesetze oder des HDSG möglich sei, öffentlich gemacht (s. a. 39. Tätigkeitsbericht, Ziff. 3.3.4). Unabhängig hiervon wird sich für den nächsten Zensus die Frage nach Verbesserungsmöglichkeiten stellen, um eine noch datenschutzgerechtere Verarbeitung von Statistikdaten bei privaten Dritten sicherzustellen. So bleibt festzuhalten, dass künftig eine vollständige von anderen Verarbeitungsprozessen räumliche Abgrenzung erforderlich erscheint. Unter den gegebenen Verhältnissen haben die Auftragnehmer das offensichtlich Mögliche realisiert, um diesem Anspruch weitestgehend gerecht zu werden. Dennoch ergeben sich hier Optimierungsmöglichkeiten, die bei einem nächsten Zensus von den Auftraggebern sowohl eingefordert wie auch von den Auftragnehmern umgesetzt werden müssen. Im Übrigen erscheint es wegen der nunmehr gemachten Erfahrungen angezeigt, frühzeitiger als beim Zensus 2011 erfolgt, die erforderlichen Modalitäten einer externen Verarbeitung festzulegen.

3.3.4.1.4
Fazit

Das Projekt Zensus 2011 ist unter den Aspekten von Datenschutz und Datensicherheit weitgehend unproblematisch vollzogen worden. Der von meiner Dienststelle in diesem Zusammenhang erbrachte personelle Aufwand war beträchtlich. Hinsichtlich der Komplexität des Unternehmens sowie der

Einschaltung externer Dienstleister haben meine Mitarbeiter eine Fülle von Terminen wahrgenommen, etwa 40 Prüfungen durchgeführt und eine Vielzahl von Unterlagen gesichtet und bewertet. Von seinem Ablauf war der Zensus 2011 im Vergleich zu bisherigen Erhebungen völlig anders aufgebaut. Anstatt der klassischen Totalerhebung begnügte man sich im Bereich der Haushaltebefragung mit einer Stichprobe. Wesentliche, in den nächsten Quartalen anstehende Arbeitsschritte erfolgen durch die Zusammenführung der hierfür vorgesehenen Register unter Einbeziehung der Stichprobenergebnisse. Zu hinterfragen wäre datenschutzpolitisch, ob eine registergestützte Erhebung dem Gebot von Transparenz und Nachvollziehbarkeit eher entspricht als das Mittel der klassischen Totalerhebung. Eine Fragestellung, welche insbesondere auch unter statistikfachlichen Betrachtungen für die nächste Erhebung im Jahr 2021 von Bedeutung ist.

3.3.5
Sozialwesen

3.3.5.1
Mitwirkungspflichten bei der Beantragung von Sozialleistungen

Antragsteller bzw. Leistungsempfänger von Sozialleistungen sind auf Grund ihrer Mitwirkungsobliegenheiten u. a. gehalten, ihre Kontoauszüge vorzulegen. Dieses Verlangen der Sozialleistungsträger bewegt sich im Rahmen der datenschutzrechtlichen Vorschriften. Ohne Vorliegen konkreter Anhaltspunkte ist jedoch das standardmäßige Verlangen eines Sozialleistungsträgers, der Einholung von Bankauskünften zuzustimmen, rechtswidrig.

Im Berichtszeitraum erreichten mich diverse Beschwerden über Sozialleistungsträger und deren Forderung zur Vorlage von Kontoauszügen bei gleichzeitig geforderter Abgabe einer sog. „Kontoerklärung“, also einer Vollmacht zur Abfrage von Bankkonten der Antragsteller bzw. Leistungsempfänger. Die Beschwerden richteten sich im Bereich Grundsicherung für Arbeitsuchende mehrfach gegen eine hessische Optionskommune (SGB II) und im Bereich Sozialhilfe gegen Sozialämter hessischer Landkreise (SGB XII).

Konkreter Gegenstand der Beschwerden war in allen Fällen, dass die jeweiligen Sozialleistungsträger von den Betroffenen verlangten, mit ihrem Erst- bzw. Weiterbewilligungsantrag auf Sozialleistungen sowohl Kontoauszüge der letzten drei bzw. sechs Monate vorzulegen, als auch gleichzeitig der Behörde eine Bankvollmacht (Auskunftsermächtigung) zu erteilen. Entsprechende „Musteranschreiben“ bzw. Formulare der angesprochenen Behörden wurden mir hierzu vorgelegt.

3.3.5.1.1
Vorlage von Kontoauszügen

Nach § 60 SGB I hat derjenige, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen. Weiterhin sind Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen.

§ 60 SGB I

(1) Wer Sozialleistungen beantragt oder erhält, hat

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

Satz 1 gilt entsprechend für denjenigen, der Leistungen zu erstatten hat.

(2) Soweit für die in Absatz 1 Satz 1 Nr. 1 und 2 genannten Angaben Vordrucke vorgesehen sind, sollen diese benutzt werden.

Kontoauszüge sind Beweisurkunden, jedenfalls aber ein Beweismittel im Sinne dieser Vorschrift. Die Vorlagepflicht ist insofern auch nicht auf konkrete Verdachtsfälle beschränkt. Ebenso wenig ist die Vorlagepflicht nicht durch § 65 SGB I begrenzt.

§ 65 SGB I

(1) Die Mitwirkungspflichten nach den §§ 60 bis 64 bestehen nicht, soweit

1. *ihre Erfüllung nicht in einem angemessenen Verhältnis zu der in Anspruch genommenen Sozialleistung oder ihrer Erstattung steht oder*
2. *ihre Erfüllung dem Betroffenen aus einem wichtigen Grund nicht zugemutet werden kann oder*
3. *der Leistungsträger sich durch einen geringeren Aufwand als der Antragsteller oder Leistungsberechtigte die erforderlichen Kenntnisse selbst beschaffen kann.*

Antragsteller bzw. Leistungsempfänger sind auf Grund der auch im SGB II und SGB XII geltenden Mitwirkungsobliegenheiten gemäß §§ 60 ff. SGB I gehalten, ihre Kontoauszüge vorzulegen. Mit diesem Vorlageverlangen halten sich Sozialleistungsträger regelmäßig im Rahmen der datenschutzrechtlichen Vorschriften gemäß § 35 SGB I (Sozialgeheimnis) und §§ 67 ff.

SGB X (Schutz der Sozialdaten), wenngleich § 67 Abs. 12 SGB X hinsichtlich der dort genannten besonderen Daten weitere Schutzvorkehrungen zu Gunsten des Betroffenen gebietet (hierzu nachfolgend noch Anmerkungen).

Bestätigt wird dies durch das Urteil des Bundessozialgerichtes in Kassel vom 19. September 2008 (Entscheidung des 14. Senats, Az.: B 14 AS 45/07 R), in dem das Gericht zur Feststellung der Berechtigung zur Anforderung von Kontoauszügen durch die Sozialbehörden ausführt:

Von daher liegt es auf der Hand, dass es im Rahmen eines aus Steuermitteln finanzierten Fürsorgesystems, das strikt an die Hilfsbedürftigkeit der Leistungsempfänger als Anspruchsvoraussetzung anknüpft, keine unzumutbare und unangemessene Anforderung darstellt, Auskunft über den Bestand an Konten und die Kontenbewegungen (durch die Vorlage von Kontoauszügen) zu geben, jedenfalls soweit die Einnahmeseite betroffen ist (…). Dies gilt auch für den Fall, dass der Betroffene schon Leistungen bezogen hat und Grundsicherungsleistungen für Folgezeiträume geltend macht. Angesichts der Vielfalt jederzeit möglicher Änderungen gibt es für eine differenzierende Beurteilung der Vorlagepflicht keinen Grund. Dies gilt auch in zeitlicher Hinsicht, jedenfalls soweit – wie hier – Kontoauszüge für die letzten drei Monate angefordert worden sind. Der Senat hat nicht darüber zu befinden, inwieweit die Vorlagepflicht von Kontoauszügen für die letzten zwölf Monate noch im Rahmen des § 65 SGB I hinnehmbar wäre (anders LSG Niedersachsen-Bremen, Beschluss vom 12. Juli 2007 – L 6 AS 378/07 ER). Gegen die Aufforderung, die Kontoauszüge für die letzten drei Monate vorzulegen, bestehen aber keine grundsätzlichen Bedenken.

Einschränkungen der Auskunftsobliegenheit bei Kontoauszügen ergeben sich aus § 67 Abs. 12 SGB X i. V. m. § 67a Abs. 1 Satz 2 SGB X. Nach § 67a Abs. 1 Satz 2 SGB X ist für besondere Arten personenbezogener Daten gesondert zu prüfen, ob deren Kenntnis zur Erfüllung der Aufgabe der erhebenden Stelle erforderlich ist. § 67 Abs. 12 SGB X nennt als besondere Arten personenbezogener Daten Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

§ 67 SGB X

(12) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

§ 67a SGB X

(1) Das Erheben von Sozialdaten durch in § 35 des Ersten Buches genannte Stellen ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. Dies gilt auch für besondere Arten personenbezogener Daten (§ 67 Abs. 12). Angaben über die rassische Herkunft dürfen ohne Einwilligung des Betrof-

fenen, die sich ausdrücklich auf diese Daten beziehen muss, nicht erhoben werden. Ist die Einwilligung des Betroffenen durch Gesetz vorgesehen, hat sie sich ausdrücklich auf besondere Arten personenbezogener Daten (§ 67 Abs. 12) zu beziehen.

Für die Erfüllung der gesetzlichen Aufgaben des Sozialleistungsträgers – z. B. bei der Grundsicherung die Sicherung des Lebensunterhalts und Eingliederung in Arbeit, vgl. § 1 Abs. 2 SGB II – ist es nicht erforderlich, dass dieser Kenntnis über das Ausgabeverhalten der Sozialleistungsempfänger in den in § 67 Abs. 12 SGB X genannten Bereichen erlangt. Dies gilt insbesondere hinsichtlich der Adressaten/Empfänger der Zahlungen. Geht etwa aus den Empfängerangaben hervor, dass der Sozialleistungsempfänger Beiträge an eine politische Partei, Gewerkschaft oder Religionsgemeinschaft überweist, so ist die Kenntnis der jeweils begünstigten Partei, Religionsgemeinschaft etc. für die Aufgaben des Grundsicherungsträgers grundsätzlich irrelevant.

Allerdings muss im Hinblick auf die Regelungen in § 31 Abs. 4 Nr. 1 und Nr. 2 SGB II a. F. (heute Abs. 2), die Sanktionen bei unwirtschaftlichem Verhalten des Hilfebedürftigen vorsehen, gewährleistet bleiben, dass die vom jeweiligen Sozialleistungsempfänger überwiesenen Beträge der Höhe nach erkennbar bleiben. Geschützt ist mithin nur die Geheimhaltung des Verwendungszwecks bzw. des Empfängers der Überweisung, nicht deren Höhe (vgl. Urteil des Bundessozialgerichts vom 19. Februar 2009 – B 4 AS 10/08 R, Rdnr. 20).

§ 31 SGB II

...

(2) Eine Pflichtverletzung von erwerbsfähigen Leistungsberechtigten ist auch anzunehmen, wenn

1. *sie nach Vollendung des 18. Lebensjahres ihr Einkommen oder Vermögen in der Absicht vermindert haben, die Voraussetzungen für die Gewährung oder Erhöhung des Arbeitslosengeldes II herbeizuführen,*
2. *sie trotz Belehrung über die Rechtsfolgen oder deren Kenntnis ihr unwirtschaftliches Verhalten fortsetzen,*
3. *ihr Anspruch auf Arbeitslosengeld ruht oder erloschen ist, weil die Agentur für Arbeit das Eintreten einer Sperrzeit oder das Erlöschen des Anspruchs nach den Vorschriften des Dritten Buches festgestellt hat, oder*
4. *sie die im Dritten Buch genannten Voraussetzungen für das Eintreten einer Sperrzeit erfüllen, die das Ruhen oder Erlöschen eines Anspruchs auf Arbeitslosengeld begründen.*

Eine Vorlage von Kontoauszügen der letzten drei Monate war schon vor diesem Grundsatzurteil, auch datenschutzrechtlich als nicht unverhältnismäßig akzeptiert (a. A. nur Hessisches Landessozialgericht, Beschluss vom

22. August 2005 – L 7 AS 32/05 ER). Auch die Vorlage von Kontoauszügen der letzten sechs Monate ist nach meiner Auffassung regelmäßig noch zulässig.

Es kann in diesem Zusammenhang auch nicht vorgebracht werden, aus dem Rechtsgedanken des § 65 SGB I sei abzuleiten, dass zunächst ein konkreter Verdacht auf einen Leistungsmissbrauch vorliegen müsse, damit ein entsprechendes Mitwirkungsbegehren des Sozialleistungsträgers rechtmäßig sein kann. Diese Voraussetzung kann dem Wortlaut des § 60 Abs. 1 Satz 1 Nr. 3 SGB I nicht entnommen werden. Auch aus § 65 SGB I kann keine Einschränkung der Mitwirkungsobliegenheit dahingehend abgeleitet werden, dass nur bei einem konkreten Verdacht jeweils die Vorlage von bestimmten Beweisurkunden vom Sozialleistungsempfänger gefordert werden könne. Die Mitwirkungsobliegenheiten der §§ 60 ff. SGB I bestehen grundsätzlich unabhängig vom Vorliegen von Verdachtsmomenten gegen den Leistungsempfänger. Die geforderten Unterlagen in Form von Kontoauszügen sind auch nicht unverhältnismäßig schwer beizubringen (vgl. Urteil des Bundessozialgerichts vom 19. Februar 2009 – B 4 AS 10/08 R, Rdnr. 18).

3.3.5.1.2
Bankvollmacht/Zustimmung zur Einholung von Bankauskünften

Von der Aufforderung zur Vorlage von Kontoauszügen zu trennen ist die vielfach ebenfalls „standardmäßig“ abgeforderte Zustimmung zur Einholung von Bankauskünften.

Allein die Tatsache der Beantragung von Sozialleistungen (und der Verpflichtung zu wahrheitsgemäßen Angaben hierbei) als solche reicht grundsätzlich nicht aus, um den Angaben des Antragstellers in seinem schriftlichen Antrag auf Gewährung von Sozialleistungen keinen Glauben zu schenken. Die zur Prüfung der Anspruchsvoraussetzung für den Erhalt von Sozialleistungen erforderlichen Entscheidungsgrundlagen stehen aufgrund der Angaben des Antragstellers zu seinen persönlichen und wirtschaftlichen Verhältnissen grundsätzlich fest. Zusätzlicher behördlicher Ermittlungen durch den Sozialleistungsträger bedarf es daher hier nicht. Ein pauschaler Allgemeinverdacht gegenüber den von einem Hilfesuchenden abgegebenen Erklärungen und Angaben ist nicht ausreichend, um dem Hilfesuchenden eine besondere Beweisführung aufzugeben.

Ohne Vorliegen konkreter Anhaltspunkte ist das Verlangen, der Einholung von Bankauskünften zuzustimmen, eine überflüssige Ermittlungstätigkeit des Sozialhilfeträgers und somit nicht „erforderlich“ im Sinne von § 60

Abs. 1 Nr. 1 SGB I (Leitsatz des Beschlusses des HessVGH vom 7. Februar 1995 – 9 TG 3113/94).

Auch die Befugnis des Sozialleistungsträgers, im Rahmen des ihm nach § 20 SGB X eingeräumten Ermessens, über das Ausmaß der Ermittlungen zu entscheiden, bedeutet nicht, dass die Behörde auf der Grundlage einer nicht näher begründeten pauschalen Verdächtigung grundsätzlich davon ausgehen darf, die von dem Hilfesuchenden abgegebene Erklärung über seine Einkommensverhältnisse und Vermögensverhältnisse könnten unwahr sein, um sich auf diese Weise in betrügerischer Absicht Sozialleistungen zu erschleichen.

§ 20 SGB X

(1) Die Behörde ermittelt den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen; an das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden.

(2) Die Behörde hat alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände zu berücksichtigen.

(3) Die Behörde darf die Entgegennahme von Erklärungen oder Anträgen, die in ihren Zuständigkeitsbereich fallen, nicht deshalb verweigern, weil sie die Erklärung oder den Antrag in der Sache für unzulässig oder unbegründet hält.

Der Umfang der Ermittlungspflicht ist jedoch nicht in das Belieben der Behörde gestellt. Dies ergibt sich eindeutig aus der amtlichen Begründung zu § 20 SGB X, wonach „der Untersuchungsgrundsatz nicht bedeutet, jede Behauptung müsste bezweifelt werden und könne erst dann zugrunde gelegt werden, wenn sie bewiesen sei. Die Aufklärungspflicht beschränkt sich insoweit auf die Behebung eigener Zweifel. Die Behörde braucht daher, sofern sich nicht aus der Gesamtlage des Falles Bedenken aufdrängen, einem Tatumstand nicht durch eigene Ermittlungen nachzugehen, wenn er von niemandem bestritten wird“ (vgl. Entscheidungsgründe des Hessischen Verwaltungsgerichtshofes und BTDrucks. 8/2034 zu § 20).

Die standardmäßige Verwendung einer „Bankauskunftsklausel“ ist demnach unzulässig, egal in welcher Form und unter welchem Namen sie von einem Antragsteller abverlangt wird (vgl. v. Petersdorff, Rdnr. 25, in Roßnagel, Handbuch Datenschutzrecht, Datenschutz in der Sozialverwaltung, 2003).

Lediglich sofern konkrete Anhaltspunkte dafür sprechen, dass die Angaben des Antragstellers bzw. die von ihm vorgelegten Nachweise nicht vollständig und/oder nicht wahrheitsgemäß sind, ist gegen das Verlangen, einer Bankauskunft zuzustimmen, grundsätzlich nichts einzuwen-

den. Dem Betroffenen ist aber dann zu erläutern, warum in seinem Fall ausnahmsweise eine Bankauskunft notwendig erscheint, ob Alternativen dazu denkbar sind und welche Voraussetzungen und Folgen diese haben.

Ich habe das HSM, welches die Fachaufsicht über die hessischen Optionskommunen und Sozialämter ausübt, um Stellungnahme gebeten, ob es sich meiner Rechtsposition anschließt. Das HSM stimmt mit meiner Bewertung der Rechtslage vollständig überein und antwortete:

> *Mit Ihrer detaillierten Betrachtung und Einschätzung über die Rechtmäßigkeit von „Mitwirkungspflichten bei der Beantragung von Sozialleistungen, vor allem im Bereich SGB II und SGB XII“ aus datenschutzrechtlicher Sicht stimmen wir überein. Insbesondere Ihre Ausführungen über die Rechtmäßigkeit einer standardmäßig vom Antragsteller/in abgeforderten Zustimmung zur Einholung von Bankauskünften entsprechen unserer Rechtsauffassung.*
>
> *Auch wir halten eine solche standardmäßige Verwendung einer „Bankauskunftsklausel“ für unzulässig, egal in welcher Form und unter welchem Namen sie vom Antragsteller/in abverlangt wird. Nur bei konkreten Anhaltspunkten, d. h. bei berechtigten Zweifeln an der Vollständigkeit der vorgelegten Nachweise oder den wahrheitsgemäßen Angaben des/der Antragstellers/in, kann eine Zustimmungsverpflichtung des Betroffenen zur Einholung entsprechender Auskünfte bestehen.*
>
> *Bereits im Jahre 2006 hatten wir in einer Stellungnahme zum 34. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten zum Punkt 5.9.1 (Hartz IV – Vorlage von Kontoauszügen) unsere Zustimmung zu den erfolgten Ausführungen des Datenschutzbeauftragten erteilt. Diese Zustimmung und Stellungnahme hat auch heute noch Bestand.*

Die Beschwerdeführer habe ich jeweils per Stellungnahme über meine Rechtsauffassung informiert. In einem Rundschreiben an alle hessischen Optionskommunen und Landkreise habe ich diese allesamt über meine, vom HSM unterstützte Rechtsposition ebenfalls informiert und zur Beachtung der Vorgaben aufgefordert.

3.3.5.2
Datenübermittlung des Jobcenters an die Ausländerbehörde bei SGB II-Anträgen durch europäische Unionsbürgerinnen und -bürger

Die Frage, ob ein Jobcenter Daten an die Ausländerbehörde übermitteln darf, wenn europäische Unionsbürgerinnen oder -bürger einen Antrag auf SGB II-Leistungen stellen, betrifft nicht primär eine datenschutzrechtliche, sondern eine ausländerrechtliche Thematik. Grundsätzlich ist eine Sozialdatenübermittlung seitens des Jobcenters, soweit es für dessen Aufgabenerfüllung erforderlich ist, zulässig.

3.3.5.2.1
Der Anlass

Die behördliche Datenschutzbeauftragte eines Jobcenters bat mich um Auskunft zu dem Themenkomplex „Datenübermittlung von Sozialdaten durch den Sozialleistungsträger (hier: das Jobcenter) an die Ausländerbehörde“. Dort würden sich zunehmend Fragen in Bezug auf die Zulässigkeit der Übermittlung von Sozialdaten an das Ausländeramt ergeben, wenn ein Antrag auf SGB II-Leistungen durch nach Deutschland eingereiste Unionsbürger gestellt werde. Hintergrund sei, dass für Ausländer ein Ausschluss auf Leistungen nach dem SGB II für die ersten drei Monate nach ihrer Einreise bestehe sowie – wenn die Einreise allein zum Zwecke der Arbeitssuche erfolgt sei – auch für die anschließende Zeit. Dies bedeute im Umkehrschluss, dass grundsätzlich ein Anspruch auf Leistungen bestehe, wenn der Aufenthalt nicht dem Zweck der Arbeitssuche diene.

Nach früherer Rechtslage habe ein Anspruch auf Leistungen nach dem SGB II für Angehörige von Vertragsstaaten des Europäischen Fürsorgeabkommens EFA (die sich aus einem großen Teil der EU und auch der Türkei zusammensetzten) bestanden, unabhängig von der Frage, ob die Antragsteller „allein zum Zwecke der Arbeitssuche“ eingereist seien. Das habe sich daraus ergeben, dass Angehörige von solchen Vertragsstaaten den eigenen Staatsangehörigen in Bezug auf Sozialleistungen gleichzustellen gewesen seien und sich somit ein unmittelbarer Anspruch auf SGB II-Leistungen ergeben habe. Aufgrund eines ausgesprochenen Vorbehalts der Bundesrepublik Deutschland gegen das EFA, wonach dieses nicht mehr anzuwenden sei, stelle sich mittlerweile das Problem der Zulässigkeit der Übermittlung von Sozialdaten an die Ausländerbehörde vermehrt deshalb, weil nun öfter Leistungen abgelehnt würden als früher.

Es sei nun ansteigende Praxis bei Jobcentern, für den Fall, dass kein Ausschluss auf Leistungen nach § 7 Abs. 1 Satz 2 Nr. 2 SGB II angenommen werden könne (d. h. also eine Einreise nicht nur zum Zwecke der Arbeitssuche erfolgt ist), die Beantragung des Leistungsbezugs an das zuständige Ausländeramt zu melden. Dieses entziehe sodann die Freizügigkeit.

§ 7 Abs. 1 SGB II

Leistungen nach diesem Buch erhalten Personen, die

1. *das 15. Lebensjahr vollendet und die Altersgrenze nach § 7a noch nicht erreicht haben,*
2. *erwerbsfähig sind,*
3. *hilfebedürftig sind und*
4. *ihren gewöhnlichen Aufenthalt in der Bundesrepublik Deutschland haben (erwerbsfähige Leistungsberechtigte).*

Ausgenommen sind

1. *Ausländerinnen und Ausländer, die weder in der Bundesrepublik Deutschland Arbeitnehmerinnen, Arbeitnehmer oder Selbständige noch aufgrund des § 2 Abs. 3 des Freizügigkeitsgesetzes/EU freizügigkeitsberechtigt sind, und ihre Familienangehörigen für die ersten drei Monate ihres Aufenthalts,*
2. *Ausländerinnen und Ausländer, deren Aufenthaltsrecht sich allein aus dem Zweck der Arbeitsuche ergibt, und ihre Familienangehörigen,*
3. *Leistungsberechtigte nach § 1 des Asylbewerberleistungsgesetzes.*

Satz 2 Nr. 1 gilt nicht für Ausländerinnen und Ausländer, die sich mit einem Aufenthaltstitel nach Kapitel 2 Abschnitt 5 des Aufenthaltsgesetzes in der Bundesrepublik Deutschland aufhalten. Aufenthaltsrechtliche Bestimmungen bleiben unberührt.

In einem Fall vor dem Sozialgericht Darmstadt sei wegen der Ablehnung von Leistungen einstweiliger Rechtsschutz eingelegt worden, worauf das Gericht das Vorliegen des Merkmals der Arbeitssuche verneint habe. Die Kammer sei also davon ausgegangen, dass ein Anspruch bestehe, habe jedoch darauf hingewiesen, dass für das Jobcenter „der Zeitraum bis zum Hauptsacheverfahren genügen müsste, um eine Entscheidung der Ausländerbehörde des Antragsgegners aufgrund § 5 Abs. 5 bzw. § 6 FreizügG/EU herbeizuführen, wodurch der rechtmäßige Aufenthalt der Antragsteller im Bundesgebiet beendet würde."

Es stelle sich die Frage, ob eine solche Übermittlung aus Sicht des Jobcenters zulässig ist.

3.3.5.2.2
Bedeutung des Sozialdatenschutzes

Hinsichtlich der Problematik sind neben datenschutzrechtlichen Vorschriften auch diejenigen des Ausländer- und Aufenthaltsrechts maßgebend. Meine Stellungnahme konnte sich nur auf die Betrachtung sozialdatenschutzrechtlicher Belange konzentrieren.

Grundsätzlich gilt im Datenschutzrecht, dass jeder Austausch von Informationen/Daten und damit jede Übermittlung nur zulässig ist, wenn zwei Voraussetzungen erfüllt sind: die Stelle, die die Information haben möchte, muss sich auf eine Datenerhebungsnorm stützen können, und für die Stelle, die die Daten liefern soll, ist eine Übermittlungsnorm notwendig.

Dabei ist es nicht ausreichend, wenn es eine allgemeine gesetzliche Regelung zur Zusammenarbeit gibt. Sondern notwendig ist (auch) eine Regelung, die einen konkreten Informationsaustausch zulässt. Die Amtshilfeverpflichtung allein ist niemals Grundlage für eine Datenübermittlung. Die datenschutzrechtlichen Ge- und Verbote zum Datenaustausch gehen der Amts-

hilfe vor. Im Einzelfall kann die allgemein geltende Verpflichtung allerdings dazu führen, dass sich eine mögliche Datenübermittlung zu einer Übermittlungsverpflichtung verdichtet. Bereichsspezifische Regelungen zum Informationsaustausch gehen den allgemeinen Datenverarbeitungsnormen aus den Datenschutzgesetzen vor.

Bezogen auf vorliegende Fragestellung ist für das Jobcenter eine Übermittlungsvorschrift im SGB II nicht vorhanden – die §§ 50 bis 52a SGB II (Datenerhebung, -verarbeitung und -nutzung) sind hier nicht anwendbar. Zu prüfen ist daher, ob sich aus den Vorschriften zum Schutz der Sozialdaten aus dem Zweiten Kapitel SGB X, §§ 67 bis 85a, eine Mitteilungsbefugnis oder -verpflichtung ergibt.

Eine Übermittlung von Sozialdaten ist gemäß § 67d 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 gemäß § 67d Abs. 2 Satz 1 SGB X die übermittelnde Stelle.

§ 67d SGB X

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

(2) 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.

Vorliegend kommt (neben § 69 Abs. 1 Nr. 1, 2. Alt. SGB X; hierzu später ausführlich) als Übermittlungsvorschrift § 71 SGB X in Betracht. § 71 SGB X regelt abschließend die Fälle, in denen besondere gesetzliche Mitteilungspflichten dem Sozialgeheimnis vorgehen. Dessen Abs. 2 enthält abschließende Regelungen zur Übermittlung von Sozialdaten von Ausländern an die Ausländerbehörde. Während Abs. 2 Satz 1 Nr. 1 Buchstabe a bis d die Übermittlungen auf Ersuchen der Ausländerbehörde im Einzelfall regelt, sind in Satz 1 Nrn. 2 und 3 die Übermittlungen aufgrund von Mitteilungspflichten nach dem Aufenthaltsgesetz festgelegt.

§ 71 Abs. 2 SGB X

Eine Übermittlung von Sozialdaten eines Ausländers ist auch zulässig, soweit sie erforderlich ist

1. *im Einzelfall auf Ersuchen der mit der Ausführung des Aufenthaltsgesetzes betrauten Behörden nach § 87 Abs. 1 des Aufenthaltsgesetzes mit der Maßgabe, dass über die Angaben nach § 68 hinaus nur mitgeteilt werden können*

a) für die Entscheidung über den Aufenthalt des Ausländers oder eines Familienangehörigen des Ausländers Daten über die Gewährung oder Nichtgewährung von Leistungen, Daten über frühere und bestehende Versicherungen und das Nichtbestehen einer Versicherung,

b) für die Entscheidung über den Aufenthalt oder über die ausländerrechtliche Zulassung oder Beschränkung einer Erwerbstätigkeit des Ausländers Daten über die Zustimmung nach § 4 Abs. 2 Satz 3, § 17 Satz 1, § 18 Abs. 2 Satz 1, § 18a Abs. 1, § 19 Abs. 1 Satz 1 und § 19a Abs. 1 des Aufenthaltsgesetzes,

c) für eine Entscheidung über den Aufenthalt des Ausländers Angaben darüber, ob die in § 55 Abs. 2 Nr. 4 des Aufenthaltsgesetzes bezeichneten Voraussetzungen vorliegen, und

d) durch die Jugendämter für die Entscheidung über den weiteren Aufenthalt oder die Beendigung des Aufenthalts eines Ausländers, bei dem ein Ausweisungsgrund nach den §§ 53 bis 56 des Aufenthaltsgesetzes vorliegt, Angaben über das zu erwartende soziale Verhalten,

2. *für die Erfüllung der in § 87 Abs. 2 des Aufenthaltsgesetzes bezeichneten Mitteilungspflichten oder*
3. *für die Erfüllung der in § 99 Absatz 1 Nummer 14 Buchstabe d, f und j des Aufenthaltsgesetzes bezeichneten Mitteilungspflichten, wenn die Mitteilung die Erteilung, den Widerruf oder Beschränkungen der Zustimmung nach § 4 Abs. 2 Satz 3, § 17 Satz 1, § 18 Abs. 2 Satz 1, § 18a Abs. 1, § 19 Abs. 1 Satz 1 und § 19a Absatz 1 des Aufenthaltsgesetzes oder eines Versicherungsschutzes oder die Gewährung von Leistungen zur Sicherung des Lebensunterhalts nach dem Zweiten Buch betrifft.*

Daten über die Gesundheit eines Ausländers dürfen nur übermittelt werden,

1. *wenn der Ausländer die öffentliche Gesundheit gefährdet und besondere Schutzmaßnahmen zum Ausschluss der Gefährdung nicht möglich sind oder von dem Ausländer nicht eingehalten werden oder*
2. *soweit sie für die Feststellung erforderlich sind, ob die Voraussetzungen des § 55 Abs. 2 Nr. 4 des Aufenthaltsgesetzes vorliegen.*

Die Mitteilungspflicht nach § 71 Abs. 2 Satz 1 Nr. 2 SGB X ist von Sozialleistungsträgern ohne Anfrage der Ausländerbehörde von Amts wegen zu erfüllen und umfasst die Weitergabe von Kenntnissen über einen Ausweisungsgrund nach § 87 Abs. 2 AufenthG.

Die Mitteilungspflicht nach Abs. 2 Satz 1 Nr. 3 bezieht sich auf die Erfüllung von Mitteilungspflichten in § 99 Abs. 1 Nr. 14 Buchstaben d, f und i des AufenthG. Danach kann durch Rechtsverordnung bestimmt werden, dass Sozial- und Jugendämter der Bundesagentur für Arbeit ohne Ersuchen den Ausländerbehörden Sozialdaten von Ausländern, Amtshandlungen und sonstige Maßnahmen gegenüber Ausländern mitzuteilen haben, soweit diese Angaben zur Aufgabenerfüllung der Ausländerbehörden erforderlich sind. Die Mitteilungspflicht wird durch § 71 Abs. 2 Satz 1 Nr. 3 SGB X eingeschränkt. Sie besteht nicht umfassend für alle Aufgaben der Ausländerbehörden, sondern nur, wenn die Mitteilung u. a. die Gewährung von Leis-

tungen zur Sicherung des Lebensunterhaltes nach dem SGB II betrifft (vgl. Bergmann/Möhrle/Herb, Datenschutzrecht, Kommentar zum Sozialgesetzbuch, 42. Erg.Lfg. Januar 2011, § 71 SGB X, Rdnr. 2, 28, 30, 31).

Ausländer ist gemäß § 2 Abs. 1 AufenthG jeder, der nicht Deutscher i. S. d. Art. 116 Abs. 1 GG ist. Gemäß § 71 Abs. 2 SGB X können keine Übermittlungsbefugnisse begründet werden, soweit das AufenthG auf bestimmte Ausländer nicht anwendbar ist. Nach § 1 Abs. 2 Nr. 1 AufenthG gilt dies z. B. für Ausländer, deren Rechtsstellung von dem Freizügigkeitsgesetz (FreizügG) geregelt wird.

§ 71 Abs. 2 Satz 1 Nr. 2 SGB X gestattet den Leistungsträgern die unverzügliche Übermittlung von Sozialdaten für die Erfüllung der in § 87 Abs. 2 AufenthG bezeichneten Mitteilungspflichten. Die Übermittlungsbefugnis dieser „Spontanmitteilung“ besteht ersuchensunabhängig. Keine Übermittlungsbefugnis begründet diese Vorschrift in Hinsicht auf die Sozialdaten der Staatsangehörigen anderer Mitgliedsstaaten der Europäischen Union – der Unionsbürger nach § 1 FreizügG/EU – und ihrer Familienangehörigen. Zwar statuiert § 11 Abs. 1 Satz 2 FreizügG/EU, dass die Mitteilungspflichten nach § 87 Abs. 2 Nr. 1-3 AufenthG gleichfalls bestehen, wenn die dort genannten Umstände für die Feststellung nach §§ 5 Abs. 5, 6 Abs. 1 AufenthG entscheidungserheblich sein können. Hiermit wird zwar eine Mitteilungspflicht der Leistungsträger insoweit auch auf die Unionsbürger erstreckt, jedoch sieht Nr. 2 keine korrespondierende Befugnis vor. § 11 Abs. 1 Satz 2 FreizügG/EU läuft insoweit ins Leere (so Seidel in Diering/Timme/Waschull, LPK-SGB X, 2. Auflage 2007, § 71, Rdnr. 21, 28).

§ 11 Abs. 1 FreizügG/EU erfordert aber die Anwendung der ausländerrechtlichen Mitteilungsvorschriften nach § 87 AufenthG bei Unionsbürgern, sodass für eine Übermittlung der Sozialdaten von Unionsbürgern ebenfalls § 71 Abs. 2 SGB X gilt. Allerdings ist z. B. die Tatsache des ALG II- oder Sozialhilfebezugs bei Unionsbürgern nur dann aufenthaltsrechtlich relevant (und damit ein zulässiger Übermittlungstatbestand), wenn dies deren Freizügigkeitsrecht bzw. Aufenthaltsrecht in der Bundesrepublik Deutschland nach § 5 Abs. 5 FreizügG/EU, §§ 6 oder 7 FreizügG/EU entfallen lassen würde. Grundsätzlich kann jedoch nach Art. 14 Abs. 1 RL 2004/38 für Unionsbürger die Inanspruchnahme von ALG II oder Sozialhilfe nicht zu einer Aufenthaltsbeendigung führen. Allenfalls eine „unangemessene“ Inanspruchnahme würde dies rechtfertigen, nicht z. B. nur vorübergehende Schwierigkeiten (vgl. Weichert in Huber, § 6 FreizügG/EU, Rdnr. 30). Nach Beginn des Daueraufenthaltsstatus gem. § 4a FreizügG/EU, d. h. nach fünf Jahren rechtmäßigen Aufenthalts, rechtfertigen ohnehin nur noch „schwerwiegende Gründe“ i. S. v. schweren Gefahren für die öffentliche Sicherheit

und Ordnung eine Beendigung des Aufenthalts (vgl. Hailbronner, AuslR, § 6 FreizügG/EU, Rdnr. 55). Eine Inanspruchnahme von ALG II oder Sozialhilfe rechtfertigt diese Annahme nicht. Darüber hinaus sind Staatsangehörige der Mitgliedsstaaten des EFA vom 6. Mai 1983 (BGBl. II S. 337) besonders privilegiert. Sie dürfen gem. Art. 6 EFA auch bei Hilfebedürftigkeit grundsätzlich nicht ausgewiesen werden. Nach Maßgabe des § 23 Abs. 3 Satz 1 SGB XII besteht allerdings für Unionsbürger dann keine Freizügigkeitsberechtigung, wenn sie lediglich zum Zwecke des Sozialhilfebezugs eingereist sind. Etwas anderes gilt jedoch für Unionsbürger, die sich ohne ausreichende eigene Mittel zum Zwecke der Arbeitssuche in die Bundesrepublik Deutschland begeben haben (vgl. Sommer in Krahmer, Sozialdatenschutz nach SGB I und X, Kommentar, 3. Auflage, § 71, Rdnr. 21 und 22 unter Verweis auf Hailbronner, AuslR, § 2 FreizügG/EU, Rdnr. 49 bis 51 und Valgolio in Hauck/Noftz, § 7 SGB II, Rdnr. 122 bis 129).

Es handelt sich im Ergebnis bei der Frage, ob ein Jobcenter auf Grundlage der §§ 67d, 71 SGB X Daten zulässig übermitteln darf, nicht um eine primär datenschutz-, sondern ausländerrechtliche Fragestellung, weshalb ich eine abschließende Bewertung nicht vornehmen kann. Es ist im Einzelfall zu entscheiden, ob eine Datenübermittlung gerechtfertigt werden kann.

3.3.5.2.3
Übermittlungsbefugnis zur Erfüllung eigener Aufgaben des Jobcenters

Wenn abseits von § 71 SGB X und dafür die §§ 67d, 69 SGB X zu Grunde legend ein Jobcenter die Auffassung vertritt, dass für seine Aufgabenerfüllung bei richtigem Rechtsverständnis im Einzelfall Sozialdatenübermittlungen an die Ausländerbehörde erforderlich sind, steht als Rechtsgrundlage für diese 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.*

Die Vorschrift des § 69 SGB X beruht auf der Überlegung, dass die nach dem SGB erhobenen Sozialdaten für die Erfüllung sich aus dem SGB insgesamt ergebender Aufgaben bestimmt sind. Insoweit berücksichtigt die Norm, dass diese Aufgaben nicht von einer einheitlichen Sozialverwaltung, sondern von einer Vielzahl verschiedener Stellen wahrgenommen werden.

§ 69 Abs. 1 Nr. 1 SGB gestattet daher 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 die Übermittlung von Sozialdaten zulässig für die Erfüllung der Zwecke, für die die Daten erhoben worden sind. Nr. 2 erlaubt die Übermittlung für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach dem SGB, d. h. für die Erfüllung einer sog. Eigenaufgabe und nach Nr. 3 ist die Übermittlung für die Erfüllung einer gesetzlichen Aufgabe des Dritten, an den Daten übermittelt werden, wenn er eine in § 35 SGB I genannte Stelle ist, d. h. für die Erfüllung einer sog. Fremdaufgabe zulässig.

Die Datenübermittlung legitimiert sich aus den vorangegangenen Schritten des Datenumgangs. Da eine Datenerhebung nach § 67a Abs. 1 SGB X und eine Datenspeicherung ohne vorausgehende Erhebung nach § 67c Abs. 1 SGB X nur zulässig ist, wenn die Kenntnis der Daten zur Erfüllung einer Aufgabe nach dem SGB erforderlich ist, setzt auch die Datenübermittlung eine gesetzliche Aufgabe voraus, so dass in allen drei Fällen die Übermittlung zur Erfüllung einer gesetzlichen Aufgabe nach dem SGB durch eine in § 35 Abs. 1 SGB I genannte Stelle erforderlich ist. Voraussetzung für eine Übermittlung nach § 69 Abs. 1 Nr. 1 SGB X ist in allen drei Fällen daher, dass die Übermittlung (1.) für die Erfüllung einer gesetzlichen Aufgabe (2.) nach dem SGB (3.) erforderlich ist.

Eine Übermittlung von Sozialdaten ist im 2. Fall zulässig zur Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach diesem Gesetzbuch. Als gesetzliche Aufgabe ist jede Aufgabe anzusehen, die sich aus dem SGB insgesamt ergibt. Dabei ist es nicht erforderlich, dass eine ausdrückliche Bezeichnung als Aufgabe vorliegt, sondern es genügt, dass für die Aufgabe eine gesetzliche Grundlage i. S. d. § 31 SGB I vorhanden ist. Die Erfüllung einer nur rechtmäßigen Aufgabe genügt hier jedoch nicht. Die Voraussetzung, dass sich die Aufgabe aus einem Gesetz ergeben muss, wird nicht schon dadurch erfüllt, dass sie nicht gegen ein solches verstößt.

Wenn ein Jobcenter bei der Prüfung eines Antrags und wegen vorliegender Informationen selbst zu dem Ergebnis kommt, dass im konkreten Einzelfall ein Verdacht auf Leistungsmissbrauch besteht, dann kann eine Datenübermittlung an die Ausländerbehörde auf der Grundlage von § 69 Abs. 1 Nr. 1, 2. Alt. SGB X erwogen werden.

3.3.5.2.4
Ergebnis und Konsequenzen

Diese Rechtslage habe ich der behördlichen Datenschutzbeauftragten mitgeteilt.

Gleichzeitig habe ich den Hessischen Landkreistag über meine Rechtsauffassung informiert und Kontakt zum HMDIS im Hinblick auf dessen Zuständigkeit für Fragen des Ausländer- und Asylrechts sowie dem HSM als Fachaufsicht über die hessischen Optionskommunen gesucht und auch diesen Ministerien meine Rechtsauffassung mitgeteilt.

Der Hessische Landkreistag hat in Eigeninitiative alle hessischen Optionskommunen sowie Ausländerbehörden per Informationsschreiben und Kopie meiner Stellungnahme zur Beachtung meiner Rechtsposition aufgefordert.

Die Stellungnahmen der Ministerien lagen mir bis Redaktionsschluss dieses Tätigkeitsberichts noch nicht vor.

3.3.5.3
Zugriffsberechtigungen auf EDV-Programme des Jobcenters

Die dauerhafte Zugriffsberechtigung z. B. der Kreiskasse oder der Revision auf die in EDV-Programmen des Jobcenters gespeicherten Datensätze von Leistungsempfängerinnen und -empfängern ist rechtswidrig.

Bei einer hessischen Kreisverwaltung bzw. Optionskommune hatte es im Berichtszeitraum einen großen, auch medien- und öffentlichkeitswirksamen Betrugsfall innerhalb der SGB II-Stelle gegeben, bei dem es einer Mitarbeiterin gelungen war, Gelder in nicht unwesentlicher Höhe auf ihr eigenes Konto umzuleiten. Dies führte nach Aufdeckung dieses Vergehens u. a. zu einer gerichtlichen Verurteilung der mittlerweile ehemaligen Mitarbeiterin. Dieser Fall stieß innerhalb der betroffenen Kreisverwaltung eine Debatte hinsichtlich der aus dieser Erfahrung zu ziehenden organisatorischen Schlüsse an.

Der behördliche Datenschutzbeauftragte dieser Kreisverwaltung bzw. SGB II-Optionskommune wandte sich mit folgender Fragestellung an mich:

Die Mitarbeiter des dortigen externen Rechnungswesens (Kreiskasse) verfügten seit geraumer Zeit über eine Leseberechtigung (Lizenz) für das im Bereich des Sozial- und Arbeitswesens verwendete EDV-System. Deren Zugriffsberechtigung sei mit dem Hinweis begründet worden, dass erheblicher zusätzlicher Arbeitsaufwand vermieden werden solle, der u. a. durch

ständige Zuordnungsprobleme bei Geldrückläufen oder Geldeingängen der Leistungsempfänger und deren jeweiligen Sachbearbeitern entstehe.

Über das dortige Leserecht könne man, so stellte der behördliche Datenschutzbeauftragte fest, alle Sozialdaten der dort gespeicherten Personen sowie den jeweils zuständigen Sachbearbeiter bzw. die Sachbearbeiterin erfahren. Er war skeptisch hinsichtlich der Zulässigkeit von Genehmigungen der Behörde, Leserechte für Beschäftigte anderer Fachbereiche der Kreisverwaltung in Programme der Optionskommune einzuräumen.

In meiner Reaktion gegenüber dem behördlichen Datenschutzbeauftragten habe ich den Betrugsfall als Hintergrund für die Einräumung der Leserechte berücksichtigt. Trotzdem: Auch wenn die Führungsebenen innerhalb der Kreisverwaltung bzw. Optionskommune seit der Berichterstattung in den Medien sehr sensibel auf Sachverhalte reagierten, die im Zusammenhang mit Korruption und Untreue stehen könnten, und auch wenn der Themenkomplex „Compliance“ losgelöst von diesem konkreten Fall auch in der öffentlichen Verwaltung zunehmend an Bedeutung gewinnt, so ist die geschilderte Vorgehensweise unverhältnismäßig und aus sozialdatenschutzrechtlicher Sicht nicht akzeptabel.

Dass ausnahmslos alle Mitarbeiterinnen und Mitarbeiter des externen Rechnungswesens (Kreiskasse) einen dauerhaften Lesezugriff auf die EDV-gestützten Programme der Optionskommune im Bereich des Sozial- und Arbeitswesens haben, ist schon vor dem Hintergrund von § 35 Abs. 1 SGB I nicht hinnehmbar.

§ 35 Abs. 1 SGB I

Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 Zehntes Buch) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. (…)

Die vorliegende Fallkonstellation ist vergleichbar mit dem in meinem 38. Tätigkeitsbericht, Ziff. 4.8.2, geschilderten Fall „Prüfung von Beihilfevorgängen durch die Innenrevision“. In diesem Beitrag hatte ich darauf hingewiesen, dass die Innenrevision, die typischerweise nicht mit der Bearbeitung von Personalangelegenheiten betraut ist, nur ausnahmsweise Zugang zu Personalakten erhalten kann. Dies kann bspw. der Fall sein, wenn es anlassbezogen oder auch stichprobenartig um die Überprüfung der Aktenführung durch die Personalsachbearbeiter geht. Die Unzulässigkeit, die Innenrevision durchgängig in die Beihilfebearbeitung einzubeziehen, habe ich dabei klar herausgestellt.

Dem anfragenden behördlichen Datenschutzbeauftragten habe ich mitgeteilt, dass auch in dem von ihm geschilderten Fall das Sozialgeheimnis zu beachten ist: Die Mitarbeiterinnen und Mitarbeiter des externen Rechnungswesens dürfen nur anlassbezogen oder stichprobenartig auf die für ihre konkrete Prüfung erforderlichen Daten zugreifen.

Parallel hierzu habe ich Kontakt zur Arbeitsgemeinschaft der Kommunalen Jobcenter des Hessischen Landkreistages gesucht und dieser meine Rechtsposition mitgeteilt, da ich die Fallkonstellation auch in anderen Optionskommunen für denkbar hielt und halte. Der Hessische Landkreistag hat meiner Rechtsauffassung in einer Stellungnahme ausdrücklich zugestimmt und zusätzlich beschlossen, sich mit dem Thema nochmals vertieft zu befassen, um mögliche rechtswidrige dauerhafte Zugriffsberechtigungen endgültig abzustellen und auszuschließen.

3.3.5.4
Informations- und Datenaustausch zwischen Kindergarten und Schule

Der Austausch von objektiv sachlichen Informationen und Personenstandsdaten zwischen einem Kindergarten und einer Schule ist unter Beachtung der Vorgaben des Kinder- und Jugendhilferechts zulässig. Einer gesonderten Einwilligung der Eltern bedarf es in diesen Fällen nicht.

Immer wieder werde ich von Eltern als auch von Fachkräften von Kindergärten bzw. -tageseinrichtungen gefragt, ob Daten und Informationen über ein Kind ohne Weiteres durch die Erzieherinnen an eine Schule weitergegeben werden dürfen. Hintergrund ist hierfür auch die Tatsache, dass ohne die Mitwirkung und Beteiligung der Eltern die meisten Angebote der Kinder- und Jugendhilfe leerlaufen. Die Erziehungsberechtigten sind an den Entscheidungen in wesentlichen Angelegenheiten der Erziehung, Bildung und Betreuung zu beteiligen. Ich weise die Anfragenden und Ratsuchenden auf zwei Normen des Achten Buches Sozialgesetzbuch SGB VIII hin.

Gem. § 22a Abs. 2 Satz 1 Nr. 2 und Nr. 3 SGB VIII sollen die Träger der öffentlichen Jugendhilfe sicherstellen, dass die Fachkräfte in ihren Einrichtungen zusammenarbeiten mit anderen kinder- und familienbezogenen Institutionen und Initiativen im Gemeinwesen, insbesondere solchen der Familienbildung und -beratung (Nr. 2) und mit den Schulen, um den Kindern einen guten Übergang in die Schule zu sichern und um die Arbeit mit Schulkindern in Horten und altersgemischten Gruppen zu unterstützen (Nr. 3). Die Erziehungsberechtigten sind an den Entscheidungen in wesentlichen Angelegenheiten der Erziehung, Bildung und Betreuung zu beteiligen, § 22a Abs. 2 Satz 2 SGB VIII.

§ 22a Abs. 1 und 2 SGB VIII

(1) Die Träger der öffentlichen Jugendhilfe sollen die Qualität der Förderung in ihren Einrichtungen durch geeignete Maßnahmen sicherstellen und weiterentwickeln. Dazu gehören die Entwicklung und der Einsatz einer pädagogischen Konzeption als Grundlage für die Erfüllung des Förderungsauftrags sowie der Einsatz von Instrumenten und Verfahren zur Evaluation der Arbeit in den Einrichtungen.

(2) Die Träger der öffentlichen Jugendhilfe sollen sicherstellen, dass die Fachkräfte in ihren Einrichtungen zusammenarbeiten

1. *mit den Erziehungsberechtigten und Tagespflegepersonen zum Wohl der Kinder und zur Sicherung der Kontinuität des Erziehungsprozesses,*
2. *mit anderen kinder- und familienbezogenen Institutionen und Initiativen im Gemeinwesen, insbesondere solchen der Familienbildung und -beratung,*
3. *mit den Schulen, um den Kindern einen guten Übergang in die Schule zu sichern und um die Arbeit mit Schulkindern in Horten und altersgemischten Gruppen zu unterstützen. Die Erziehungsberechtigten sind an den Entscheidungen in wesentlichen Angelegenheiten der Erziehung, Bildung und Betreuung zu beteiligen.*

Vor diesem Hintergrund ist eine Datenübermittlung und -nutzung i. S. v. § 64 SGB VIII zulässig. Denn nach § 64 Abs. 1 SGB VIII dürfen Sozialdaten zu dem Zweck übermittelt oder genutzt werden, zu dem sie erhoben worden sind.

§ 64 Abs. 1 SGB VIII

Sozialdaten dürfen zu dem Zweck übermittelt oder genutzt werden, zu dem sie erhoben worden sind.

Sofern die Auskünfte von der zuständigen Erzieherin im Kindergarten an die Schulleitung der Schule, die das betroffene Kind im Anschluss an den Kindergarten besuchen soll, sich lediglich auf sachliche Informationen und Personenstandsangaben beziehen, bewegt sich diese Datenübermittlung im gesetzlich zulässigen Rahmen des § 22a Abs. 2 Satz 1 Nr. 3 SGB VIII. Denn es zählt auch zu den gemeinsamen Aufgaben von Kindertageseinrichtungen und Grundschulen, den Übergang der Kinder zu gestalten. Arbeit mit den Kindern bedeutet hier, Mädchen und Jungen auf die Schule einzustimmen und Fragen zu klären. Kinder des letzten Kindertagesstätten-Jahres werden z. B. in die Schule eingeladen und dürfen einmalig (einige Tage) am Unterricht teilnehmen. Diese Zusammenarbeit dient der Sicherung eines reibungslosen Übergangs vom Kindergarten in die Grundschule.

Der 12. Kinder- und Jugendbericht des Bundesministeriums für Familie, Senioren, Frauen und Jugend hebt die Notwendigkeit von kooperativen Arbeitsstrukturen in Form von kontinuierlichen Absprachen und Treffen in lokalen und regionalen Arbeitskreisen hervor. Auch bei einer neben der Schule

erfolgenden Betreuung eines Kindes in einem Hort oder einer altersgemischten Gruppe soll durch die Zusammenarbeit wiederum die Kontinuität des Entwicklungsprozesses gewährleistet werden (so Fischer in: Schellhorn/Fischer/Mann/Kern, SGB VIII, § 22a, Rdnr. 9).

Die in diesem Zusammenhang erforderlichen Datenübermittlungen sind durch die vorgenannte Vorschrift gedeckt. Einer ausdrücklichen vorherigen Einwilligung durch die Eltern bedarf es hier nicht.

Etwas anders gestaltet sich die Situation z. B. bei der Weitergabe von sog. Entwicklungsberichten des Kindes. In einem Entwicklungsbericht werden neben „allgemeinen Daten“ (Angaben zum Kind, zu den Erziehungsberechtigten und Geschwistern, zum Kindergarten) regelmäßig noch andere sensible Daten erfasst. Dazu zählen z. B. solche zum familiären Hintergrund (Versorgung, Hygiene usw.), zum Sozial- und Kontaktverhalten, zum Kommunikations-, Spiel- und Lernverhalten, zur Sprache, Motorik, Wahrnehmung, zum kognitiven und lebenspraktischen Bereich. Soweit hier ein personenbezogener Informationsaustausch zwischen Kindergarten und Schule stattfinden soll, ist dieser aus datenschutzrechtlicher Sicht mit den Eltern abzustimmen. § 22a Abs. 2 Satz 2 SGB VIII meint in diesem Kontext mit Beteiligung der Eltern dann eine hinreichende Einflussnahme der Eltern auf die Entscheidungen (so Fischer in: Schellhorn/Fischer/Mann/Kern, SGB VIII, § 22a Rdnr. 7 bis 9). Deshalb sollten diese z. B. einen solchen Bericht gemeinsam mit der Leitung der Kindertageseinrichtung unterschreiben. Diese Rechtslage teile ich den Anfragenden, sowohl Eltern als auch Fachkräften der Kindertageseinrichtungen, regelmäßig mit. Dabei betone ich auch die besondere Bedeutung der dem Wohl der Kinder dienenden Zusammenarbeit der Fachkräfte mit den Erziehungsberechtigten. Die Verpflichtung zur Zusammenarbeit trägt der Erkenntnis Rechnung, dass insbesondere für ein Kleinkind ein möglichst gleich bleibendes Erziehungsmilieu gesichert werden muss. Dies kann nur dadurch erreicht werden, dass zwischen den Hauptbezugspersonen ein reger gegenseitiger Informationsaustausch und ein gutes persönliches Klima herrschen.

3.3.5.5
Archivierung von Akten des Jugendamts

Akten des Jugendamts können zur Archivierung einem Stadt- oder dem Landesarchiv angeboten werden, ohne dass datenschutzrechtliche Vorschriften dem entgegen stehen. Dies gilt auch für regelmäßig besonders sensible Beistands-, Vormunds- und Amtspflegschaftsakten.

Das bei mir anfragende Jugendamt einer hessischen Stadt vernichtet entsprechend den Vorgaben aus einer städtischen Allgemeinen Geschäftsan-

weisung und wegen gesetzlicher Löschfristen turnusgemäß und datenschutzgerecht Akten. Vorher werden diese jedoch dem dortigen Stadtarchiv zur Archivierung angeboten. Es taucht dabei die Frage auf, wie mit Akten aus Beistands-, Vormunds- und Amtspflegschaftsfällen umzugehen ist, da es hier eine datenschutzrechtliche Sonderregelung im SGB VIII (Kinder- und Jugendhilfe) gibt.

Zu dieser Frage wurde auch vorher das Deutsche Institut für Jugendhilfe und Familienrecht e. V. (DIJuF) kontaktiert, das eine Stellungnahme zu dem Problem „Aktenabgabe an das zuständige Archiv“ verfasst und zur Verfügung gestellt hat. Das DIJuF kommt dabei jedoch zu dem falschen Schluss, Akten aus diesem Bereich dürften nicht an das zuständige Archiv abgegeben werden.

Im Kinder- und Jugendhilferecht gibt es für die Tätigkeit von Bediensteten des Jugendamts als Beistand, Amtspfleger, Amtsvormund und Gegenvormund eine datenschutzrechtliche Sonderregelung im § 68 SGB VIII:

§ 68 SGB VIII

(1) Der Beamte oder Angestellte, dem die Ausübung der Beistandschaft, Amtspflegschaft oder Amtsvormundschaft übertragen ist, darf Sozialdaten nur erheben und verwenden, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Die Nutzung dieser Sozialdaten zum Zweck der Aufsicht, Kontrolle oder Rechnungsprüfung durch die dafür zuständigen Stellen sowie die Übermittlung an diese ist im Hinblick auf den Einzelfall zulässig.

(2) Für die Löschung und Sperrung der Daten gilt § 84 Abs. 2, 3 und 6 des Zehnten Buches entsprechend.

(3) Wer unter Beistandschaft, Amtspflegschaft oder Amtsvormundschaft gestanden hat, hat nach Vollendung des 18. Lebensjahres ein Recht auf Kenntnis der zu seiner Person gespeicherten Informationen, soweit nicht berechtigte Interessen Dritter entgegenstehen. Vor Vollendung des 18. Lebensjahres können ihm die gespeicherten Informationen bekannt gegeben werden, soweit er die erforderliche Einsichts- und Urteilsfähigkeit besitzt und keine berechtigten Interessen Dritter entgegenstehen. Nach Beendigung einer Beistandschaft hat darüber hinaus der Elternteil, der die Beistandschaft beantragt hat, einen Anspruch auf Kenntnis der gespeicherten Daten, solange der junge Mensch minderjährig ist und der Elternteil antragsberechtigt ist.

(4) Personen oder Stellen, an die Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verwenden, zu dem sie ihnen nach Absatz 1 befugt weitergegeben worden sind.

(5) Für die Tätigkeit des Jugendamts als Gegenvormund gelten die Absätze 1 bis 4 entsprechend.

Diese Sonderregelung normiert für diesen Bereich der Kinder- und Jugendhilfe den Datenschutz abschließend, so dass weder die §§ 62 bis 67 SGB VIII noch § 35 SGB I und die §§ 67 bis 85a SGB X unmittelbar anwendbar sind. Dies entspricht der ausdrücklichen Herausnahme dieser Tätigkeiten des

Trägers der Jugendhilfe aus dem Anwendungsbereich der §§ 61 bis 67 SGB VIII in § 61 Abs. 2 SGB VIII.

§ 61 Abs. 2 SGB VIII

Für den Schutz von Sozialdaten bei ihrer Erhebung und Verwendung im Rahmen der Tätigkeit des Jugendamts als Amtspfleger, Amtsvormund, Beistand und Gegenvormund gilt nur § 68.

Gemäß § 68 Abs. 2 SGB VIII gilt für die Löschung und Sperrung der Daten aber § 84 Abs. 2, 3 und 6 SGB X entsprechend.

§ 84 Abs. 2, 3 und 6 SGB X

(2) Sozialdaten sind zu löschen, wenn ihre Speicherung unzulässig ist. Sie sind auch zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. *einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,*
2. *Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder*
3. *eine Löschung wegen der besonderen Art der Speicherung nicht oder nicht mit angemessenem Aufwand möglich ist.*

...

(6) § 71 Abs. 1 Satz 3 bleibt unberührt.

Eine Aktenaufbewahrung über das Ende der Beistandschaft, Amtsvormundschaft/-pflegschaft hinaus ist damit grundsätzlich nur zulässig, wenn sie zur Erfüllung der daraus folgenden Aufgaben erforderlich bleibt. Dies kann Probleme schaffen, weil die Aufbewahrung von Aktenunterlagen beim gesetzlichen Vertreter grundsätzlich eine andere Bedeutung als bei einer Behörde hat. Die Akte des Beistands, Amtspflegers/Amtsvormunds gibt nicht nur den Ablauf von verwaltungsmäßigen Vorgängen wieder. Sie ist auch ein Hinweis auf die Biografie des Betroffenen. Mit der Beendigung der Vertretungsmacht des Beistands, Amtspflegers/Amtsvormunds nach § 68 Abs. 3 SGB VIII haben die Betroffenen ein Recht auf Datenkenntnis (vgl. Wiesner § 68 Rdnr. 11 f.). Deshalb ist vor der Löschung zu prüfen, ob wegen schutzwürdiger Interessen von Betroffenen die Daten zunächst nur zu sperren sind (Proksch in Münder/Meysen/Trenczek, § 68 Rdnr. 11).

Gemäß § 84 Abs. 6 SGB X bleibt jedoch § 71 Abs. 1 Satz 3 SGB X unberührt.

§ 71 Abs. 1 SGB X

Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflichten […]. Erklärungspflichten als Drittschuldner, welche das Vollstreckungsrecht vorsieht, werden durch Bestimmungen dieses Gesetzbuches nicht berührt. Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Pflichten zur Sicherung und Nutzung von Archivgut nach den §§ 2 und 5 des Bundesarchivgesetzes oder entsprechenden gesetzlichen Vorschriften der Länder, die die Schutzfristen dieses Gesetzes nicht unterschreiten. Eine Übermittlung von Sozialdaten ist auch zulässig, soweit sie erforderlich ist, Meldebehörden nach § 4a Abs. 3 des Melderechtsrahmengesetzes über konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit von diesen auf Grund Melderechts übermittelter Daten zu unterrichten.

Mit § 71 Abs. 1 Satz 3 SGB X ist klargestellt, dass die Löschungsanordnung nach § 84 Abs. 2 SGB X nicht die Übermittlung an das Bundesarchiv oder ein Landesarchiv hindern soll (unzulässig gespeicherte Daten sind von der Verpflichtung, sie vor ihrer Löschung einem Archiv anzubieten, natürlich ausgenommen). Eine Übermittlung von Sozialdaten ist demnach zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Pflichten zur Sicherung und Nutzung von Archivgut nach den §§ 2 und 5 des Bundesarchivgesetzes oder entsprechender gesetzlicher Vorschriften der Länder, die die Schutzfristen dieses Gesetzes nicht unterschreiten.

In Hessen gilt als dem Bundesarchivgesetz entsprechende Vorschrift das Hessische Archivgesetz (HArchivG). Dieses erlaubt in § 4 HArchivG den Gemeinden, Landkreisen und kommunalen Verbänden, die Archivierung ihres Archivgutes im Rahmen ihrer Leistungsfähigkeit und nach den in diesem Gesetz vorgegebenen Grundsätzen durch Satzung zu regeln. Eine solche Satzung existiert bei der betroffenen Stadt – sie wurde mir zur Verfügung gestellt und begegnete keinen datenschutzrechtlichen Bedenken.

Im Ergebnis war und ist es also zulässig, Akten aus dem Bereich Vormund-, Pfleg- und Beistandschaft dem kommunalen Archiv anzubieten. Dies ergibt sich aus § 68 Abs. 2 SGB VIII i. V. m. § 84 Abs. 6 SGB X und § 71 Abs. 1 Satz 3 SGB X. Diese Rechtslage habe ich der anfragenden Stadt mitgeteilt.

3.3.6
Personalwesen

3.3.6.1
Löschung von Daten im SAP R/3 HR-System

Das Programm zur Löschung der urlaubs- und krankheitsbedingten Abwesenheiten wird in vielen Bereichen der Landesverwaltung nicht oder nicht zeitnah eingesetzt.

In meinem 40. Tätigkeitsbericht (Ziff. 3.10.3) hatte ich über den Sachstand zur Löschung von Krankheits- und Urlaubsdaten im SAP R/3 HR-System, die am 31. Dezember 2006 schon hätten gelöscht sein müssen, berichtet. Es handelte sich um 7.559 Datensätze.

In ihrer Stellungnahme zu diesem Bericht hatte die Landesregierung ausgeführt, dass zwischenzeitlich die Löschung des größten Teils dieser Daten erfolgt sei.

Eine erneute Überprüfung der Löschpraxis im SAP R/3 HR-System hat ergeben, dass auch am 1. Oktober 2012 noch immer 2.968 Datensätze aus diesem Zeitraum nicht gelöscht waren.

Es handelt sich um

25 Datensätze des Hessischen Rechnungshofs
54 Datensätze des Hessischen Statistischen Landesamts
42 Datensätze des Ministeriumspersonals des HMdIuS
23 Datensätze des Landesamtes für Verfassungsschutz
667 Datensätze im Bereich der Schulen
72 Datensätze im Bereich der Erwachsenenbildung
132 Datensätze im Bereich der Ämter für Lehrerfortbildung
6 Datensätze im Bereich des Justizvollzugs
35 Datensätze des Ministeriumspersonals des HMDF
30 Datensätze bei der Hessischen Bezügestelle
69 Datensätze bei der Hessischen Zentrale für Datenverarbeitung
536 Datensätze bei der Vorsorgekasse
146 Datensätze beim Hessischen Baumanagement
32 Datensätze des Ministeriumspersonals des HMWVL
491 Datensätze bei Hessen Mobil
260 Datensätze bei der Hessischen Verwaltung Bodenmanagement und Geoinformation
91 Datensätze des Ministeriumspersonals des HSM
70 Datensätze beim Hessischen Landesamt für Umwelt und Geologie

In dieser Auflistung sind nur die Buchungskreise enthalten, bei denen mehr als 10 Datensätze nicht gelöscht wurden. Bei allen betroffen Dienststellen können auch die schon längst zur Löschung anstehenden Daten des Jahres 2008 nicht gelöscht sein, weil das Löschprogramm immer alle Daten, die älter als drei Jahre sind, abfragt.

Ich stelle fest, dass es sich hierbei um einen erheblichen Verstoß gegen die Vorschriften des § 107f Abs. 2 HBG handelt.

§ 107f Abs. 2 HBG

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.

Von einer Beanstandung der weiteren Verarbeitung von Personaldaten gegenüber den oben angeführten verantwortlichen Dienststellen mit dem SAP R/3 HR-System habe ich bisher abgesehen, weil mein 40. Tätigkeitsbericht dazu geführt hat, dass ein großer Teil der zu löschenden Daten sofort gelöscht wurde, wie es auch der Stellungnahme der Landesregierung zu diesem Bericht zu entnehmen ist.

Eine weitere Überprüfung der „Löschpraxis“ im SAP R/3 HR-System hat ergeben, dass am 1. Oktober 2012 noch immer 15.320 Datensätze nicht gelöscht wurden, die bis zum 31. Dezember 2008 hätten gelöscht werden müssen.

Ich verzichte an dieser Stelle auf eine wiederholte Nennung der Buchungskreise und stelle nochmals ausdrücklich fest, dass die betroffenen Buchungskreise der Verpflichtung zur Löschung von Urlaubs- und Krankheitsdaten nach § 107f Abs. 2 HBG wider besseren Wissens nicht ausreichend nachkommen. Die Erfahrungen beim Einsatz des fehlerfrei funktionierenden Löschreports haben gezeigt, dass der Einsatz des Programms problemlos ist.

Bisher sind mir gegenüber keine Begründungen für die Nichtlöschung der Daten abgegeben worden. Ich werde zum 1. Mai 2013 feststellen, ob die Daten aus den Jahren 2006 bis 2009 gelöscht sind, und jede weitere Verarbeitung der Personaldaten mit dem SAP R/3 HR-System für die personal führenden Dienstellen, die nach dem HDSG verantwortlich sind und der Löschverpflichtung nicht nachkommen, gem. § 27 HDSG beanstanden.

§ 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.

In meinem 40. Tätigkeitsbericht hatte ich weiterhin ausgeführt, dass lt. Mitteilung des Produktmanagements LRM HR bis zum 31. Dezember 2011 das Fachkonzept zum Löschen ganzer Datensätze im SAP R/3 HR-System erstellt werden soll. Dieses Fachkonzept wurde im Februar 2012 durch das Produktmanagement abgenommen und die Programme zum Löschen ganzer Datensätze werden nach meiner Kenntnis am 13. Dezember 2012 produktiv gesetzt. Da auch in diesen Fällen die Fristen nach § 107 ff. HBG bereits überschritten sind, werde ich eine konkrete Überprüfung des Einsatzes dieser Programme zum 1. Mai 2013 vornehmen.

3.3.7
Kommunale Selbstverwaltungskörperschaften

3.3.7.1
Änderung der Hessischen Gemeindeordnung

Im Dezember 2011 hat der Hessische Landtag eine Änderung der Hessischen Gemeindeordnung verabschiedet, die aus datenschutzrechtlicher Sicht eine gravierende Änderung mit sich bringt. In den Sitzungen der Kommunalparlamente dürfen nun Bild- und Tonaufnahmen erstellt werden, wenn die Mehrheit der Gemeindevertreter dies beschlossen hat.

Am 10. Mai 2011 haben die Regierungsfraktionen von CDU und FDP einen Gesetzentwurf für ein Gesetz zur Änderung der Hessischen Gemeindeordnung und anderer Gesetze (LTDrucks. 18/4031) vorgelegt. Der Hessische Landtag hat mir Gelegenheit gegeben, in schriftlicher und mündlicher Anhörung zu diesem Gesetzentwurf Stellung zu nehmen.

Diese Gelegenheit zur Stellungnahme habe ich gerne wahrgenommen und einige wenige Anmerkungen zu dem Gesetzentwurf gemacht:

– § 7 des HGO-Entwurfs (ebenso wie § 6 des Änderungsentwurfs zur Landkreisordnung) sah vor, dass die öffentliche Bekanntmachung neben der bisherigen Bekanntmachung über Amtsblatt oder Aushang künftig auch über das Internet erfolgen kann. Diese Regelung habe ich begrüßt, da dies für die Kommunen Rechtssicherheit schafft. Ich hatte in der Vergangenheit immer wieder vertreten, dass dieser Weg der Veröffentlichung nur aufgrund einer klaren gesetzlichen Regelung möglich ist. Diese ist nun mit Verabschiedung dieser Norm geschaffen worden.

– Der Entwurf sah in § 58 Abs. 1 die Erleichterung der Nutzung von E-Mail vor. Danach sollten insbesondere Einladungen zu Sitzungen der Gemeindevertretung künftig per Mail verschickt werden können, ohne dass es der Unterzeichnung mit einer qualifizierten elektronischen Signatur bedürfte. Diesen Vorschlag habe ich zwar für tolerierbar gehalten, allerdings habe ich betont, dass gewisse datenschutzrechtliche Rahmenbedingungen eingehalten werden müssen, wie ich Sie bereits in meinem 36. Tätigkeitsbericht (Ziff. 6.1.5) dargestellt hatte (alleinige Zugriffsberechtigung des Empfängers, Benutzerkennung und Passwort, aktueller Virenschutz etc.). In der Begründung des Gesetzentwurfs ist auf diese Bedingungen Bezug genommen worden. Ich hätte es begrüßt, wenn sie Bestandteil des Gesetzes selbst geworden wären. Leider ist der Gesetzgeber dieser Anregung nicht gefolgt.

– § 111 sollte dahingehend geändert werden, dass Kassengeschäfte künftig auf einen Dritten übertragen werden können. Hier fehlte mir eine Regelung zur datenschutzrechtlichen Verantwortlichkeit. Der Entwurf ließ im Unklaren, ob diese Übertragung in Form einer Funktionsübertragung oder als Datenverarbeitung im Auftrag erfolgen soll. Schon aufgrund der Überlegung, dass auch Steuerdaten bei der Übertragung von Kassengeschäften auf einen Dritten betroffen sind, habe ich die Funktionsübertragung für rechtlich unzulässig gehalten. Eine Datenverarbeitung im Auftrag halte ich jedoch datenschutzrechtlich für zulässig, da hier die öffentliche Stelle verantwortlich bleibt und der Bürger seine Grundrechtsposition ihr gegenüber geltend machen kann. Der Gesetzgeber hat diesen Einwand aufgegriffen, indem er in § 111 Abs. 1 Satz 2 HGO ausdrücklich auf die Geltung des § 4 (Auftragsdatenverarbeitung) HDSG hingewiesen hat. Damit ist klargestellt, dass es sich bei dieser Form der Aufgabenerledigung um Auftragsdatenverarbeitung i. S. d. des HDSG handelt.

In die weitere parlamentarische Beratung des Gesetzentwurfes brachten die Regierungsfraktionen überraschend einen Änderungsantrag zu § 52 HGO – neuer Abs. 3 – mit folgendem Wortlaut ein:

§ 52 HGO

Die Hauptsatzung kann bestimmen, dass in öffentlichen Sitzungen Film- und Tonaufnahmen durch die Medien mit dem Ziel der Veröffentlichung zulässig sind.

In der Begründung wird zu § 52 Abs. 3 ausgeführt:

Die durch das Internet in der Praxis immer bedeutsamere Frage der sog. Medienöffentlichkeit bei den Sitzungen der Gemeindevertretungen soll ebenso wie jüngst in Mecklenburg-Vorpommern gesetzlich geregelt werden. Die bisherige Rechtslage – Zulassung des Internet-Streams mit einfacher Mehrheit, jedoch Veto-Recht für die Minderheitsangehörigen bei eigenen Wortmeldungen – erscheint zunehmend unattraktiv und unbefriedigend.

Eine generelle – vom Willen der Gemeindevertreter unabhängige – gesetzliche Erlaubnis zum „Streamen", wie im Gesetzentwurf der Fraktion DIE LINKE v. 8. November 2010 vorgesehen (LT-Drucks. 18/3116), ginge jedoch zu weit und kommt daher nicht in Betracht. Vielmehr soll es den Mandatsträgern vor Ort obliegen, die Hauptsatzung der Gemeinde entsprechend anzupassen, wenn sie die Internetübertragung wollen.

Dieser Passus, der erhebliche datenschutzrechtliche Bedeutung hat, ist mir erst im Verlauf einer Innenausschusssitzung des hessischen Landtags bekannt geworden. Die Abgeordneten hatten den Text einen Tag zuvor erhalten.

Ich habe mir daraufhin mit Rücksicht auf meine Beratungsfunktion im Zusammenhang mit der Garantie der informationellen Selbstbestimmung erlaubt, zur Neufassung von § 52 Abs. 3 HGO auf Bedenken gegen das Procedere hinzuweisen.

In der Sache habe ich angemerkt, dass die Frage, ob öffentliche Sitzungen der kommunalen Vertretungsorgane der Saal- oder auch der Medienöffentlichkeit unterworfen werden können, im Schrifttum und in der Rechtsprechung umstritten ist. Auf dem Spiel stehen die Medienfreiheit und deren „demokratietheoretisch relevante Kontrollfunktion", auf der anderen Seite die Funktionsinteressen der kommunalen Vertretungskörperschaften. Im Kern geht es um die Verwendung von Informationen, die einerseits die Medien verbreiten wollen und die andererseits Abgeordnete ungestört austauschen wollen. Auf den ersten Blick liegt es nahe, die kommunalen Abgeordneten mit den staatlichen Abgeordneten gleichzustellen und sie ebenfalls der Medienöffentlichkeit zu unterwerfen. Im Unterschied zu diesen üben die kommunalen Abgeordneten aber auch Verwaltungstätigkeiten aus und müssen sich mit Detailfragen des kommunalen Wirkungskreises beschäftigen. Für die demokratische Kontrollfunktion reicht es daher aus meiner Sicht aus, eine lokale Öffentlichkeit unter Einbeziehung der Lokalpresse herzustellen. Eine weltweite zeitgleiche Öffentlichkeit für kommunale Abstimmungen kann die gleiche Wirkung erzielen wie eine umfassende Video-

überwachung der Bürgerinnen und Bürger, d. h. die Dauerbeobachtung kann Verhalten steuernd wirken und die freie informationelle Selbstbestimmung beeinträchtigen. Dies führt nicht zwingend dazu, dass die Güterabwägung zu Lasten der Medienöffentlichkeit gehen muss, hätte aber vor einer gesetzgeberischen Entscheidung für die eine oder andere Lösung mit berücksichtigt werden sollen.

Meines Erachtens ist es dem parlamentarischen Gesetzgeber unbenommen, sich für die eine oder andere Lösung zu entscheiden. Denn wesentliche Entscheidungen hat der Gesetzgeber zu treffen und zu verantworten. Die viel berufene Wesentlichkeitstheorie besagt aber auch, dass über wesentliche Entscheidungen auch wesentliche Debatten geführt werden müssen. Zumindest hätte mir für eine derartige Entscheidung Gelegenheit zur Stellungnahme gegeben werden müssen. Unter diesen Umständen habe ich darauf hingewiesen, dass ich die Novellierung von § 52 Abs. 3 HGO für wenig abgewogen halte und angeregt, das Abwägungsdefizit bei passender Gelegenheit auszuräumen.

Die Regierungsfraktionen von CDU und FDP haben daraufhin gegenüber dem Vorsitzenden des Hessischen Innenausschusses ausgeführt, dass Ziel der Gesetzesregelung sei, eine größere Medienöffentlichkeit zu erreichen. Der Gesetzentwurf sehe vor, dass es den Mandatsträgern vor Ort obliegen solle, die Hauptssatzung der Gemeinde entsprechend anzupassen, wenn sie die Internetübertragung wollen. Durch die für diese Entscheidung erforderliche qualifizierte Mehrheit gem. § 6 Abs. 2 Satz 1 HGO solle ein ausreichender Minderheitenschutz gewährleistet sein.

Das Parlament hat letztlich in Ausübung seiner Entscheidungsbefugnis den oben zitierten Änderungsantrag unverändert beschlossen.

3.3.7.2
Datenschutzverstoß durch den Magistrat der Stadt Bad Homburg

Eine 14 Jahre zurückliegende kurze kommunalpolitische Tätigkeit macht einen Bürger noch nicht zu einer Person der Zeitgeschichte.

Ein Bürger der Stadt Bad Homburg hatte gegen den Oberbürgermeister seiner Stadt eine Dienstaufsichtsbeschwerde beim Regierungspräsidium Darmstadt erhoben. Beschwerdegrund war das Verhalten des Oberbürgermeisters bei der Stellenbesetzung der Fachbereichsleitung „Zentrale Verwaltung“ in seiner Stadt.

In verschiedenen Presseartikeln war in der Folge zu lesen, dass das Regierungspräsidium Darmstadt diese Dienstaufsichtbeschwerde zurückgewie-

sen hat. In diesen Presseartikeln war auch zu lesen, wer die Dienstaufsichtsbeschwerde beim Regierungspräsidium eingelegt hatte. Da der Bürger selbst mit dieser Beschwerde nicht an die Öffentlichkeit getreten war, sah er in der Nennung seines Namens eine Verletzung seiner Persönlichkeitsrechte und wandte sich an meine Dienststelle mit der Bitte, den Sachverhalt zu überprüfen.

Ich habe daraufhin die Stadt Bad Homburg um Stellungnahme zu dem vorgetragenen Sachverhalt gebeten. Die Erwiderung der Stadt ergab Folgendes: Nachdem das Regierungspräsidium Darmstadt die Dienstaufsichtsbeschwerde zurückgewiesen hatte, hat die Pressestelle des Magistrats der Stadt Bad Homburg in einer Pressemitteilung dieses Ergebnis kommuniziert.

In der Pressemitteilung stand auch der volle Name des Bürgers, der die Dienstaufsichtsbeschwerde eingelegt hatte. Deshalb konnte in verschiedenen Zeitungen der Name des Beschwerdeführers im Zusammenhang mit der Dienstaufsichtsbeschwerde gegen den Oberbürgermeister gelesen werden. Auf meine Frage, warum man sich berechtigt sah, eine namentliche Benennung des Beschwerdeführers vorzunehmen, wurde mir mitgeteilt, dass den Ausschlag dafür die Tätigkeit des Beschwerdeführers als Stadtverordneter gegeben habe. Der Beschwerdeführer sei, auch wenn er das Amt heute nicht mehr ausübe, auf Grund seiner Bereitschaft, als Mitglied der Stadtverordnetenversammlung an Entscheidungen über die Angelegenheiten der Stadt mitzuwirken, spätestens durch die Wahl und die erfolgte Annahme des Mandats in Bad Homburg eine Person des öffentlichen Lebens. Die Nennung seines Namens stehe dem berechtigten Schutz personenbezogener Daten deshalb nicht entgegen, zumal diese Nennung in Zusammenhang mit einem Vorgang erfolgt sei, dessen öffentliche Diskussion in wesentlichen Teilen der Politik zuzuordnen sei, also dem Bereich, in dem auch der Beschwerdeführer gewirkt habe.

Dieser Rechtsauffassung konnte ich mich nicht anschließen, worüber ich den Magistrat der Stadt Bad Homburg in Kenntnis gesetzt habe.

Der Beschwerdeführer ist seit 14 Jahren kein Stadtverordneter von Bad Homburg mehr und er war es auch nur für relativ kurze Zeit. Auch seine Mitgliedschaft in einer politischen Partei liegt schon über ein Jahrzehnt zurück, sodass keineswegs davon gesprochen werden kann, es handele sich bei ihm um eine Person des öffentlichen Lebens der Stadt Bad Homburg. Zum Zeitpunkt der Stadtverordnetentätigkeit hätte man dies anders beurteilen können, heute jedoch ist der Petent ein Bürger Bad Homburgs wie jeder andere auch. Er muss insoweit darauf vertrauen können, dass seine Persönlichkeitsrechte von der Verwaltung gewahrt werden. Mit der Namensnennung in der Pressemitteilung hat der Magistrat der Stadt Bad Homburg in

unzulässiger Weise in die Persönlichkeitsrechte des Beschwerdeführers eingegriffen, da die Namensnennung ohne Rechtsgrundlage erfolgte. Der Ausgang des dienstaufsichtsbehördlichen Verfahrens hätte ohne Weiteres ohne Namensnennung der Person erfolgen können und müssen, die die Beschwerde angestrengt hatte. Das Informationsinteresse der Öffentlichkeit wäre dadurch durchaus befriedigt worden.

3.3.7.3
Stadtverordnete fragen den Magistrat nach der Parteimitgliedschaft städtischen Führungspersonals

Die Speicherung der Parteimitgliedschaft führender Mitarbeiter in den Akten der Verwaltung ist unzulässig. Deshalb können der Stadtverordnetenversammlung darüber auch keine Auskünfte erteilt werden.

Die Stadtverordneten einer Kommune hatten in einem Berichtsantrag den Magistrat um Auskunft darüber gebeten, welche Führungspositionen mit Mitgliedern welcher Parteien besetzt seien. Der Magistrat dieser Stadt wandte sich daraufhin an meine Dienststelle, um zu erfragen, ob diese Auskünfte überhaupt erteilt werden dürfen.

Ich habe dem Magistrat daraufhin mitgeteilt, dass der Magistrat dieses Datum zulässigerweise von seinen Mitarbeitern gar nicht erfragen darf. Bei der Parteizugehörigkeit handelt es sich um ein Datum gem. § 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.*

Diese Daten dürfen nach Maßgabe der §§ 33 bis 35 HDSG verarbeitet werden oder wenn eine Rechtsvorschrift dies ausdrücklich zulässt. Gem. § 34 Abs. 1 HDSG darf der Arbeitgeber Daten seiner Beschäftigten nur verarbeiten, soweit 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 dies vorsieht. Eine Rechtsvorschrift, die diese Datenverarbeitung zuließe, gibt es nicht. Die Erhebung des Datums Parteizu-

gehörigkeit ist auch nicht zur Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich, sodass eine Verarbeitung dieses Datums durch die Gemeinde rechtlich unzulässig wäre und diese Information sich auch nicht in den Akten/Personalakten der Verwaltung befinden darf. Erkenntnisse aus dem persönlichen Bereich dürfen hier nicht herangezogen werden.

Eine Mitteilung über Parteizugehörigkeiten von Führungskräften an die Stadtverordnetenversammlung ist deshalb schon wegen der fehlenden Zulässigkeit der Speicherung dieser Information rechtlich nicht zulässig.

3.3.7.4
Falsche Angaben gegenüber dem Betroffenen und dem Hessischen Datenschutzbeauftragten widersprechen dem Transparenzgrundsatz

Auch wenn die eigentliche Datenübermittlung aus der Einwohnermeldedatei rechtmäßig und datenschutzrechtlich von mir nicht zu beanstanden war, führten Falschauskünfte zu unnötigen und aufwändigen Ermittlungen.

Die geplante Erweiterung des Erdgasnetzes in Bromskirchen veranlasste den dortigen Energieversorger die Bürger anzuschreiben, um das Interesse an einer erweiterten Erdgasversorgung einschätzen zu können. Ein Bürger bat mich um datenschutzrechtliche Prüfung, ob die Gemeinde hier den Datenschutz verletzt haben könnte, da er der Übermittlung seiner persönlichen Daten widersprochen habe.

Auf Nachfrage teilte mir der Energieversorger mit, dass er Adressdaten bei der Deutschen Post gemietet hätte, eigene Kunden informiert habe und auch das örtliche Telefonbuch von Bromskirchen genutzt habe. Mit dieser Auskunft war der Betroffene nicht einverstanden, da der Energieversorger bei der Adressierung seinen zweiten Vornamen benutzt hatte, der nur dem Einwohnermeldeamt bekannt sei. In der Stellungnahme der Gemeinde Bromskirchen wurde ausdrücklich festgestellt, dass an den Energieversorger keine Einwohnermeldedaten übermittelt wurden. Auch nach einer Konfrontation mit dem Ergebnis einer Auswertung des Protokolls zu Abfragen in der Einwohnermeldedatei, die nachwies, dass im fraglichen Zeitraum der Einwohnermeldedatensatz des Betroffenen abgefragt wurde, blieb die Gemeinde Bromskirchen bei ihrer Aussage, dass keine Einwohnermeldedaten übermittelt wurden. Für die eingeholte Hausauskunft wurden andere verwaltungsinterne Gründe genannt.

Meine datenschutzrechtlichen Möglichkeiten zur Aufklärung des Sachverhalts waren damit zunächst erschöpft, dies habe ich dem Betroffenen entsprechend mitgeteilt. Vier Monate später legte mir der Betroffene eine er-

neute Auskunft des Energieversorgers zur Herkunft der Adressdaten für das Anschreiben an potentielle Erdgasanschlussnehmer vor. Danach erhielt der Energieversorger vom Einwohnermeldeamt der Gemeinde Bromskirchen eine sogenannte Gruppenauskunft aller Einwohner einer Straße. Nach § 34 Abs. 3 HMG ist eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) zulässig, wenn sie im öffentlichen Interesse liegt.

Im Hinblick auf den Klimawandel gehört der Einsatz des umweltfreundlicheren Energieträgers Erdgas zur allgemeinen Daseinsvorsorge und liegt durchaus im öffentlichen Interesse. Daher ist die erteilte Gruppenauskunft an den Energieversorger datenschutzrechtlich nicht zu beanstanden. Bei der Erteilung einer Gruppenauskunft an einen Dritten sind hierbei ausschließlich Auskunftssperren nach § 34 Abs. 5 HMG zu beachten (Gefährdung für Leben, Gesundheit, persönliche Freiheit u. Ä.). Die von dem Betroffenen angeführte Auskunftssperre nach § 34a HMG verbietet ausschließlich eine einfache Melderegisterauskunft in einem automatisierten Verfahren über das Internet und spielt bei Gruppenauskünften keine Rolle.

Umso unverständlicher ist mir das Auskunftsverhalten der Gemeinde Bromskirchen und des Energieversorgers. Dieses widerspricht dem datenschutzrechtlichen Transparenzgrundsatz. Jeder Betroffene hat gemäß § 18 Abs. 3 HDSG einen Anspruch auf Auskunft über die Herkunft seiner Daten. Werden hier falsche Angaben gemacht, wird dieses Recht ad absurdum geführt. Das Auskunftsrecht des Hessischen Datenschutzbeauftragten nach § 29 HDSG wurde hierbei ebenfalls nicht beachtet.

Gerade in diesem Fall hätte die Erteilung einer korrekten Auskunft letztlich dazu gedient, die Gemeinde von unberechtigten Vorwürfen zu entlasten.

Im Hinblick darauf, dass die Datenübermittlung an den Energieversorger rechtmäßig war, habe ich darauf verzichtet, die falschen Auskünfte der Gemeinde Bromskirchen und des Energieversorgers förmlich zu beanstanden. Der Betroffene wurde entsprechend informiert.

3.3.7.5
Personenbezogene Information über das Ergebnis eines gerichtlichen Musterverfahrens an die übrigen Widerspruchsführer

Vor einer Übermittlung personenbezogener Daten an Dritte ist grundsätzlich zu prüfen, ob die Voraussetzungen hierfür vorliegen. Die Tatsache, dass der Betroffene in einer Angelegenheit schon einmal als Sprecher in der Öffentlichkeit aufgetreten ist, rechtfertigt nicht automatisch eine solche Datenübermittlung.

In einer hessischen Kommune gab es Auseinandersetzungen mit Bürgern über die Rechtmäßigkeit der Heranziehung zu Straßenbeiträgen. Der Antrag eines dieser Bürger auf Aussetzung der Vollziehung des Heranziehungsbescheides gemäß § 80 Abs. 5 VwGO wurde durch Beschluss des Verwaltungsgerichts Kassel abgelehnt. Die Kommune nutzte den Beschluss unter Nennung des Namens dieses Bürgers, um alle Beschwerdeführer über den Ausgang des Verfahrens zu informieren und zur Rücknahme des Widerspruchs aufzufordern.

Dieses Schreiben übersandte mir der Betroffene zur datenschutzrechtlichen Prüfung. Auf meine Aufforderung zur Stellungnahme begründete die Kommune in ihrer Antwort die Weitergabe personenbezogener Daten in dem Informationsschreiben an die übrigen Widerspruchsführer damit, dass der Betroffene bereits seit Jahren im Zusammenhang mit den Auseinandersetzungen um die Baumaßnahme und die Straßenbeiträge als Sprecher der Anliegergemeinschaft aufgetreten sei. Gegen die Heranziehungsbescheide zu Straßenbeiträgen für diese Baumaßnahme wurden 18 Widersprüche eingelegt, aber nur der Betroffene habe im August 2011 beim zuständigen Verwaltungsgericht um vorläufigen Rechtsschutz gem. § 80 Abs. 5 VwGO nachgesucht. Bis zum Abschluss dieses Eilverfahrens wurden alle Widersprüche der Anlieger in der Hauptsache nicht weiter bearbeitet. Die Kommune ging davon aus, dass allen Widerspruchsführern bekannt war, dass der Betroffene ein Musterverfahren vor dem Verwaltungsgericht führte. Insoweit könne sie nicht erkennen, dass mit der Nennung des Namens des Beschwerdeführers eine Verletzung datenschutzrechtlicher Vorschriften vorliegen könne.

Diese Rechtsauffassung der Kommune konnte ich nicht teilen. Mit der Namensnennung des Beschwerdeführers wurde gegen § 7 bzw. § 16 HDSG verstoßen. Die Übermittlung dieser Information an Dritte ist eine Verarbeitung personenbezogener Daten, die nach § 7 HDSG nur zulässig ist, wenn eine Rechtsvorschrift sie vorsieht oder der Betroffene ohne jeden Zweifel eingewilligt hat. § 16 HDSG lässt eine Übermittlung personenbezogener Daten an Personen außerhalb des öffentlichen Bereichs nur zu, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten hat und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können. Diese Voraussetzungen für eine Datenübermittlung wurden hier nicht erfüllt. Aus der Tatsache, dass der Betroffene als Sprecher der Anliegergemeinschaft aufgetreten ist, lässt sich keine Einwilligung in eine solche Datenübermittlung ableiten. Es lag auch kein Fall des § 17 HVwVfG vor. Eine Information der Widerspruchsführer wäre auch ohne Namensnennung möglich gewesen.

Ich habe die Kommune aufgefordert, zukünftig vor der Übermittlung personenbezogener Daten an Dritte genau zu prüfen, ob eine solche Übermittlung zur rechtmäßigen Erfüllung von Aufgaben erforderlich ist, und sich in Zweifelsfällen an mich zu wenden. Den Beschwerdeführer habe ich entsprechend informiert.

3.3.7.6
Bauschildinformationen im Internet

Die Bauschildinformationen dienen der Gefahrenabwehr an der Baustelle. Eine Einstellung dieser Daten in das Internet ist von der Rechtsgrundlage der hessischen Bauordnung nicht gedeckt.

Nach der Hessischen Bauordnung (HBO) müssen für Bauvorhaben, die nicht genehmigungsfrei sind, an der Baustelle sog. Bauschilder aufgestellt werden, die Informationen über das geplante Bauvorhaben geben. Angegeben werden müssen auch die Namen und Anschriften der am Bau Beteiligten wie die Bauherrschaft (§ 48 HBO), der Entwurfsverfasser (§ 49 HBO), das beauftragte Bauunternehmen (§ 50 HBO) und die Bauleitung (§ 51 HBO).

§ 10 Abs. 2 HBO

Für die Dauer der Ausführung von Vorhaben, die nicht nach § 55 oder aufgrund des § 80 Abs. 4 Satz 1 Nr. 1 baugenehmigungsfrei sind, ist an der Baustelle ein Schild dauerhaft anzubringen, das mindestens die Nutzungsart des Gebäudes, die Zahl seiner Geschosse und die Namen und Anschriften der am Bau Beteiligten (§§ 48 bis 51) enthalten muss. Das Schild muss vom öffentlichen Verkehrsraum sichtbar sein.

Eine hessische Kommune war unter Berufung auf das Umweltinformationsgesetz (HUIG) dazu übergangen, die Bauschildinformationen auch ins Internet zu stellen. Baustellenlärm und die auf Baustellen entstehende Staubentwicklung gehörten laut HUIG zu den Umweltinformationen, auf die ein Anspruch auf freien Zugang bestünde. Um diesen Zugang zu eröffnen, sehe das HUIG auch die Nutzung elektronischer Datenbanken vor.

Da die Rechtmäßigkeit dieser Form der Veröffentlichung durch den behördlichen Datenschutzbeauftragten infrage gestellt worden war, hat die Stadt das hessische Wirtschaftsministerium um Stellungnahme zur Zulässigkeit der Internetveröffentlichung gebeten. Daraufhin hat das Ministerium erfragt, ob aus meiner Sicht die Regelung der Hessischen Bauordnung als Rechtsgrundlage für eine Veröffentlichung der Informationen im Internet geeignet sei.

In meiner Antwort an das Wirtschaftsministerium habe ich dargelegt, dass ich die Veröffentlichung der „Bauschildangaben“ im Internet nicht von der Rechtsgrundlage des § 10 Abs. 2 HBO umfasst sehe.

§ 10 Abs. 2 HBO regelt, dass das Schild auf der Baustelle aufzustellen ist und vom öffentlichen Verkehrsraum sichtbar sein muss.

Es hat die Funktion, eine schnelle Inanspruchnahme der für den Bau Verantwortlichen zur Abwehr oder Beseitigung von Gefahren sicherzustellen. Sollte von der Baustelle eine Gefahr ausgehen, sollen die mit der Bauüberwachung beauftragten Personen sich ohne besondere Probleme über den Inhalt des Bauschildes informieren können, auch wenn hierzu ein Betreten des Grundstücks erforderlich ist. Dritte, die zum Betreten des Grundstücks nicht befugt sind, können deshalb nicht ohne Weiteres den Inhalt des Bauschildes lesen.

Von einer Veröffentlichung im Internet ist in § 10 Abs. 2 HBO nicht die Rede. Betroffene müssen und können nicht damit rechnen, dass ihre Daten im Internet veröffentlicht werden. Auch in anderen Bereichen, in denen eine Bekanntmachung aufgrund gesetzlicher Vorgaben erfolgen muss, habe ich immer vertreten, dass dies keine Internetveröffentlichung mit umfasst.

Soweit die Stadt vorgetragen hat, dass hier das HUIG zur Anwendung gelangt und die Veröffentlichung deshalb zulässig oder sogar geboten sei, habe ich dem widersprochen. Zur Funktion des Bauschildes habe ich bereits oben Ausführungen gemacht. Von einer Baustelle können in der Tat Emissionen ausgehen, dann könnten hierzu auch Informationen nach dem HUIG gegeben werden. Aber die generelle Veröffentlichung eines Bauschildes im Internet unter Berufung auf das HUIG geht fehl, weil hier völlig verschiedene Funktionen angesprochen werden.

4. Aufsichtsbehörde nach § 38 BDSG

4.1
Der Hessische Datenschutzbeauftragte als Bußgeldbehörde

4.1.1
Überblick der Bußgeldverfahren im Jahr 2012

Im laufenden Jahr waren 32 Bußgeldverfahren abschließend zu bearbeiten. Darunter waren keine, die über den Einzelfall hinaus Bedeutung hatten.

Das Berichtsjahr war das erste vollständige Jahr, in dem ich auch die Zuständigkeit zur Verfolgung von Ordnungswidrigkeiten bei Verstößen gegen das BDSG hatte.

§ 24 Abs. 4 HDSG

(4) Der Hessische Datenschutzbeauftragte ist zuständige Behörde für die

1. ...

2. Verfolgung und Ahndung von Ordnungswidrigkeiten

a. nach § 43 des Bundesdatenschutzgesetzes,

b. nach § 16 Abs. 2 Nr. 2 bis 5 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 31. Mai 2010 (BGBl. I S. 692)

Die in meinem Haus abgewickelten Verfahren in Bußgeldsachen lassen sich in drei Gruppen einsortieren.

Zunächst gibt es die von mir als Aufsichtsbehörde angestoßenen Verfahren, insbesondere zu formalen Verstößen gegen Regelungen des BDSG. Diese erfüllen Tatbestände aus § 43 Abs. 1 BDSG.

§ 43 Abs. 1 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 Abs. 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Abs. 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Abs. 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der 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 Abs. 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 Abs. 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Abs. 1a, entgegen § 34 Abs. 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Abs. 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Abs. 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Abs. 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.

Weiterhin gibt es Eingaben von Bürgern, die vermeintliche Datenschutzverstöße zum Inhalt haben und ausdrücklich als Ordnungswidrigkeiten-Anzeige bezeichnet sind. Das ist häufig der Fall, wenn die entsprechenden Anzeigen durch Rechtsanwälte erfolgen. Diese Anzeigen hätten in vielen Fällen, wenn sie als Eingabe an die Aufsichtsbehörde gerichtet worden wären, nicht zu einem Bußgeldverfahren geführt, da keine oder nur marginale Verstöße festzustellen waren. Deswegen ist in dieser Kategorie die Anzahl der eingestellten Verfahren hoch.

Zur dritten Gruppe gehören Verfahren, die von Staatsanwaltschaften abgegeben werden. Häufig handelt es sich dabei um Fälle, in denen eine Tat keinen Straftatbestand erfüllt, die Verwirklichung eines Bußgeldtatbestandes jedoch nicht ausgeschlossen ist. Nicht immer hat die Staatsanwaltschaft dabei Überlegungen angestellt, ob ein Bußgeldtatbestand wirklich in Betracht kommt, sondern das Strafverfahren eingestellt, weil die Voraussetzungen des § 44 BDSG – Tat gegen Entgelt oder in Schädigungsabsicht – nach ihrer Einschätzung nicht vorlagen.

Meist liegt diesen Verfahren der Vorwurf zugrunde, dass unberechtigt Daten verarbeitet wurden.

§ 43 Abs. 2 BDSG

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 Abs. 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,*

5b. *entgegen § 28 Abs. 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,*

6. *entgegen § 30 Abs. 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.*

Der Rahmen der zu verhängenden Bußgelder ist gem. § 43 Abs. 3 BDSG zwar hoch, in der Mehrzahl der Fälle wird unter Berücksichtigung der Schwere des Verstoßes sowie auch der wirtschaftlichen Situation des Betroffenen dieser Rahmen bei weitem nicht ausgeschöpft.

§ 43 Abs. 3 BDSG

Die Ordnungswidrigkeit kann im Fall des Abs. 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Abs. 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.

Aus dem ersten Komplex wurden im Laufe des Jahres elf Fälle abgeschlossen, davon wurden sechs mit einem Bußgeld rechtskräftig beendet und fünf eingestellt. Einem Einspruch konnte nicht abgeholfen werden, sodass dieses Verfahren an die Staatsanwaltschaft abgegeben wurde zur Vorbereitung der gerichtlichen Entscheidung.

Von den sechs Verfahren der zweiten Gruppe wurden fünf eingestellt.

Von den 15 Verfahren, die von Staatsanwaltschaften abgegeben worden sind, führte nur eins zu einem rechtskräftigen Bußgeldbescheid. Vier Fälle wurden an die jeweils örtlich zuständige Bußgeldbehörde in einem anderen Bundesland abgegeben. Ein Verfahren wurde an das zuständige Ministerium (vgl. Ziff. 4.1.2.1) weitergereicht.

Insgesamt wurden im laufenden Jahr 3.900 EUR vereinnahmt.

Neben der Möglichkeit, einen Verstoß gegen Vorschriften des BDSG als Ordnungswidrigkeit zu verfolgen, stehen mir weitere Sanktionsmöglichkeiten zur Verfügung.

Die formalen Verpflichtungen der Daten verarbeitenden Stellen, insbesondere die Auskunftserteilung an den Datenschutzbeauftragten als Aufsichtsbehörde können auch mit einem Zwangsgeld durchgesetzt werden. Ein solches musste bis jetzt nicht festgesetzt werden, da schon die Androhung der Festsetzung dazu führte, dass die betroffenen Daten verarbeitenden Stellen ihrer Auskunftsverpflichtung nachgekommen sind.

In der Sache kann dieses Vorgehen im Einzelfall sinnvoller sein als ein Bußgeldverfahren. Denn selbst wenn das Bußgeldverfahren rechtskräftig abgeschlossen ist, ist nicht immer sichergestellt, dass dann auch die ausstehende Antwort im notwendigen Umfang erfolgt; so dass ggf. eine erneutes Vorgehen gegen diese Daten verarbeitende Stelle notwendig werden kann.

4.1.2
Datenschutzverstöße aus anderen Bereichen

Für die Verfolgung von Datenschutzverstößen bei der Anwendung anderer Gesetze ist der Hessische Datenschutzbeauftragte nicht zuständig. Die Übertragung der Zuständigkeit auch für solche Datenschutz-Ordnungswidrigkeiten sowie die Aufnahme eines weiteren Ordnungswidrigkeitentatbestandes zur Schließung einer Lücke sollte bei einer Novellierung erwogen werden.

4.1.2.1
Verstöße gegen das HDSG

Solche Verfahren spielen in der Praxis kaum eine Rolle. Dies liegt nicht zuletzt daran, dass in Hessen – anders als teilweise in anderen Landesdatenschutzgesetzen – lediglich die zweckwidrige Verwendung von Daten durch Private, die die entsprechenden Daten von einer öffentlichen Stelle für einen konkreten Zweck übermittelt bekommen haben, nach § 41 HDSG bußgeldbewehrt ist.

§ 41 HDSG

(1) Ordnungswidrig handelt, wer entgegen § 16 Abs. 2 oder § 33 Abs. 3 Daten nicht für den Zweck verwendet, zu dessen Erfüllung sie ihm übermittelt wurden.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

Da die Bußgeldvorschrift des § 41 HDSG in der Aufzählung des § 24 Abs. 4 HDSG nicht enthalten ist, richtet sich die sachliche Zuständigkeit zur Verfolgung solcher Ordnungswidrigkeiten nach den gesetzlichen Regelungen im OWiG. Gemäß § 36 Abs. 1 Nr. 2a OWiG ist Ordnungswidrigkeitenbehörde die für solche Verfahren fachlich zuständige oberste Landesbehörde. Da jeweils die einzelnen Ministerien für ihren Bereich die Ausführung des Datenschutzgesetzes sicherzustellen haben, sind sie damit auch gleichzeitig zuständige Bußgeldbehörde.

Ich halte es für sachgerecht, bei einer zukünftigen Novellierung des HDSG mir auch die Zuständigkeit für die Verfolgung dieser Ordnungswidrigkeiten zu übertragen und § 22 Abs. 4 HDSG entsprechend zu ergänzen.

4.1.2.2
Verfolgung von Ordnungswidrigkeiten aufgrund anderer gesetzlicher Regelungen

Schließlich gibt es auch weitere datenschutzrechtliche Bußgeldtatbestände, für die ich derzeit nicht zuständig bin. Dies gilt insbesondere für Verstöße im Bereich des Sozialdatenschutzes. Da es auch in diesem Kontext keine ausdrückliche gesetzliche Regelung zur Zuständigkeit gibt, gilt hier ebenfalls die allgemeine Regelung, dass die fachlich zuständige oberste Landesbehörde zu entscheiden hat.

Da die Situation der des BDSG vergleichbar ist – gerade auch im Umfang der Bußgeldtatbestände – wäre für eine zukünftige Novellierung des HDSG überlegenswert, auch die Zuständigkeit entsprechend zu regeln, so wie es in einigen Bundesländern erfolgt ist.

Stelle ich im Rahmen meiner Zuständigkeit zur Datenschutzkontrolle Verstöße gegen die Datenschutzregelungen aus dem Bereich des Sozialdatenschutzes fest, die den Verdacht einer Straftat nahelegen, steht auch mir ausdrücklich das Recht zu, Strafanzeige zu erstatten. Dies entspricht der Anforderung aus Art. 28 Abs. 3 der EG-Datenschutzrichtlinie an die Kompetenzen der unabhängigen Datenschutzkontrollinstanzen.

Art. 28 Abs. 3 EG-Datenschutzrichtlinie

Jede Kontrollstelle verfügt insbesondere über

- *Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;*
- *wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;*
- *das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.*

Da es eine entsprechende Regelung im HDSG nicht gibt, sollte auch dies bei einer zukünftigen Novellierung Berücksichtigung finden.

4.1.2.3
Lücke bei der Ahndung von Datenschutzverstößen

Immer wieder wenden sich Eingeber an mich, um die Sanktionierung anderer Verstöße als die von § 41 HDSG erfassten zu erreichen. Im Rahmen des HDSG ist eine Verfolgung jedoch nur denkbar, wenn die Voraussetzung der Ahndung als Straftat erfüllt ist. Dazu muss der Verstoß mit Schädigungs- oder Bereicherungsabsicht begangen werden.

§ 40 HDSG

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten entgegen den Vorschriften dieses Gesetzes

1. *erhebt, speichert, zweckwidrig verwendet, verändert, übermittelt, zum Abruf bereithält oder löscht,*
2. *abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder einen Dritten veranlasst,*

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Abs. 1 findet nur Anwendung, soweit die Tat nicht in anderen Vorschriften mit Strafe bedroht ist.

Dass Fehler der Daten verarbeitenden Stelle als Teil der öffentlichen Verwaltung nicht bußgeldbewehrt sind, erklärt sich daraus, dass der Staat sich nicht selbst bestrafen kann. Solche Fälle kann ich nur dadurch sanktionieren, indem eine formale Beanstandung ausspreche.

Allerdings ist nicht jedes Fehlverhalten eines Mitarbeiters bei der Datenverarbeitung der Daten verarbeitenden Stelle selbst zuzurechnen. Dies gilt insbesondere für die Fälle, in denen einzelne Mitarbeiter Daten, auf die sie zu dienstlichen Zwecken zugreifen dürfen, nutzen, um sie im privaten Kontext zu verwenden. Vor allem dann, wenn mit solchen Kenntnissen gegenüber Dritten geprahlt wird oder etwa ein Polizeibeamter wissen möchte, ob über seine neuen Bekannten etwas bei der Polizei bekannt ist, wird in aller Regel die Voraussetzung für eine Straftat nicht vorliegen. Denn er handelt dann nicht gegen Entgelt oder in der Absicht, sich selbst oder einen anderen zu bereichern oder zu schädigen.

Zwar kann in solchen Fällen ein Disziplinarverfahren erfolgen, den Betroffenen ist aber häufig nur schwer vermittelbar, warum keine weitere Ahndung erfolgt. Insbesondere wenn sie wissen, dass sie selbst bei einer vergleichbaren Handlung im Anwendungsbereich des BDSG mit einem Bußgeldverfahren rechnen müssten. In anderen Bundesländern ist der Katalog der möglichen Ordnungswidrigkeiten weiter. Der Gesetzgeber sollte daher bei einer zukünftigen Novellierung des Gesetzes auch in Hessen an eine Ausweitung der Bußgeldtatbestände auf Verfehlungen von Behördenbediensteten denken.

4.1.3
Bußgeldverfahren, weil der gesetzliche Vertreter einer juristischen Person einen Datenschutzverstoß verantwortet

Verantwortlich für die Einhaltung des BDSG ist die Daten verarbeitende Stelle. Wenn diese eine juristische Person ist, handelt für sie ein gesetzlicher Vertreter. Bei der Ahndung in Bußgeldverfahren wird damit zunächst an seine Verantwortung angeknüpft.

Die Bußgeldstelle hat im vergangen Jahr wegen verschiedener Datenschutzverstöße gegen juristische Personen ermittelt. Gerade im Zusammenhang mit Fällen, in denen es darum geht, dass Auskunftsverlangen der Aufsichtsbehörde nicht beantwortet werden (§ 43 Abs. 1 Nr. 10 i. V. m. § 38 Abs. 3 Satz 1 BDSG), kam es nach Zustellung des Bußgeldbescheides zu heftigen Reaktionen der Verantwortlichen. Sie beschwerten sich telefonisch darüber, dass sie die Schreiben der Aufsichtsbehörde nicht erhalten hätten und man sie dafür nicht verantwortlich machen könne.

§ 30 OWiG ermöglicht es, Geldbußen gegen juristische Personen oder Personenvereinigungen zu verhängen, wenn eine ihrer Leitungspersonen eine Straftat oder Ordnungswidrigkeit begangen hat, die die juristischen Personen bzw. Personenvereinigungen treffende Pflichten verletzt oder die zu deren Bereicherung geführt hat, bzw. führen sollte.

Der juristischen Person selbst oder der Personenvereinigung kann keine Ordnungswidrigkeit vorgeworfen werden. Über § 30 OWiG wird das Handeln der Organe und Vertreter der juristischen Person oder Personenvereinigung zugerechnet und sie wird so gestellt, als hätte sie selbst (wie eine natürliche Person) die Tat begangen. Die Festsetzung der Geldbuße gegen die juristische Person bzw. Personenvereinigung erfolgt dann als Nebenfolge der Ordnungswidrigkeit eines gesetzlichen oder sonstigen Vertreters in leitender Stellung.

§ 30 Abs. 1 OWiG

(1) Hat jemand

1. *als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs,*
2. *als Vorstand eines nicht rechtsfähigen Vereins oder als Mitglied eines solchen Vorstandes,*
3. *als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft,*
4. *als Generalbevollmächtigter oder in leitender Stellung als Prokurist oder Handlungsbevollmächtigter einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung oder*
5. *als sonstige Person, die für die Leitung des Betriebs oder Unternehmens einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung verantwortlich handelt, wozu auch die Überwachung der Geschäftsführung oder die sonstige Ausübung von Kontrollbefugnissen in leitender Stellung gehört,*

eine Straftat oder Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, so kann gegen diese eine Geldbuße festgesetzt werden.

§ 9 OWiG ermöglicht es, den Vertreter zur Verantwortung zu ziehen. Zwar liegen die Tatbestandsmerkmale mit besonderem persönlichen Bezug, wie z. B. die Auskunftspflicht aus § 38 BDSG, beim Vertreter nicht vor, aber sie werden ihm über § 9 OWiG zugerechnet, ohne dass die juristische Person oder die Personenvereinigung entlastet wird. Pflicht und Handeln fallen in diesen Konstellationen auseinander. Die Lücke wird durch § 9 OWiG geschlossen, indem der Anwendungsbereich von Bußgeldvorschriften, die die juristische Person oder Personenvereinigung treffen, auch auf die gesetzlichen Vertreter und die Beauftragten ausgeweitet wird. Wer zum Kreis der Vertreter gehört, wird im Einzelnen durch das Privat-, Handels- und Gesellschaftsrecht bestimmt (z. B. Geschäftsführer, Vorstand, etc.). § 9 OWiG zählt die Zurechnungsmöglichkeiten abschließend auf.

§ 9 OWiG

(1) Handelt jemand

1. *als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs,*
2. *als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft oder*
3. *als gesetzlicher Vertreter eines anderen,*

so ist ein Gesetz, nach dem besondere persönliche Eigenschaften, Verhältnisse oder Umstände (besondere persönliche Merkmale) die Möglichkeit der Ahndung begründen, auch auf den Vertreter anzuwenden, wenn diese Merkmale zwar nicht bei ihm, aber bei dem Vertretenen vorliegen.

(2) Ist jemand von dem Inhaber eines Betriebes oder einem sonst dazu Befugten

1. *beauftragt, den Betrieb ganz oder zum Teil zu leiten, oder*
2. *ausdrücklich beauftragt, in eigener Verantwortung Aufgaben wahrzunehmen, die dem Inhaber des Betriebes obliegen,*

und handelt er auf Grund dieses Auftrages, so ist ein Gesetz, nach dem besondere persönliche Merkmale die Möglichkeit der Ahndung begründen, auch auf den Beauftragten anzuwenden, wenn diese Merkmale zwar nicht bei ihm, aber bei dem Inhaber des Betriebes vorliegen. Dem Betrieb im Sinne des Satzes 1 steht das Unternehmen gleich. Handelt jemand auf Grund eines entsprechenden Auftrages für eine Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, so ist Satz 1 sinngemäß anzuwenden.

(3) Die Absätze 1 und 2 sind auch dann anzuwenden, wenn die Rechtshandlung, welche die Vertretungsbefugnis oder das Auftragsverhältnis begründen sollte, unwirksam ist.

Deshalb hat die Bußgeldbehörde zwei Möglichkeiten. Wie sie sich entscheidet, hängt vom Einzelfall ab: Die Ahndung der Ordnungswidrigkeit erfolgt entweder im einheitlichen Verfahren (§ 30 Abs. 1 OWiG), dann wird eine Geldbuße gegen den Vertreter und eine Geldbuße gegen die juristische Person bzw. Personenvereinigung als Nebenfolge der Ordnungswidrigkeit des Vertreters festgesetzt (z. B. gegen eine GmbH und ihren Geschäftsführer). Oder aber die Ahndung erfolgt im selbstständigen Verfahren (§ 30 Abs. 4 OWiG), dann wird eine Geldbuße nur gegen die juristische Person bzw. die Personenvereinigung als Nebenfolge der Ordnungswidrigkeit des Vertreters festgesetzt.

4.2 Videoüberwachung

Die Videoüberwachung wird als Sicherheitstechnik stets kontrovers diskutiert. Bereits im Jahre 2005 erlangte „die Videoüberwachung“ zweifelhaften Ruhm, als sie in der Kategorie Technik für die schleichende Degradierung von Menschen zu überwachten Objekten und Verharmlosung von Tenden-

zen zu flächendeckender Überwachung den „Big Brother Award“ zugesprochen bekam. Trotzdem nimmt die Zahl der installierten Überwachungssysteme im Privatbereich stetig zu.

4.2.1
Allgemeines

Seit dem 1. Juli 2011 obliegt mir die Datenschutzaufsicht neben dem öffentlichen auch für den privaten Bereich. Hierzu zählt u. a. die in § 6b BDSG geregelte 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 Abs. 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.

Die Anzahl von Beschwerden über installierte Überwachungskameras steigt stetig. Im zurückliegenden Berichtszeitraum haben sich viele Bürgerinnen und Bürger an mich gewandt, weil sie durch die Installation von Überwachungskameras ihr Recht auf informationelle Selbstbestimmung beeinträchtigt sehen.

Die Beschwerden richten sich hauptsächlich gegen Überwachungen in Kaufhäusern und Gastronomiebetrieben sowie deren Außenfassaden, Wohnanlagen und Firmengebäude. Aber auch am Arbeitsplatz und im pri-

vaten Bereich sehen sich Bürgerinnen und Bürger zunehmend einer Kameraüberwachung ausgesetzt.

Gemäß § 6b Abs. 1 BDSG ist eine Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig. Es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Grundsätzlich ist von einer Videoüberwachung abzusehen, wenn der Überwachungszweck auch mit milderen Mitteln erreicht werden kann. Der Umstand der Beobachtung und die verantwortliche Stelle (§ 3 Abs. 7 BDSG) sind nach § 6b Abs. 2 BDSG durch geeignete Maßnahmen erkennbar zu machen.

Auch Kameraattrappen (sog. „Dummies“) sind als Geräte zur Videoüberwachung zu werten. Hierbei wird vor allem auf den „Überwachungsdruck“ abgestellt, der bereits durch die bloße Möglichkeit einer Videoüberwachung entsteht. Die betroffenen Personen können sich nicht sicher sein, ob sie beobachtet und/oder aufgezeichnet werden oder nicht. So entsteht ein (beabsichtigter) Verhaltenszwang, der als unzulässiger Eingriff in das Persönlichkeitsrecht zu werten ist.

Liegt mir eine Beschwerde gegen eine Videoüberwachung vor, fordere ich die für die Videoüberwachung verantwortliche Stelle unter Schilderung der gesetzlichen Bestimmungen zu einer Stellungnahme auf. Hierfür wird der verantwortlichen Stelle ein Fragenkatalog übersandt. Nach § 38 Abs. 3 BDSG haben mir die verantwortlichen Stellen auf Verlangen die notwendigen Auskünfte zu erteilen. 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 EUR geahndet werden.

4.2.2
Videoüberwachung in Kaufhäusern und Einzelhandelsgeschäften

Kaufhäuser und Einzelhandelsgeschäfte setzen zur Prävention von Straftaten immer mehr auf – mitunter flächendeckende – Videoüberwachung. Gegen eine Videoüberwachung in Anlieferungszonen, in Lagerräumen und nicht ständig besetzten Kassenbereichen bestehen in der Regel keine Bedenken, da der Arbeitsplatz von Bediensteten in diesen Fällen keiner permanenten Kameraüberwachung ausgesetzt ist.

Oftmals werden jedoch auch Bereiche erfasst, in denen eine Videoüberwachung datenschutzrechtlichen Bedenken begegnet oder unzulässig ist, bei-

spielsweise in Umkleidekabinen und Aufenthaltsräumen der Bediensteten, oder wenn durch die Ausrichtung einer Videokamera permanent der Arbeitsplatz von Bediensteten erfasst wird. Letzteres ist ausschließlich unter den Voraussetzungen des § 32 Abs. 1 BDSG zulässig.

§ 32 Abs. 1 BDSG

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Insbesondere Bäckereien und Friseursalons habe ich im Berichtszeitraum zum Entfernen oder Neuausrichten von installierten Videokameras auffordern müssen.

4.2.3
Videoüberwachung in Gastronomiebetrieben

In Gastronomiebetrieben dürfen Kundenbereiche, die mit Tischen und Sitzgelegenheiten ausgestattet sind, nicht mit Videokameras überwacht werden. In öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, wird das Persönlichkeitsrecht durch eine ständige Videoüberwachung erheblich beeinträchtigt.

Im Berichtszeitraum habe ich mehrere Gastronomiebetriebe überprüft. Neben den Kundenbereichen wurden mitunter auch Arbeitsplätze oder Straßen, Gehwege und Fußgängerzonen (Außenbestuhlung eines Cafes) von den Überwachungskameras erfasst. Durch das Entfernen oder Neuausrichten einzelner Überwachungskameras konnte stets ein datenschutzkonformer Zustand der Videoüberwachung hergestellt werden.

4.2.4
Videoüberwachung in Wohnanlagen

Die Zulässigkeit von Videokameras in Wohnanlagen ist einzelfallabhängig zu bewerten. Hier kommt es zunächst darauf an, wer verantwortliche Stelle nach § 3 Abs. 7 BDSG ist.

> *§ 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.*

Dies kann zum Einen die von der Wohnungseigentümergemeinschaft bestellte Hausverwaltung, aber auch ein Mieter oder Eigentümer sein.

Der Beschluss einer Wohnungseigentümergemeinschaft, dass eine Kameraüberwachung in den Eingangsbereichen von Hochhäusern einer Wohnanlage installiert werden soll, liegt in der Regungskompetenz der Gemeinschaft gemäß den §§ 15, 21 des Gesetzes über das Wohnungseigentum und das Dauerwohnrecht (WEG) bezüglich des Gebrauchs des Gemeinschaftseigentums. Hier kann der Einsatz von Überwachungskameras beispielsweise dann zulässig sein, wenn es in der Vergangenheit nachweislich zu Schäden durch Vandalismus gekommen ist. Gleiches gilt für die Videoüberwachung in einer zu der Wohnanlage gehörenden Tiefgarage, zu welcher ausschließlich die Mieter und Eigentümer Zutritt haben.

In seinem Urteil vom 8. April 2011 (Az.: V ZR 210/10) erachtet der Bundesgerichtshof eine Videokamera in einem Klingeltableau einer Wohnanlage 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.

Einzelnen Mietern oder Wohnungseigentümern ist zur Wahrung des Hausrechts lediglich die Überwachung ihres Sondereigentums gem. § 6b Abs. 1 Ziff. 2 BDSG gestattet.

4.2.5
Videoüberwachung im privaten Bereich

Eine Videoüberwachung zur Wahrung des Hausrechts ist im privaten Bereich grundsätzlich zulässig. Somit bestehen gegen die Kameraüberwachung des eigenen Grundstücks der verantwortlichen Stelle (dies kann

gem. § 3 Abs. 7 BDSG eine natürliche, als auch juristische Person sein) grundsätzlich keine Bedenken.

Werden jedoch auch öffentlich-zugängliche Bereiche erfasst, beispielsweise öffentliche Straßen, Parks und Gehwege, ist eine Kameraüberwachung nur zulässig, wenn die Voraussetzungen des § 6b Abs. 1 BDSG erfüllt sind.

> *§ 6b Abs. 1 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.*

Im Berichtszeitraum hat sich eine große Anzahl von Bürgerinnen und Bürgern an mich gewandt, die sich durch Videokameras von Nachbarn oder Firmen in der Nachbarschaft in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt sahen.

In vielen Fällen konnte durch ein persönliches Gespräch mit den verantwortlichen Stellen ein datenschutzgerechter Zustand der Kameraüberwachung herbeigeführt werden, da vielen Bürgerinnen und Bürgern das Bundesdatenschutzgesetz schlichtweg unbekannt ist. Vereinzelt stößt mein Tätigwerden bei Privatpersonen jedoch auf Unverständnis. Die von mir angeforderten Stellungnahmen werden nicht, nicht vollständig oder nicht rechtzeitig abgegeben. Einige zeigen sich auch gegen Erinnerungen resistent, sodass in diesen Fällen die Einleitung eines Ordnungswidrigkeitenverfahrens unumgänglich ist.

Durch verlockende Angebote von Discountern und Elektrofachmärkten gehe ich davon aus, dass die Zahl der Beschwerden im Bereich der privaten Videoüberwachung weiter steigen wird.

4.2.6
Videoüberwachung durch Tierbeobachtungskameras in hessischen Wäldern

Mir lagen im Berichtszeitraum mehrere Anfragen bezüglich der Rechtmäßigkeit des Einsatzes von Tierbeobachtungskameras vor. Als Tierbeobachtungskameras werden hier alle Geräte und Einrichtungen bezeichnet, die dazu dienen, Bilder und/oder Filme aufzuzeichnen.

Im 23. Tätigkeitsbericht für den nicht-öffentlichen Bereich in Hessen (2009), LT Drucks. 18/2942, wurde bereits unter Ziff. 13.1 zur Videobeobachtung an einer „Wildschweinkirrung“ Stellung bezogen.

Wie verbreitet der Einsatz von Tierbeobachtungskameras in hessischen Wäldern ist, ist leider nur schwer nachvollziehbar.

§ 24 des Hessischen Forstgesetzes (ForstG) erlaubt in Abs. 1, S. 1 grundsätzlich jedem das Betreten des Waldes, sodass der Wald als öffentlich-zugänglicher Bereich im Sinne des § 6b BDSG zu sehen ist. Auch ein Wald, der sich im Privateigentum befindet, ist öffentlich zugänglich, da § 24 des ForstG explizit von „jedem“ Wald spricht. § 6b Abs. 1 Ziff. 2 BDSG (Ausübung des Hausrechts) ist daher nicht anwendbar.

Nach § 6b Abs. 1 Ziff. 3 BDSG ist die Videobeobachtung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig, soweit sie erforderlich ist und keine Anhaltspunkte bestehen, das schutzwürdige Interessen der Betroffenen überwiegen.

Mit dem HMUELV (Oberste Jagdbehörde) vertrete ich gemeinsam folgende Rechtsauffassung:

Die Interessen der Betroffenen (Waldbesucher, Spaziergänger etc.) haben regelmäßig Vorrang und das rein private Betreiben von Tierbeobachtungskameras im öffentlich zugänglichen Raum ist datenschutzrechtlich grundsätzlich (auch z. B. zum Schutz vor Eigentum) nicht erlaubt. Eine Ausnahme bildet der Betrieb von Tierbeobachtungskameras zu konkreten, wissenschaftlichen Zwecken. Dies bedeutet:

1. Der Betrieb von Tierbeobachtungskameras wird von einer zuständigen Behörde (entgeltlich oder unentgeltlich) beauftragt oder findet im Rahmen einer solchen Beauftragung statt und die Ergebnisse werden der zuständigen Behörde zur Verfügung gestellt.
2. Das Vorhaben ist konkret beschrieben, nachvollziehbar begründet und dokumentiert (Ziel und Zweck des Vorhabens, Einsatzbereich, Zeitraum des Einsatzes, verantwortliche Person/Institution).
3. Der Umstand der Beobachtung sowie die verantwortliche Stelle sind im Umfeld der Tierbeobachtungskameras erkennbar zu machen.

Abbildungen von Personen sind unverzüglich unkenntlich zu machen oder zu löschen.

4.3
Keine Bestätigung eines in den Medien behaupteten Missbrauchs der Videoanlage in einem Discountermarkt in Südhessen

Enthüllungsjournalismus vermag zwar oft auch der Datenschutzbehörde sachdienliche Hinweise zu geben. Im konkreten Fall gingen jedoch die Behauptungen – soweit überprüfbar – datenschutzrechtlich ins Leere. Sie beschädigten die Reputation eines nur vermeintlich Betroffenen.

Der Aufmacher-Bericht eines Nachrichtenmagazins verbunden mit einer am Vorabend gesendeten Talkshow schreckte an einem Montagmorgen auf: Bei einem großen Discounter soll in einigen hessischen Filialen die Videoanlage in den Verkaufsräumen dazu genutzt worden sein, „sommerlich-leicht bekleidete Kundinnen“ heimlich zu filmen. Die „Filmchen seien dann auf CD gebrannt sogar unter der Hand im Kollegenkreis“ verteilt worden. Es sei ein „offenes Geheimnis“, dass sich Filialleiter einen Spaß daraus machten, vor allem die Bildaufzeichnungen von Frauen in kurzen Röcken oder mit ausgeschnittenen Tops, wenn sie sich über die Kühltheke beugten oder vor Regalen bückten, heranzuzoomen. Zudem soll es durch die Kameraeinstellung möglich sein, im EC-Karten-Bereich der Kassen die PINs auszuspionieren. Geschehen sei dies alles in den Filialen in Frankfurt und einem südhessischen Ort. Zeitgleich mit dem Artikel und der Sendung wurde die Neuerscheinung des Buches eines ehemaligen Mitarbeiters des Discounters beworben, der diese Vorwürfe erhob.

Ich habe auf die Veröffentlichungen unverzüglich reagiert und das Nachrichtenmagazin noch am selben Vormittag gebeten, nähere Angaben zu den meiner Zuständigkeit unterliegenden Filialen zu machen, damit ich diesen ungeheuerlichen Vorwürfen nachgehen konnte. Leider bekam ich von dem Magazin keine weiteren Informationen, sodass ich mich mit eigenen Recherchen begnügen musste.

Ich habe die einzige für mich aus dem Artikel eindeutig identifizierbare Filiale in dem südhessischen Ort unverzüglich aufgesucht und eine Vor-Ort-Überprüfung durchgeführt sowie den Filialleiter, der die Filiale seit 2006 übernommen hat, angehört. Die Zentralverwaltung habe ich aufgefordert, zu den Einstellungen der Videoanlage Stellung zu nehmen und mir anhand der vorhandenen Protokolldateien nachzuweisen, ob bzw. welche Zugriffe in das Videosystem erfolgt sind und ob Einstellungen der Kameras verändert oder Bilder (Daten) auf CDs übertragen wurden.

Die Zentrale der Gesellschaft zeigte sich von den Vorwürfen ebenfalls schockiert, sagte bereitwillige Kooperation und umfängliche Unterstützung bei der Aufklärung zu. Sie stellte die angeforderten Unterlagen und Aus-

künfte unverzüglich zur Verfügung. Da das Unternehmen ein umfangreiches Datenschutzkonzept zum Einsatz von Videokameras in seinen Filialen umsetzt, war insbesondere die zur Zugriffskontrolle eingesetzte Protokollierung für die Sachaufklärung von Bedeutung.

Die Auswertung der Protokolle ergab, dass im gespeicherten Zeitraum von einem Monat keine Zugriffe irgendwelcher Art erfolgten. Auch stellte sich heraus, dass die Vorwürfe, in der Filiale würden voyeuristische Aufnahmen gefertigt, in sich widersprüchlich und unstimmig waren. Eine Videoüberwachung gibt es dort erst, seitdem der jetzige Filialleiter die Leitung übernommen hat. Da dieser aber – wie einer der beiden Autoren in einem späteren Radio-Interview erklärte – nicht betroffen sei, können in dieser Filiale die behaupteten Aufnahmen gar nicht gemacht worden sein.

Zudem war die Filiale zwischenzeitlich in neue Räumlichkeiten umgezogen. Die dort vorgefundenen Einstellungen des Video-Systems lassen den geschilderten Missbrauch bereits technisch und organisatorisch nicht zu. CDs können mangels Laufwerk nicht verwendet werden. Lediglich bei besonderen Vorfällen (wie z. B. Überfällen) können, durch ein bestimmtes Procedere abgesichert, protokollierte Auszüge für polizeiliche Ermittlungen erstellt werden. Auch die Überprüfung der Kameraeinstellungen im Kassenbereich ergab, dass ein Ausspionieren von Karten-PINs nicht möglich ist. Weder Kunde noch Bezahlvorgang sind auf dem Bildschirm erkennbar. Die entsprechenden Bildabschnitte sind geschwärzt.

Erst zweieinhalb Monate nach der Überprüfung äußerte sich einer der beiden Autoren des Artikels des Nachrichtenmagazins und teilte mir mit, dass es aus grundsätzlichen Erwägungen keine Rechercheunterlagen herausgibt. Eine frühere Nachricht aus seinem Hause habe mich unerklärlicher Weise nicht erreicht. Die dennoch beigefügten – vertraulichen – Hinweise führten zu keinen anderen Feststellungen. Wenn die Vorfälle tatsächlich stattgefunden haben sollten, dann kann dies nur vor mindestens sechs Jahren geschehen sein. Nach dieser langen Zeit ist ein Nachweis nicht mehr zu führen. Auch das angeblich „offene Geheimnis“ der auf CD gebrannten voyeuristischen Videoaufnahmen war den befragten Mitarbeitern nicht bekannt.

Im Ergebnis haben sich die gegenüber der Filiale in dem südhessischen Ort erhobenen Vorwürfe nicht bestätigt. Die Veröffentlichung personenbeziehbarer Daten – ohne Nachprüfung des Wahrheitsgehaltes oder Bezugnahme auf den (lange zurückliegenden) Zeitraum – hat erhebliche Auswirkungen auf den vermeintlich betroffenen Filialleiter gehabt: Er war in diesen Tagen einem öffentlichen Spießrutenlauf ausgesetzt und musste mit großem Aufwand versuchen, sich vor Familie, Verwandten, Nachbarn und Kundschaft

zu rechtfertigen und sich gegen die falschen Verdächtigungen zu verteidigen.

Der Fall zeigte aber auch, dass eine wirksame Umsetzung von technischen und organisatorischen Datenschutzmaßnahmen (§ 9 BDSG) in Unternehmen nicht Selbstzweck ist, sondern bereits aus Eigeninteresse der Firmen zur Abwehr von Vorwürfen von Datenschutzverletzungen erforderlich sein kann.

4.4
Immer wieder „bcc“-Fehler beim Versenden von Massen-E-Mails

Das Versenden von Massen-E-Mails zu Werbezwecken und geschäftlichen Informationen stellt im Geschäftsalltag vieler Firmen oft eine Routinetätigkeit dar, die beiläufig erledigt wird. Die Verantwortlichen müssen trotzdem durch entsprechende (auch wiederholte) Anweisungen sicherstellen, dass ihre Beschäftigten die Empfängerliste datenschutzgerecht bearbeiten.

Auch in diesem Berichtsjahr kam es mehrfach zu Beschwerden, weil bei der Versendung von Massen-E-Mails durch Unternehmen alle E-Mail-Adressen im „An“ oder „cc“-Adressfeld für alle Empfänger offen lesbar aufgeführt wurden. Erneut waren es Unternehmen, die z. B. einen Newsletter oder Kundeninformationen verschickten.

Aus datenschutzrechtlicher Sicht handelt es sich bei jedem einzelnen Adressdatum, das im offenen Verteiler an alle Empfänger aufgeführt wird, um die Übermittlung personenbezogener Daten. Diese Übermittlung ist, soweit sie ohne Rechtsgrundlage erfolgt, nicht erforderlich und damit datenschutzrechtlich unzulässig. Es handelt sich um einen Ordnungswidrigkeitstatbestand, der mit einer Geldbuße bis zu 300.000 EUR geahndet werden kann.

Wie sich bei der jeweiligen Aufklärung der einzelnen Fälle herausstellte, geschahen die Vorfälle immer aufgrund von Flüchtigkeitsfehlern, in Eile oder durch Unaufmerksamkeit und fehlende Sorgfalt bei der Bearbeitung. Die Konsequenzen dieser Fahrlässigkeiten können mitunter jedoch erheblich sein:

Mit der Datenübermittlung werden Empfänger gegen ihren Willen als Kunde oder Kontaktperson des Unternehmens „geoutet“. Eine Information, die möglicherweise aus guten Gründen bislang vertraulich war und deren Offenlegung dann sehr verärgert. Hinzu kommt, dass andere E-Mail-Empfänger die erhaltenen E-Mail-Adressen ihrerseits für unverlangte Werbe-E-Mails nutzen können. Die hohe Zahl der dann eingehenden E-Mails kann zur Funktionsunfähigkeit eines E-Mail-Accounts führen. Zudem werden durch

diese Adressiervariante die E-Mail-Adressen der Empfänger einer kaum einschätzbaren Gefährdung durch Schadprogramme ausgesetzt. Wenn z. B. auch nur ein einziger E-Mail-Empfänger nicht über einen aktuellen Virenschutz verfügt, kann ein entsprechendes Schadprogramm auf seinem PC die mit der Massen-E-Mail übermittelten Daten zur eigenen Weiterverbreitung und/oder zur Fälschung der Absenderangaben entsprechender Trojaner-E-Mails nutzen.

Je nach Art des Unternehmens und Inhalt der E-Mail können Betroffene das Vertrauen in das Unternehmen verlieren, das ja bereits mit den E-Mail-Adressdaten nicht sorgfältig umgeht und geschäftliche Konsequenzen ziehen, die sich auch auf die Beschäftigten auswirken können, die den Fehler verursacht haben.

Besonders folgenreich war die „offene" Meinungsumfrage einer Personalberatung. Dort wurde einem Studienpraktikanten Gelegenheit gegeben, Informationen für seine Hausarbeit durch Versenden von Fragebögen an die Kunden einzuholen. Weil er dabei versehentlich alle Kunden im offenen Empfängerfeld aufführte, beendete der Arbeitgeber das Praktikum aufgrund des Vorfalles vorzeitig.

Grundsätzlich gilt, dass sich E-Mails mit offen gelegten E-Mail-Adressen oder für alle Empfänger offen lesbaren E-Mail-Verteilern nur für geschlossene Benutzergruppen (z. B. innerhalb eines Unternehmens) eignen und ansonsten **nur als Blindkopie („bcc")** verschickt werden dürfen, bei der eine unzulässige Übermittlung personenbezogener Daten über ein E-Mail-Adressierfeld ausgeschlossen ist.

Die Unternehmensleitung ist für die sachgerechte Umsetzung dieser Datenschutzanforderung verantwortlich. Sie muss die Beteiligten immer wieder aufs Neue auf die Risiken aufmerksam machen, informieren und ggf. auch kontrollieren, wenn die bearbeitende Person in der Handhabung nicht geübt ist.

4.5
Zuständigkeitsbereich des betrieblichen Datenschutzbeauftragten

Betriebliche Datenschutzbeauftragte sind nicht nur für die Überwachung der ordnungsgemäßen und datenschutzkonformen Verarbeitung von Kundendaten zuständig, sondern haben die gleiche Verantwortung auch für die personenbezogenen Daten der Mitarbeiter im Unternehmen.

Ein Mitarbeiter eines mittelständischen Unternehmens fragte bei mir an, was er dagegen tun könne, dass die Geschäftsleitung seine Krankmeldung jeweils durch eine an alle Mitarbeiter des Unternehmens verschickte E-Mail

publik mache. Aus dieser könne man dann ersehen, dass er z. B. vier Tage krankgeschrieben sei.

Ich empfahl dem Petenten, sich mit seinem Anliegen zunächst an den betrieblichen Datenschutzbeauftragten zu wenden. Falls es diesem nicht gelinge, das datenschutzrechtlich unkorrekte Verhalten des Unternehmens abzustellen, könne er sich gerne wieder an mich wenden und ich würde dann entsprechend tätig werden.

Daraufhin entgegnete mir der Mitarbeiter ganz erstaunt, dass er davon ausgegangen sei, dass der betriebliche Datenschutzbeauftragte lediglich für die Kundendaten zuständig sei und ihm nicht bewusst gewesen sei, dass diesem auch die Aufsicht über die Mitarbeiterdaten obliege.

Diese Auffassung hörte ich nicht zum ersten Mal von Mitarbeitern, mit denen ich in Kontakt stand. Darüber hinaus musste ich feststellen, dass auch bestellte Datenschutzbeauftragte sich vorrangig für den Kundendatenschutz zuständig fühlen und der Arbeitnehmerdatenschutz oft völlig in den Hintergrund tritt.

Hier erscheint es sinnvoll, über die Berufsverbände der betrieblichen Datenschutzbeauftragten darauf hinzuweisen, dass der Arbeitnehmerdatenschutz mit der gleichen Intensität wie der Kundendatenschutz betrieben werden muss und dass die Verantwortlichkeit des betrieblichen Datenschutzbeauftragten auch für die Mitarbeiterdaten in den Unternehmen intensiver kommuniziert werden muss.

4.6
Interessenkonflikte beim betrieblichen Datenschutzbeauftragten – „Inkompatibilität“

Bei der Bestellung eines nebenamtlichen Datenschutzbeauftragten sind nicht nur betriebliche Interessenskollisionen zu vermeiden. Auch private Beziehungen können ein Ausschlusskriterium für eine Bestellung sein.

Immer wieder erreichen mich Anfragen von Unternehmen, mit welcher Funktion und aus welchem Aufgabengebiet ein Mitarbeiter oder eine Mitarbeiterin zum bzw. zur betrieblichen Datenschutzbeauftragten (bDSB) bestellt werden kann.

Grundsätzlich ist bei der Bestellung von nebenamtlichen bDSB darauf zu achten, dass die betreffende Person nicht mit ihren übrigen Aufgaben in Interessenkollision gerät, da andernfalls die Zuverlässigkeit, die das BDSG in § 4f Abs. 2 fordert, infrage gestellt wird und die beabsichtigte Kontrollfunktion nicht erfüllt werden kann.

§ 4f BDSG

(1)...

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. ...

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei....

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nichtöffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(5) ...

Betriebliche Datenschutzbeauftragte können in eine Situation geraten, in der sie auch gegen die Interessen oder Meinungen der Unternehmensleitung handeln müssen. In keinem Fall kann daher der Inhaber selbst, der Geschäftsführer oder ein Vorstandmitglied gleichzeitig bDSB sein. Zum einen, weil er sich selbst kontrollieren müsste, und zum anderen, weil das BDSG die unmittelbare Unterstellung des bDSB unter die Leitung des Unternehmens verlangt (§ 4f Abs. 3 BDSG) und damit der Unternehmer selbst, die Mitglieder der Geschäftsleitung oder des Vorstandes von dieser Funktion ausgeschlossen sind.

Darüber hinaus sollte auch nicht der Leitung der Datenverarbeitung, der Leitung der Personalabteilung, der Leitung des Vertriebs oder der Leitung der Marketing-Abteilung die Funktion des nebenamtlichen bDSB übertragen werden, denn immer dann, wenn Beschäftigte zum bDSB bestellt werden, die als bDSB ihre eigene Tätigkeit in einer anderen Funktion im Unternehmen kontrollieren müssen, ist ein Interessenkonflikt vorprogrammiert.

Daher sollte vor jeder Bestellung von Personen, insbesondere aus einem der genannten Organisationsbereiche, immer kritisch geprüft werden, wie wahrscheinlich ein Interessenskonflikt sein kann, der über das unvermeidbare Maß hinausgeht, insbesondere, wenn z. B. eigene Vorgesetzte kontrolliert werden müssten.

Ein besonderer Fall lag mir vor, als die kaufmännische Assistentin eines Verlages anfragte, ob etwas dagegen spräche, dass sie als kaufmännische Assistentin und Ehefrau des Geschäftsführers zur bDSB bestellt würde. Die notwendige Fachkunde sei vorhanden und zuverlässig sei sie auch.

Das BDSG und einschlägige Kommentare stellen lediglich auf den Interessenkonflikt bezüglich der Funktion im Unternehmen ab. Mögliche verwandtschaftliche oder persönliche Beziehungen und daraus resultierende Konflikte werden nicht thematisiert.

Es spricht auch formaljuristisch nichts dagegen, wenn ein fachkundiger Verwandter oder Ehepartner des Geschäftsführers zum bDSB bestellt würde, trotzdem riet ich davon ab und empfahl, eine andere Lösung zu suchen. Denn auch verwandtschaftliche oder enge persönliche Beziehungen können problematisch sein, weil die notwendige Distanz zur verantwortlichen Stelle und die erforderliche Bereitschaft, einen Konflikt durchzustehen, fehlen können. Aufgrund der engen persönlichen Beziehung in der geschilderten Konstellation sind Interessenkonflikte ggf. auch privater Natur nicht auszuschließen, und damit kann die notwendige Zuverlässigkeit infrage stehen.

Darüber hinaus nimmt der bDSB auch eine Vertrauensstellung gegenüber den übrigen Mitarbeitern und Mitarbeiterinnen des Unternehmens ein. Gemäß § 4f Abs. 4 und 4a BDSG ist er zu Verschwiegenheit über die Identität des Betroffenen verpflichtet, und es steht ihm u. U. ein Zeugnisverweigerungsrecht zu. Hier sollte bereits jeglicher Anschein vermieden werden, der diese Vertrauensposition in Frage stellt und Mitarbeiter und Mitarbeiterinnen ggf. davon abhält, ihr Recht auf informationelle Selbstbestimmung gegenüber dem Arbeitgeber geltend zu machen.

Das Unternehmen war einsichtig und hat von der Bestellung der Ehefrau des Geschäftsführers als nebenamtliche Datenschutzbeauftragte abgesehen.

4.7
Das unabdingbare Recht auf Auskunft über die eigenen Daten nach § 13 Abs. 7 TMG und § 34 Abs. 1 BDSG

Einigen Unternehmen ist immer noch nicht geläufig, dass Betroffene ein unabdingbares und unentgeltliches Recht auf Auskunft über die zu ihrer Person gespeicherten Daten und zu deren Herkunft haben. Auch der gesetzlich geregelte Umfang des Auskunftsrechts ist häufig unbekannt.

Das Recht darauf, nach § 13 Abs. 7 TMG und § 34 Abs. 1 BDSG Auskunft über die bei einer nicht öffentlichen Stelle gespeicherten Daten zur eigenen

Person zu erhalten und dabei auch erfahren zu können, woher diese Stelle die Daten empfangen und an wen diese weitergegeben wurden, ist oft der erste datenschutzrechtliche Anspruch, den Betroffene gegenüber personalisiert mittels Postbrief oder E-Mail werbenden Unternehmen und allen anderen verantwortlichen Stellen, die personenbezogene Daten verarbeiten, geltend machen.

Erst wenn die Daten den Betroffenen genau benannt sowie Herkunft und mögliche Empfänger offenbart wurden, können weitere datenschutzrechtliche Schutzmechanismen, wie die Rechte auf Berichtigung, Löschung oder Sperrung (§ 35 BDSG) greifen. Den Betroffenen wird durch die Auskunftserteilung weiterhin die Möglichkeit eröffnet, ihre Rechte auch den Stellen gegenüber geltend zu machen, von denen ihre Daten stammten und an die ihre Daten übermittelt wurden. Das Auskunftsrecht gehört daher zu den unabdingbaren Rechten von Betroffenen nach § 6 Abs. 1 BDSG.

§ 6 Abs. 1 BDSG

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

§ 34 Abs. 1 BDSG

Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

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

§ 13 Abs. 7 TMG

Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.

Obwohl es sich bei § 34 Abs. 1 BDSG um eine Rechtsvorschrift handelt, die auch schon vor den BDSG-Novellen der letzten Jahre Bestand hatte, wenden sich immer noch viele Betroffene mit der Bitte um Unterstützung an mich, da Unternehmen, Werbetreibende, Betreiber von Homepages und E-Mail-Versender ihre datenschutzrechtliche Auskunftspflicht gegenüber Betroffenen nicht genau kennen oder nicht sonderlich ernst nehmen.

Einige Bürgerinnen und Bürger beschwerten sich bei mir, weil verarbeitende Stellen ihr teilweise per Einschreiben versandtes Auskunftsersuchen nicht

beantworteten und auch Nachfragen ignorierten. Alle betroffenen Daten verarbeitenden Gewerbetreibenden, Unternehmen und Anbieter von Telemedien (Homepages) wurden von mir über die Rechtslage in Kenntnis gesetzt und auf den seit 1. September 2009 geltenden Bußgeldtatbestand des § 43 Abs. 1 Nr. 8a BDSG (Nichtbeantwortung oder unvollständige Beantwortung des Auskunftsersuchens von Betroffenen) hingewiesen. Zur zeitnahen Erledigung wurde allen Stellen eine angemessene Frist gesetzt, innerhalb derer die Auskunft an den Betroffenen zu erteilen war.

Nur wenige dieser Stellen kamen meiner Aufforderung nicht unverzüglich nach. Hierzu zählte z. B. ein Dienstleistungsunternehmen, das auch noch deutlich verspätet meine Fragen beantwortete und damit zusätzlich gegen § 38 Abs. 3 Satz 1 BDSG verstieß. Gegen dieses Unternehmen wurde ein Bußgeldverfahren nach § 43 Abs. 1 Nr. 10 BDSG eingeleitet.

Bußgeldverfahren nach § 43 Abs. 1 Nr. 8a wurden eingeleitet gegen einen professionellen Adresshändler, der ein nachweislich zugestelltes Auskunftsersuchen nicht beantwortet hatte, sowie gegen einen Versender von unerwünschter E-Mail-Werbung, der das Auskunftsersuchen ignoriert und insbesondere die Frage nach der Herkunft der E-Mail-Adresse des Beschwerdeführers nicht beantwortet hatte.

Oft erhalten Bürgerinnen und Bürger auf ihre Auskunftsersuchen an Unternehmen, von denen sie z. B. Werbe-E-Mails oder Reklamebriefe zugesandt bekommen, unvollständige Antworten, in denen aus Unkenntnis der Rechtslage die Angaben zur Datenherkunft fehlen oder in denen die gespeicherten Daten nicht genau benannt, sondern nur die jeweiligen Datenarten (Name, Anschrift etc.) abstrakt aufgezählt werden. Immer wieder musste ich im Berichtsjahr daher aufgrund von Beschwerden Betroffener speichernde Stellen darauf hinweisen, dass die gespeicherten oder zur Werbung genutzten Daten selbst genau und vollständig zu nennen sind.

Auch Datenherkunft und -empfänger sind nach § 34 Abs. 1 Nr. 1, 2 BDSG mitzuteilen, wobei Informationen über Datenquelle und Datenempfänger nur dann sinnvoll von Betroffenen genutzt werden können, wenn diese genau mit Name und Postanschrift genannt werden. Ein hessischer Adresshändler und seine Fachanwälte konnten sogar erst nach langer Diskussion mit dem Hinweis auf die Bußgeldvorschrift des § 43 Abs. 1 Nr. 8a BDSG überzeugt werden, dass er seine Kunden, an die er Datensätze Betroffener zu Werbezwecken vermietet hatte, mit Name und Postanschrift zu benennen hat. Einem Betroffenen lediglich einen Firmen- oder Markennamen als Datenempfänger zu nennen, baut für die Umworbenen unnötige Hürden bei der dortigen Inanspruchnahme ihrer Datenschutzrechte auf und erfüllt die gesetzlichen Vorgaben daher nicht. Auch falls es sich bei dem Datenemp-

fänger oder der Datenquelle um eine natürliche Person handelt, ist diese mit Name und Anschrift gegenüber dem Betroffenen zu benennen, da sie schließlich als verantwortliche Stelle nach § 3 Abs. 8 BDSG auftritt. Eine entsprechende Argumentation des Adresshändlers mit dem Ziel, diesbezüglich keine Auskunft zu erteilen, musste ich zurückweisen.

Über den gleichen Adresshändler wurde mir die Beschwerde vorgetragen, dieser mache in einem Fall den Nachweis einer Datenschutzverletzung zur Bedingung einer Selbstauskunft. Der Betroffene sollte zunächst beweisen, dass von dem Unternehmen ein Datenschutzverstoß begangen worden sei. Dies sei Bedingung für die Auskunftserteilung. Das BDSG kennt eine solche Bedingung allerdings nicht. Die Selbstauskunft an Betroffene ist deren unabdingbares Recht. Sie hat grundsätzlich von jeder Stelle, die Datenverarbeitung zu eigenen Geschäftszwecken betreibt, kostenlos und ohne weitere Voraussetzungen zu erfolgen. Auf meine Nachfrage bei dem Unternehmen stellte sich im vorliegenden Fall heraus, dass das Auskunftsersuchen den betrieblichen Datenschutzbeauftragten des Unternehmens nie erreicht hatte, sondern dass diese überraschende und grundfalsche Interpretation von § 34 Abs. 1 BDSG von einer neuen ungeschulten Mitarbeiterin im Kundenservice des Unternehmens stammte. Die Mitarbeiterin wurde entsprechend über die Rechtslage unterwiesen. Der Beschwerdeführer erhielt seine Selbstauskunft und die gewünschte Bestätigung der Sperrung seiner Daten (§ 35 Abs. 3 Nr. 2 BDSG).

Ein anderer Petent wies mich auf einen deutschsprachigen Zahlungsdienstleister hin, der nach der Gebührentabelle auf seiner Homepage für eine datenschutzrechtliche Selbstauskunft eine Gebühr von 10 EUR von anfragenden Bürgerinnen und Bürgern erhebt. Da die Konzernholding des englischen Unternehmens ihren Sitz in Hessen hat, habe ich dort unter Hinweis auf die gegenteilige Vorschrift des § 34 Abs. 8 BDSG nachgefragt, ob und wenn ja auf welcher Rechtsgrundlage eine Gebühr für die Inanspruchnahme eines grundlegenden Datenschutzrechts verlangt wird.

§ 34 Abs. 8 BDSG

Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen.

Die deutsche Konzernholding verwies in ihrer Antwort jedoch darauf, dass das BDSG in diesem Fall nicht gelte. Das deutsche Konzernunternehmen, das durchaus unter das BDSG falle, verarbeite selbst keine personenbezogenen Kundendaten. Dies geschehe ausschließlich durch ein Tochterunter-

nehmen mit Sitz in London, das auch als Telemedienanbieter im Impressum ihrer Homepage genannt werde.

Auf die Datenverarbeitung dieses englischen Unternehmens ohne Niederlassung im deutschen Inland ist gem. § 1 Abs. 5 Satz 1 BDSG nicht das deutsche, sondern das englische Datenschutzrecht anzuwenden. Nach Abschnitt 7 des englischen Data Protection Act 1998 ist es im Gegensatz zum deutschen Datenschutzrecht zulässig, von anfragenden Betroffenen eine Bearbeitungsgebühr von 10 EUR für datenschutzrechtliche Selbstauskünfte zu erheben.

4.8
Dauerwirkung von Interneteinträgen

Häufig werde ich um Hilfestellung bei der Beseitigung oder Berichtigung von via Internet veröffentlichten personenbezogenen Daten gebeten. Nicht immer gelingt das, wenn die Anbieter nicht die nach § 5 TMG vorgeschriebenen Angaben im Impressum machen. Manchen ist nicht bekannt, dass der Verstoß gegen die Impressumspflicht ein Bußgeldtatbestand ist.

Im Berichtsjahr erreichten mich viele Eingaben und Hilferufe Betroffener über die unerwünschte Online-Veröffentlichung ihrer persönlichen Daten auf privaten und gewerblichen Homepages, in Branchenbüchern, Online-Telefonbüchern und anderen Angeboten im Internet.

Dabei handelte es sich meist um die Angabe veralteter und falscher Anschriften, Telefonnummern und E-Mail-Adressen, um nicht gelöschte Alt-Einträge in Branchen- und Teilnehmerverzeichnissen entgegen § 104 TKG, aber auch um die Veröffentlichung von Bildern mit Namensnennung auf privaten Homepages oder die vergessene Schwärzung eines Namens in einem online veröffentlichten Gerichtsurteil. In allen Fällen waren die Anbieter der Inhalte von den Betroffenen nicht zu erreichen, pflegten ihr via Internet zur Verfügung gestelltes Angebot bereits lange nicht mehr oder reagierten einfach nicht auf deren Berichtigungs- oder Löschungsersuchen.

Bei der Bearbeitung der Eingaben stellte sich heraus, dass der Umgang von privaten und gewerblichen Anbietern mit ihren jeweiligen Angeboten sehr unterschiedlich ist. Während die meisten Anbieter ein korrektes Impressum mit allen Kontaktdaten und Angaben nach § 5 TMG (Anbieterkennzeichnung) führen und sich auch um die Aktualität und Korrektheit ihrer veröffentlichten personenbezogenen Inhalte bemühen, bin ich in den mir vorgelegten Beschwerdefällen immer wieder auf falsche Namen, gefälschte oder veraltete Anschriften sowie nicht funktionierende E-Mail-Adressen und Telefonnummern in den Anbieterkennzeichnungen gestoßen.

In einigen Fällen gelang es mir, die betroffenen Anbieter anhand der Domainregistrierungsdaten bei der DENIC e. G. oder durch eine Internetrecherche ausfindig zu machen und die Daten wie gewünscht löschen zu lassen. Diese Anbieter habe ich zudem alle darauf hingewiesen, dass bei einem Verstoß gegen die Pflicht zur Anbieterkennzeichnung ein Bußgeldverfahren gem. § 16 Abs. 2 Nr. 1 TMG von der hierfür zuständigen Hessischen Landesanstalt für privaten Rundfunk und neue Medien eingeleitet werden kann. Diese Information führte dann immer zu einer Aktualisierung der Angaben im dortigen Impressum. In anderen Fällen, wie z. B. bei drei polnischen Anbietern veralteter deutscher Telefonbuchdaten, konnte ich eine Berichtigung oder Löschung der Daten der Betroffenen online über die Homepages der Anbieter erreichen, die entsprechende Entfernungslinks anbieten und sich recht kooperativ zeigten.

Aber nicht immer war es mir möglich, in solchen Fällen weiterzuhelfen. Insbesondere bei Branchenbuch-Angeboten, die unter internationalen Top-Level-Domains (z. B. com, net, org oder info) ins Internet gestellt wurden und bei denen die Verantwortlichen das Angebot aus unbekannten Gründen seit langem nicht mehr betreuen und weder den Datenbestand pflegen noch ihre Kontaktdaten veröffentlichen, bin ich in einigen Einzelfällen auch an die Grenzen meiner Möglichkeiten gestoßen. Solche Angebote enthielten dann jeweils auch kein Impressum und die internationalen Domainregistrierungen erfolgten über außereuropäische Dienstleister, die auf Verschleierung der Anbieterangaben spezialisiert sind und ihren Kunden Anonymität zusichern.

4.9
Impressumspflicht bei Telemedien

Die Impressumspflicht bei Telemedien mit journalistisch-redaktionell gestalteten Inhalten beinhaltet nicht die Verpflichtung, Name und Anschrift von IT-Administratoren zu veröffentlichen.

In einer Beschwerde wandten sich IT-Administratoren dagegen, dass sie im Impressum einer Webseite als für die Redaktion Verantwortliche mit Namen und Kontaktdaten aufgelistet wurden. Das Impressum enthielt außerdem Angaben zum Verantwortlichen für den Inhalt und zum Verantwortlichen für die Technik. Die Administratoren gestalteten und pflegten nicht den Inhalt des Internetauftritts. Sie waren nicht mit redaktionellen Arbeiten betraut und hatten keinen eigenen Zugriff auf die Inhalte. Ihre Aufgabe bestand lediglich darin, die Inhalte an den Webhoster weiterzuleiten.

Webseitenbetreiber haben nach dem Telemediengesetz eine Reihe von Informationspflichten zu erfüllen. Dazu zählt, dass auf der Webseite Name

und Anschrift des Diensteanbieters sowie bei juristischen Personen die Vertretungsberechtigten genannt werden. Bei Webseiten (Telemedien) mit journalistisch-redaktionell gestalteten Inhalten muss zusätzlich ein dafür Verantwortlicher genannt werden. Werden mehrere Verantwortliche benannt, muss kenntlich gemacht werden, wer für welchen Teil des Dienstes verantwortlich ist.

§ 5 Abs. 1 TMG

Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten ...

§ 55 Abs. 2 RStV

Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten, in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, haben zusätzlich zu den Angaben nach den §§ 5 und 6 des Telemediengesetzes einen Verantwortlichen mit Angabe des Namens und der Anschrift zu benennen. Werden mehrere Verantwortliche benannt, so ist kenntlich zu machen, für welchen Teil des Dienstes der jeweils Benannte verantwortlich ist. ...

Die Regelung im Rundfunkstaatsvertrag ist den presserechtlichen Impressumsvorschriften nachgebildet (vgl. §§ 6 und 7 Hessisches Pressegesetz). Danach sind in Druckwerken Name und Anschrift des Verlegers und des verantwortlichen Redakteurs zu nennen. Der Impressumszwang dient in erster Linie dem Schutz des Persönlichkeitsrechts des von der Berichterstattung Betroffenen. Durch die Impressumspflicht erhält der Betroffene eine ladungs- und zustellungsfähige Anschrift, um sich zivilrechtlich durch Gegendarstellung und Klage auf Unterlassung, Widerruf oder Schadensersatz zur Wehr setzen zu können. Sie erleichtert außerdem den Strafverfolgungsbehörden die strafrechtliche Verfolgung von Pressedelikten.

In das Impressum sind die Personen aufzunehmen, die für die Veröffentlichung und den Inhalt der Veröffentlichung verantwortlich sind. Da die Administratoren nicht zur Leitung der Einrichtung zählten und auch keine redaktionelle Verantwortung trugen, sie lediglich die Inhalte an den Webhoster weiterzuleiten hatten, bestand telemedienrechtlich keine Notwendigkeit, ihre Kontaktdaten auf der Webseite zu veröffentlichen. Es existiert auch keine andere gesetzliche Grundlage, auf die sich unter den beschriebenen Voraussetzungen eine Veröffentlichung von Name und Anschrift der Administratoren auf der Internetseite stützen ließe. Die Veröffentlichung war daher unzulässig.

4.10
Informationsaustausch zwischen bürgender Bank und Bürgschaftsgläubiger

Eine im Rahmen eines Avalkreditvertrags bürgende Bank kann sich ohne Wissen des Hauptschuldners beim Bürgschaftsgläubiger erkundigen, ob die Bürgschaft noch benötigt wird.

Ein Bankkunde beschwerte sich darüber, dass sein Kreditinstitut, das für ihn im Rahmen eines Avalkredits eine Bürgschaft über eine halbe Millionen Euro übernommen hatte, ohne sein Wissen beim Bürgschaftsgläubiger nachgefragt hatte, ob die Bürgschaft noch benötigt werde. Die Bank hatte den Bürgschaftsgläubiger dabei aufgefordert, ihr für den Fall, dass die Bürgschaft sich erübrigt habe, die Bürgschaftsurkunde im Original zurückzugeben. Der Beschwerdeführer behauptete, ihm sei durch das Vorgehen der Bank ein erheblicher Schaden entstanden.

Die Zulässigkeit der Anfrage der Bank bei dem Bürgschaftsgläubiger richtet sich nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

> *§ 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, ...*

Demzufolge müsste die Anfrage für die Durchführung oder Beendigung des Bürgschaftsvertrages erforderlich gewesen sein. Zwischen Bank und Bürgschaftsgläubiger müsste ein Bürgschaftsvertrag abgeschlossen worden sein. Bei einem Avalkredit bestehen Rechtsbeziehungen zwischen drei Parteien: dem Bankkunden als Hauptschuldner, der Bank als Bürge und dem Gläubiger des Bankkunden als Bürgschaftsgläubiger. Im Avalkreditvertrag verbürgt sich eine Bank für die Verbindlichkeit eines Kunden gegenüber einem Dritten. Es handelt sich um einen entgeltlichen Geschäftsbesorgungsvertrag zwischen der Bank und ihrem Kunden, durch den die Bank es gegen Zahlung einer Avalprovision übernimmt, sich zugunsten des Kunden gegenüber dessen Gläubiger zu verbürgen (§ 675 Abs. 1 BGB). Dieser Vertrag begründet Verpflichtungen lediglich zwischen der Bank und ihrem Kunden, nicht aber zugunsten des Dritten, dem gegenüber die Bank sich verbürgen soll. Ein Bürgschaftsverhältnis zwischen Bank und Gläubiger entsteht erst, wenn in Ausführung des Avalkreditvertrages zwischen Bank und Gläubiger ein Bürgschaftsvertrag (§ 765 BGB)

geschlossen wird. Die Überprüfung ergab, dass zwischen dem Kreditinstitut und dem Bürgschaftsgläubiger ein solcher Bürgschaftsvertrag geschlossen worden war.

Für die Durchführung oder Beendigung des Bürgschaftsvertrages muss die Bank wissen, ob der Avalzweck weiterbesteht oder erledigt ist. Die für den Fall der Erledigung von der Bank gewünschte bedingungslose Rückgabe der Bürgschaftsurkunde im Original wäre eine konkludente Erklärung der Bürgschaftsgläubigerin, dass sie keine Ansprüche aus dem Avalkredit mehr geltend macht. Da es sich hier um ein Rechtsverhältnis zwischen Bank und Bürgschaftsgläubiger handelt, besteht datenschutzrechtlich keine Verpflichtung des Kreditinstituts, den Bankkunden zu informieren. Das Verhalten des Kreditinstituts war daher datenschutzrechtlich korrekt.

4.11
Auskunfteien

Das Bundesdatenschutzgesetz enthält spezielle Vorschriften für die Datenverarbeitung durch Auskunfteien. Die Übermittlung an Auskunfteien ist seit dem 1. April 2010 neu geregelt. Der Gesetzgeber hat den Interessen der Auskunfteien und deren Kunden gegenüber den Interessen der Betroffenen den Vorrang eingeräumt, die Datenverarbeitung aber an spezifische Voraussetzungen geknüpft. Die Rechte der Betroffenen auf Berichtigung, Löschung oder Sperrung von Daten müssen gewahrt werden.

Im Bereich der Auskunfteien ist die Zahl der Eingaben besonders hoch. Ursächlich ist vielfach Unkenntnis der Rechtslage.

Mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2010 wurden mit den §§ 28a und 28b BDSG zwei neue Vorschriften geschaffen, welche sich ausschließlich an Auskunfteien wenden. Während § 28a BDSG die Datenübermittlung an Auskunfteien regelt, werden in § 28b BDSG die Voraussetzungen für das sog. „Scoring“ normiert. Dabei handelt es sich um ein analytisch-statistisches Verfahren, welches benutzt wird, um aus erhobenen Daten anhand von Erfahrungswerten zu Risikoeinschätzungen zu kommen. Das Scoring ist für die Betroffenen oft nicht transparent. Über diese Problematik werde ich im nächsten Tätigkeitsbericht berichten.

Die folgenden Ausführungen dienen dazu, Betroffenen die Rechtslage und Voraussetzungen für die Datenverarbeitungen von Auskunfteien zu erläutern. Wesentliche Grundlage hierfür ist der neue § 28a BDSG.

§ 28a BDSG

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. *die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,*
2. *die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,*
3. *der Betroffene die Forderung ausdrücklich anerkannt hat,*
4. *a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,*
   b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,
   c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und
   d) der Betroffene die Forderung nicht bestritten hat oder
5. *das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.*

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

4.11.1
Was ist eine Auskunftei?

In der Begründung zur BDSG-Novelle wird der Begriff der Auskunftei wie folgt definiert: „Unter Auskunftei ist grundsätzlich ein Unternehmen zu verstehen, das unabhängig vom Vorliegen einer konkreten Anfrage geschäfts-

mäßig bonitätsrelevante Daten über Unternehmen oder Privatpersonen sammelt, um sie bei Bedarf seinen Geschäftspartnern für die Beurteilung der Kreditwürdigkeit des Betroffenen gegen Entgelt zugänglich zu machen“ (BTDrucks. 16/10529, S. 9).

Die für die Kreditwirtschaft wohl bekannteste und größte Organisation ist die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung). Darüber hinaus gibt es eine Reihe weiterer Unternehmen, die ihren Kunden Bonitätsangaben zu Privatpersonen, aber auch zu Unternehmen zur Verfügung stellen. Die Tatsache, dass die SCHUFA, einige Creditreform KGs und weitere kleinere Auskunfteien ihren Sitz in Hessen haben, erklärt das hohe Eingabevolumen auf diesem Gebiet.

4.11.2
Welche personenbezogenen Daten dürfen Auskunfteien erheben?

Auskunfteien beziehen im Wesentlichen zwei Arten von Informationen: Zum einen sind dies sog. Negativdaten, also alle Angaben zu nicht vertragsgemäßem Verhalten des Kunden (z. B. Forderungen nach Kündigung eines Vertrags oder Daten aus öffentlichen Schuldnerverzeichnissen). Von Interesse für die Auskunftei sind aber auch weitere Kundeninformationen, etwa die Anzahl der abgeschlossenen Mobilfunkverträge, das Bestehen eines Girokontos oder die ordnungsgemäße Rückzahlung eines Ratenkreditvertrages.

4.11.3
Fallkonstellationen für die Erhebung, Speicherung und Übermittlung durch die Auskunftei

Das BDSG beschreibt in § 29 die Voraussetzungen für die Erhebung und Speicherung personenbezogener Daten u. a. durch Auskunfteien sowie der Datenübermittlung an Dritte.

§ 29 BDSG

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. *kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,*
2. *die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder*

3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Abs. 1 Satz 2 und Abs. 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

(6) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(7) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 6a bleibt unberührt.

Die Erhebung, Speicherung und Übermittlung personenbezogener Daten an Dritte ist demnach zulässig, wenn

– kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung hat.

  Gegen die Speicherung und Übermittlung des Umstands, dass eine gerichtlich bestätigte Forderung durch Maßnahmen der Zwangsvollstreckung eingetrieben werden musste, kann der Schuldner kein schützenswertes Interesse ins Feld führen. Denn dies gehört nicht mehr in den Bereich eines „normalen Schuldnerverhaltens“. Dagegen gibt es keinen

Grund für die Erhebung und Übermittlung von personenbezogenen Daten über Schuldner, die ihre Forderung bereits ordnungsgemäß beglichen haben. Deren schutzwürdiges Interesse steht einer solchen Datenverarbeitung entgegen.

– die Daten aus allgemein zugänglichen Quellen entnommen werden können.

  Dies sind z. B. öffentliche Register, zu denen der Zugang jedermann ohne besondere Voraussetzungen offen steht wie z. B. Handelsregister, Genossenschaftsregister, Vereinsregister. Auch die Nutzung von Medien (Radio, Fernsehen, Druckerzeugnisse) fällt hierunter.

– einer der gesetzlich abschließend aufgezählten Erlaubnistatbestände zur Datenübermittlung an Auskunfteien nach § 28a Abs. 1 oder Abs. 2 BDSG vorliegt.

  Das ist z. B. der Fall, wenn die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil oder das Vorliegen eines Schuldtitels nach der Insolvenzordnung festgestellt und vom Schuldner nicht bestritten wurde oder wenn der Betroffene die Forderung ausdrücklich anerkannt hat. Zulässig ist die Übermittlung von Daten zu einer Forderung auch, wenn der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist, zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen, die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung unterrichtet hat und der Betroffenen die Forderung nicht bestritten hat. Kreditinstitute dürfen personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft an Auskunfteien übermitteln.

Bis zum 1. April 2010 lag der Datenerhebung bei Auskunfteien häufig eine Einwilligung des Betroffenen zugrunde. Am bekanntesten ist hier die „SCHUFA-Klausel“, die bei der Eröffnung eines Girokontos oder dem Abschluss eines Handyvertrages zu unterschreiben war.

Ob diese Unterschrift immer freiwillig erfolgte, war umstritten, denn in der Regel hatte der Betroffene keine Wahl, wenn er den Vertrag abschließen wollte. Die beschriebene Praxis war rechtlich also nicht unproblematisch. Da es jedoch unbestritten ebenfalls ein Bedürfnis etwa einer Bank gibt, vor Abschluss eines Darlehensvertrages die Bonität des Kunden zu überprüfen, hat der Gesetzgeber für diese Form der Datenerhebung und -verarbeitung mit der Vorschrift des § 28 Abs. 2 BDSG eine gesetzliche Grundlage geschaffen.

§ 28 Abs. 1 und 2 BDSG

(1) 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.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. *unter den Voraussetzungen des Abs. 1 Satz 1 Nummer 2 oder Nummer 3,*
2. *soweit es erforderlich ist,*
   a) zur Wahrung berechtigter Interessen eines Dritten oder
   b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. *...*

Kreditinstitute und andere Unternehmen dürfen daher auch Angaben zu mit ihnen bestehenden Verträgen und deren Abwicklung und zu Krediten an Auskunfteien übermitteln.

4.11.4.
Daten dürfen nicht unbegrenzt bei einer Auskunftei gespeichert werden

Die bei den Auskunfteien wie z. B. der SCHUFA gespeicherten Daten werden nach Ablauf bestimmter Fristen gelöscht. Diese ergeben sich aus der Vorschrift des § 35 BDSG.

§ 35 BDSG

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(2) Personenbezogene Daten können außer in den Fällen des Abs. 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. *ihre Speicherung unzulässig ist,*
2. *es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit,*

Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,

3. *sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder*
4. *sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine länger währende Speicherung nicht erforderlich ist.*

Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. *im Fall des Abs. 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,*
2. *Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder*
3. *eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.*

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(4a) Die Tatsache der Sperrung darf nicht übermittelt werden.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zweck der Übermittlung außer in den Fällen des Abs. 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. *es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und*
2. *die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.*

Kreditverpflichtungen bleiben beispielsweise bis zur vollständigen Rückzahlung im Datenbestand. Danach werden sie als erledigte Kredite für weitere drei Jahre gespeichert und anschließend gelöscht. Dies ist zulässig, da eine ordnungsgemäße Rückzahlung eines Kredites anderen Unternehmen die Zahlungswilligkeit und Zahlungsfähigkeit des Kunden vermittelt und damit für den Kunden vorteilhaft ist.

Die Daten hinsichtlich einer nicht vertragsgemäßen Abwicklung werden am Ende des dritten Kalenderjahres nach dem Jahr gelöscht, in dem die Erledigung stattgefunden hat. Haben sich diese Daten vor Ablauf dieser Löschungsfrist erledigt, z. B. weil der Kunde nach Zwangsmaßnahmen eine offene Forderung beglichen hat, so wird dies bei der SCHUFA vermerkt. Eine vorzeitige Löschung findet allerdings nicht statt, da das Interesse anderer Kredit gewährender Unternehmen an der Information, dass ein potentieller Kunde sich bereits einmal vertragswidrig verhalten hat, höher zu bewerten ist als das Interesse des Betroffenen daran, dass diesen Umstand niemand erfährt.

Die Speicherfrist führt allerdings auch zur dreijährigen Speicherung erteilter Restschuldbefreiungen nach Durchführung von Verbraucherinsolvenzverfahren.

4.11.5
Anspruch auf Löschung oder Korrektur der gespeicherten Daten

Sofern die Auskunftei unkorrekte Angaben zum Betroffenen gespeichert hat, ergibt sich ein Anspruch auf deren Berichtigung nach § 35 Abs. 1 BDSG. Zu löschen sind personenbezogene Daten dann,

- wenn ihre Speicherung unzulässig ist,
- es sich um besonders sensible Daten z. B. über die Gesundheit oder rassische Herkunft handelt, deren Richtigkeit durch die speichernde Stelle nicht bewiesen werden kann,
- die Speicherung nicht mehr erforderlich ist, weil ihre Kenntnis zur Zweckerfüllung nicht mehr erforderlich ist oder
- die Daten geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung ergibt, dass eine länger währende Speicherung nicht erforderlich ist.

An die Stelle einer Löschung kann bei bestimmten Fallkonstellationen auch eine Sperrung treten. Die Voraussetzungen hierfür ergeben sich aus § 35 Abs. 3 BDSG.

4.11.6
Praktische Probleme

Im Geschäftsleben eines Verbrauchers kommt es zu einer Vielzahl von Datenübermittlungen und Datenanfragen an bzw. bei Auskunfteien. Ob Kleinkredit, Handyvertrag oder Bestellung beim Versandhandel: Stets werden Daten in den persönlichen Datenbestand des Betroffenen bei einer Auskunftei eingepflegt bzw. die dort gespeicherten Daten an Dritte übermittelt. Das entspricht dem Geschäftszweck einer Auskunftei. Dies ist dann unproblematisch, wenn es sich nicht um Negativdaten handelt. Die Einmeldung von Negativdaten, also vertragswidriges Verhalten, weil der Kredit nicht zurückgezahlt oder die Rechung des Versandhändlers nicht beglichen wurde, führt in der Regel für den Betroffenen auf die Zukunft gerichtet zu erheblichen Problemen. Künftige Geschäftspartner, Banken u. a. werden in der Regel von avisierten Geschäften in Kenntnis der Negativdaten Abstand nehmen.

Dabei muss der oder die Betroffene selbst noch nicht einmal schuldhaft gehandelt haben. Die Verwechslung von Personen im Rahmen der Einmeldung oder die Übermittlung unzutreffender Informationen an die Auskunftei kommt immer wieder vor. In diesen Fällen wie auch bei schuldhaftem Handeln ist es für Betroffene schwer, diese Informationen wieder aus dem Datenbestand löschen zu lassen, weil ihnen die Beweislast aufgebürdet ist. Aus diesem Grund ist es erforderlich, eine Einmeldung möglichst zu vermeiden. Auf Mahnbriefe eines Gläubigers sollte deshalb unmittelbar reagiert werden. Gegebenfalls ist der Forderung schriftlich zu widersprechen. Ist die Speicherung erfolgt, muss die Auskunftei veranlasst werden, sich mit der einmeldenden Stelle in Verbindung zu setzen, um den Sachverhalt zu klären und ggf. eine Löschung der Daten vorzunehmen, sofern die Voraussetzungen für die Einmeldung nicht vorgelegen haben.

Ferner müssen die Voraussetzungen des § 28a BDSG für die Einmeldung vorgelegen haben. Die Entscheidung bzw. die Prüfung, ob dem so ist, trifft der Vertragspartner der Auskunftei. Er ist damit für die Zulässigkeit der Datenübermittlung verantwortlich. Die Auskunftei als speichernde Stelle bleibt für die Richtigkeit der von ihr vorgehaltenen Daten verantwortlich, weil deren Speicherung bzw. die Erhebung für eigene Zwecke an die Bedingungen des § 29 Abs. 1 Nr. 1 bis 3 BDSG geknüpft sind.

4.12
Datenschutzgerechte Ausgestaltung von Arztbewertungsportalen

Der bundesweit zunehmende Betrieb von Arztbewertungsportalen ist insbesondere von Ärzten kritisch diskutiert worden und war Anlass für Be-

schwerden bei meiner Dienststelle und anderen Datenschutzbeauftragten. Die für die Betreiber dieser Portale zuständigen Datenschutzaufsichtsbehörden haben sich 2012 auf eine gemeinsame Vorgehensweise zur Klärung und Bewertung der von den Portalen getroffenen Maßnahmen zur Gewährleistung des Persönlichkeitsschutzes der Ärzte verständigt und mit der Versendung eines Fragebogens zur aktuellen Verfahrensweise begonnen.

4.12.1
Einleitung

Öffentlich zugängliche Bewertungen von Waren und Dienstleistungen wie z. B. von Büchern, Restaurants und Hotels gibt es schon seit langer Zeit. Relativ neu ist jedoch der Aufbau von Portalen im Internet, in denen persönliche Urteile über Personen und ihre beruflichen Leistungen abgegeben werden, die dann von einem großen Benutzerkreis oder auch weltweit abgerufen werden können. Derartige Portale gibt es inzwischen in vielen Lebensbereichen, auch im Gesundheitsbereich.

In Deutschland gibt es bereits mehr als 15 Arztbewertungsportale. Die Reaktionen darauf sind unterschiedlich:

- Einerseits werden sie kritisiert als „digitaler Ärztepranger“, der dem im Internet anonym bewerteten Arzt keine angemessene Möglichkeit gibt, auf Kritik zu reagieren. Hingewiesen wird dabei insbesondere auf die häufig geringe und damit nicht aussagefähige Anzahl von Bewertungen pro Arzt, nicht nachvollziehbare Bewertungskriterien und die Schwierigkeit, Mehrfachbewertungen durch einen Nutzer und anderen Missbrauch der Bewertungsmöglichkeiten zu verhindern; ferner wird auch die Objektivität und Kompetenz der Patienten zur Bewertung von Ärzten in Frage gestellt.
- Andererseits werden die Portale begrüßt als wertvolles Instrument zur Herstellung von Transparenz für Patienten, das weiterentwickelt werden muss. Gerade im Gesundheitsbereich wird das Bedürfnis gesehen, die Informationsasymmetrie zwischen Leistungserbringern und Patienten bzw. Versicherten auszugleichen, Leistungen vergleichbar zu machen und die Qualität der Leistungen auf diesem Wege zu steigern. So können sich Versicherte z. B. bereits bei den Krankenkassen vergleichend über Qualitätsmerkmale der Krankenhäuser informieren. Auch der sog. Pflege-TÜV, bei dem der Medizinische Dienst der Krankenkassen die ambulanten und stationären Pflegeeinrichtungen bewertet und die Ergebnisse veröffentlicht, soll den Versicherten helfen, sich über die Qualität von Leistungen zu informieren. Im Bereich der niedergelassenen

Ärzte wird ebenfalls ein Bedarf der Patienten hinsichtlich Transparenz und Vergleichbarkeit von Leistungen gesehen.

Vor dem Hintergrund der derzeitigen Defizite der Portale haben die Bundesärztekammer und die Kassenärztliche Bundesvereinigung bereits allgemeine Qualitätskriterien für Arztbewertungsportale formuliert (www.arztbewertungsportale.de). Für die Datenschutzaufsichtsbehörden ist die datenschutzgerechte Ausgestaltung der Portale der zentrale Aspekt. Die für Betreiber von privaten, kommerziellen Arztbewertungsportalen zuständigen Datenschutzaufsichtsbehörden – zu denen auch meine Dienststelle wegen des in Hessen betriebenen Portals www.sanego.de zählt – haben sich 2012 auf eine gemeinsame Vorgehensweise zur Klärung und Bewertung der von den Portalen getroffenen Maßnahmen zur Gewährleistung des Persönlichkeitsschutzes der Ärzte verständigt.

4.12.2
Ausgangspunkt: Die rechtlichen Rahmenbedingungen für Bewertungsportale

Die Veröffentlichung von Bewertungen der beruflichen Leistungen von Personen stellt eine Verarbeitung personenbezogener Daten im Sinne von § 3 Abs. 4 BDSG dar. Die Betreiber kommerzieller Portale müssen die Vorschriften der §§ 27 ff. BDSG beachten. Die rechtlichen Anforderungen sind in den letzten Jahren durch die Rechtsprechung konkretisiert worden. Die Rechtsprechung hat den Nutzern und Betreibern von Bewertungsportalen dabei recht weite Spielräume eröffnet. Von zentraler Bedeutung für alle Portale ist das Urteil des BGH von 2009 zu dem Lehrerbewertungsportal Spick-mich.de (NJW 2009, 2888). Prüfungsmaßstab ist in dem Urteil § 29 BDSG, der das „geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung“ regelt. Der BGH kommt zu folgendem Ergebnis:

- Die Erhebung und Nutzung von Namen, Schule sowie unterrichteten Fächern der Lehrer im Portal ist zulässig, weil diese Informationen aus allgemein zugänglichen Quellen (Homepage der Schulen) abgerufen werden können.
- Die Speicherung von Bewertungen im Portal ist zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat.
- Die Übermittlung von Daten an Dritte ist nach dem Wortlaut des § 29 BDSG zulässig, wenn der Dritte ein berechtigtes Interesse an ihrer

Kenntnisnahme glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Da bei einem Abruf von Bewertungen im Internet das Vorliegen eines berechtigten Interesses des Dritten jedoch faktisch nicht geprüft werden kann, wäre es dem BGH zufolge ein Verstoß gegen die grundrechtliche Kommunikationsfreiheit, wenn ein Abruf nur unter der Voraussetzung vorgenommen werden könnte, dass der einzelne Interessent sein berechtigtes Interesse glaubhaft dargelegt hat. Die Übermittlung von Bewertungen an die Nutzer des Portals ist daher stets schon dann als zulässig zu bewerten, wenn kein schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Übermittlung besteht. Im Einzelfall ist eine Abwägung vorzunehmen zwischen den Interessen des Bewerteten einerseits und den Interessen der Nutzer des Portals andererseits. Zu unterscheiden ist dabei zwischen Bewertungen in der Form von Meinungsäußerungen, die bis zur Grenze einer sog. „Schmähkritik" (d. h. unsachlicher Kritik, deren Ziel die Diffamierung des Betroffenen ist) zulässig sind und Tatsachenbehauptungen, die grundsätzlich überprüfbar sind und der Wahrheit entsprechen müssen.

In dem vom BGH entschiedenen Fall konnte aus bestimmten Merkmalen des Lehrerbewertungsportals gefolgert werden, dass kein Interesse des Lehrers an einem Ausschluss der Übermittlung vorliegt, insbesondere weil die Portalbetreiber einer diffamierenden Herabsetzung in gewissem Maße vorbeugen durch

- die Vorgabe von Bewertungskriterien,
- die Möglichkeit von Missbrauchsmeldungen an das Portal,
- die Beschränkung des Zugriffs auf Angehörige der jeweiligen Schule und
- die auf 1 Jahr begrenzte Dauer der Speicherung jeder Bewertung.

4.12.3
Besonderheiten von Arztbewertungsportalen

Die grundsätzlichen Aussagen des BGH im Spickmich-Urteil sind auch für Arztbewertungsportale von Bedeutung:

- Die Erhebung und Nutzung von Namen, Adresse und Tätigkeitsbereich eines Arztes ist danach zulässig, wenn diese Informationen aus allgemein zugänglichen Quellen (Gelbe Seiten, Homepage der Kassenärztlichen Vereinigungen etc.) abgerufen werden können.
- Die Speicherung und Übermittlung von Bewertungen ist zulässig, wenn der betroffene Arzt kein schutzwürdiges Interesse an dem Ausschluss von Speicherung und Übermittlung der Bewertungen an die Nutzer hat.

Allerdings unterscheiden sich Bewertungen in Arztbewertungsportalen in einer Reihe von Aspekten von Bewertungen in dem vom BGH betrachteten Lehrerbewertungsportal:

- Beim Lehrerbewertungsportal wird durch die Registrierung der Nutzer der Zugriff auf Informationen über eine Lehrkraft einer bestimmten Schule beschränkt, die Registrierung setzt die Kenntnis der Schule voraus und Mehrfachbewertungen unter derselben E-Mail-Adresse sind nicht möglich. Dieser Aspekt wurde vom BGH im Spickmich-Urteil hervorgehoben. Allerdings kann auch beim Lehrerbewertungsportal wohl kaum ausgeschlossen werden, dass schulfremde Personen das Registrierungsverfahren gezielt nutzen, um eine Lehrkraft – u. U. sogar mehrfach unter Verwendung verschiedener E-Mail-Adressen – negativ zu beurteilen und ihr damit zu schaden. Bei Arztportalen sind Bewertungen im Internet ohne Beschränkungen zugänglich und in der Regel auch über Suchmaschinen aufrufbar.
- Die Bewertungskriterien sind sehr unterschiedlich und hinsichtlich der Ärzte auch komplexer.
- Für Ärzte kann es wegen der von ihnen einzuhaltenden ärztlichen Schweigepflicht schwierig sein, sich gegen Vorwürfe und Kritik zu wehren.

Ob und unter welchen Voraussetzungen ein schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Speicherung und Übermittlung von Bewertungen vorliegen kann, bedarf daher einer spezifischen Konkretisierung für die Arztbewertungsportale. Als ersten Schritt haben die Datenschutzaufsichtsbehörden einen Fragebogen zur konkreten Ausgestaltung des Bewertungsverfahrens und zu den realisierten Schutzmaßnahmen für die betroffenen Ärzte entwickelt und an die Portale versandt.

4.12.4
Fragebogen der Datenschutzaufsichtsbehörden

Der Fragebogen enthält Fragen zu folgenden Aspekten:

- Erfordernis der Registrierung von Bewertern

  Eine Registrierung kann Nutzer möglicherweise davon abhalten, gezielt Schmähkritik bzw. unwahre Tatsachenbehauptungen zu verbreiten. Zudem kann im Rahmen des Registrierungsprozesses auf Nutzungsbedingungen hingewiesen und die Bestätigung der Kenntnisnahme der Nutzungsbedingungen verlangt werden. Wenn allerdings jemand gezielt anonym beleidigende oder falsche Bewertungen abgeben will, kann er dies mit einem verhältnismäßigen Aufwand dennoch erreichen, sodass ein Registrierungsverfahren nur ein begrenzter Schutz für die Bewerteten sein kann.

- allgemeines Bewertungsverfahren
- im Portal vorgesehene Bewertungskriterien
- Möglichkeit von Freitexteintragungen im Portal und vor Veröffentlichung vorgesehene Überprüfung der Zulässigkeit

  Freitextfelder ermöglichen eine auf den Einzelfall bezogene spezifische und differenzierte Bewertung, die für andere Nutzer unter Umständen informativer sein kann als Angaben zu abschließend vorgegebenen Bewertungskriterien. Allerdings ist bei Freitextfeldern die Gefahr von Schmähkritik und unwahren Tatsachenbehauptungen deutlich größer als bei abschließend vorgegebenen Bewertungskriterien. Die optimale Datenschutzlösung bei Freitextfeldern wäre eine redaktionelle Moderation aller Bewertungen **vor** der Veröffentlichung. Ein Beschwerdeverfahren – auch wenn es gut organisiert ist – kann die berechtigten Interessen der Betroffenen nicht immer umfassend schützen. Es setzt voraus, dass der Bewertete selbst oder andere Nutzer zeitnah nach der Veröffentlichung der Bewertung dem Portal einen Missbrauch anzeigen, die betreffende Bewertung dann während der Überprüfung der Zulässigkeit der Bewertung durch das Portal nicht mehr angezeigt wird und beleidigende oder unwahre Äußerungen vom Portal gelöscht werden. Selbst wenn diese Voraussetzungen im Einzelfall gegeben sind, bleibt das Problem, dass die unzulässige Bewertung vermutlich bereits in gewissem Umfang verbreitet wurde und auch nach Herausnahme durch das Portal noch eine Weile z. B. im Google-Cache abrufbar ist. Der Bewertete muss selbst gegenüber Google aktiv werden, um eine zeitnahe Löschung der Bewertung zu erreichen. Allerdings würde eine redaktionelle Moderation aller Freitext-Bewertungen **vor** Veröffentlichung für die Portalbetreiber sehr erhebliche personelle und finanzielle Anforderungen bedeuten und wohl nach derzeitiger Lage die Aktualität der Portale in Frage stellen. Die Rechtsprechung hat entsprechende Anforderungen bisher nicht formuliert. Umso wichtiger werden dann anderweitige Schutzmaßnahmen für die betroffenen Ärzte (s. u.).
- Transparenz für die Nutzer hinsichtlich der Anzahl der abgegebenen Bewertungen und des Zeitpunkts der Abgabe der Bewertungen
- Erfordernis einer Mindestanzahl von Bewertungen vor Veröffentlichung von Bewertungen zu dem betroffenen Arzt
- Maßnahmen zur Verhinderung von Mehrfachbewertungen durch einen Nutzer innerhalb einer bestimmten Zeitspanne
- Maßnahmen des Portals zum Schutz der Ärzte gegen Schmähkritik und unwahre Tatsachenbehauptungen

– Anzeige von vorhandenen Bewertungen zu einem Arzt im Internet auch dann, wenn vom Internetnutzer nicht gezielt nach Bewertungen gesucht wird, sondern z. B. nach der Adresse des Arztes.
– Information des Arztes über neue Bewertungen und Gelegenheit zur Stellungnahme/Gegendarstellung/Kommentierung
– Dauer der Speicherung von einer Bewertung.

Nach Auswertung der Fragebögen wird meine Dienststelle zusammen mit den anderen Aufsichtsbehörden die datenschutzrechtlich gebotenen wie auch evtl. darüber hinausgehenden wünschenswerten Maßnahmen zum Schutz der bewerteten Ärzte im Dialog mit den Portalbetreibern weiter erörtern. Ziel ist eine angemessene Balance zwischen der Meinungs- und Informationsfreiheit einerseits und dem Schutz der Ärzte vor Existenz gefährdender Rufschädigung andererseits.

4.13
Bestellung von Datenschutzbeauftragten für Arztpraxen

Arztpraxen müssen einen Datenschutzbeauftragten erst dann bestellen, wenn sie mehr als neun Personen mit der Verarbeitung personenbezogener Daten beschäftigen. Im Regelfall müssen sie keine Vorabkontrolle für ihre automatisierten Verarbeitungen durchführen. Unabhängig davon haben sie aber sicherzustellen, dass die ärztliche Schweigepflicht und die weiteren rechtlichen und technischen Vorgaben für die Verarbeitung von Patientendaten eingehalten werden.

Im Berichtszeitraum habe ich eine Reihe von Anfragen insbesondere von Arztpraxen, externen Datenschutzbeauftragten und Schulungsveranstaltern erhalten bezüglich einer Verpflichtung von Arztpraxen, eine Vorabkontrolle von automatisierten Verarbeitungen durchzuführen und einen Datenschutzbeauftragten zu bestellen. Die Interpretation verschiedener Vorschriften, die bei diesem Thema zu berücksichtigen sind, hat zu Unsicherheiten geführt.

Das BDSG regelt in § 4f, wann von nicht-öffentlichen Stellen – also auch von einer Arztpraxis – ein Datenschutzbeauftragter zu bestellen ist. Gemäß Abs. 1 muss die Arztpraxis spätestens einen Monat nach Aufnahme ihrer Tätigkeit einen Datenschutzbeauftragter schriftlich bestellen, wenn sie

– in der Regel (d. h. nicht nur ausnahmsweise)
– mehr als neun Personen (gemeint ist hier die Kopfzahl)
– ständig mit der automatisierten Verarbeitung (d. h. mit der Verarbeitung von Daten im elektronischen Praxissystem, der strukturierten Patientenkartei oder in medizinischen Geräten, die Patientendaten speichern)

– personenbezogener Daten (d. h. Angaben zu bestimmten oder bestimmbaren Personen)

beschäftigt.

Unsicherheiten bezüglich der Verpflichtungen kleinerer Arztpraxen haben sich ergeben, weil Abs. 1 darüber hinaus Folgendes festlegt:

§ 4f Abs. 1 BDSG

Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

Wann eine Vorabkontrolle durchzuführen ist, regelt § 4d Abs. 5 BDSG.

§ 4d Abs. 5 BDSG

Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn
1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. ...
es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Da eine Arztpraxis Gesundheitsdaten und damit besondere Arten personenbezogener Daten i. S. v. § 3 Abs. 9 BDSG verarbeitet, besteht damit grundsätzlich die Verpflichtung, eine Vorabkontrolle durchzuführen, es sei denn, die in der Vorschrift genannten Ausnahmen liegen vor. Diese Ausnahmen werden aber in der Regel in einer Arztpraxis bei der routinemäßigen Verarbeitung von Patientendaten vorliegen; so werden z. B.

– personenbezogene Patientendaten zur Abrechnung an die gesetzlichen Krankenkassen nach den Vorschriften des SGB V (d. h. aufgrund gesetzlicher Verpflichtung) übermittelt,
– personenbezogene Patientendaten an vor-, mit- oder nachbehandelnde Ärzte mit Einwilligung des Patienten übermittelt und – vor allem –
– personenbezogene Patientendaten für die Durchführung des Behandlungsvertrages in der Arztpraxis verarbeitet.

Eine Vorabkontrolle muss daher im Regelfall von einer Arztpraxis nicht durchgeführt werden, und die Bestellung eines Datenschutzbeauftragten ist erst dann geboten, wenn die Arztpraxis mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

Soweit ein Datenschutzbeauftragter zu bestellen ist, sind seine Aufgaben (Beratung der Praxisleitung, Kontrolle der Einhaltung des Datenschutzes, Schulung von Mitarbeitern etc.) und auch seine organisatorische Stellung (insbesondere die Unabhängigkeit bei der Ausübung seiner Aufgaben) schriftlich zu konkretisieren. Damit keine Interessenkonflikte auftreten, sollte insbesondere keine Personalunion mit der Praxis-, IT- oder Personal-Leitung bestehen.

Unabhängig von der Verpflichtung zur Bestellung eines Datenschutzbeauftragten und zur Durchführung einer Vorabkontrolle im Einzelfall ist jede Arztpraxis verpflichtet, die Einhaltung der ärztlichen Schweigepflicht und der weiteren rechtlichen und technischen Vorgaben bei der Verarbeitung von Patientendaten sicherzustellen (zu Einzelheiten siehe die Empfehlungen der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, http://www.bundesaerztekammer.de/page.asp?his=0.7.47.6188).

4.14
Hinweis- und Informationssystem der Versicherungswirtschaft (HIS)

Die Auskunftei HIS ist das Ergebnis einer Abstimmung des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. mit den Datenschutzaufsichtsbehörden. Zweck dieser Auskunftei ist, Versicherungsbetrug zu bekämpfen und die Risikoprüfung effizient zu gestalten.

4.14.1
Der Anlass

Ein Bürger beschwerte sich mit seiner Eingabe darüber, dass eine Versicherung seinen Pkw betreffende Daten an die Informa Risk + Fraud Prevention GmbH in Baden-Baden übermittelt hatte, die die Auskunftei HIS betreibt. Konkret ging es um die Meldung eines Totalschadens an dem Pkw. Der Eingeber kritisierte, dass er in eine Übermittlung seiner Pkw-Daten an das HIS nicht eingewilligt habe und daher ein Datenschutzverstoß vorliege.

4.14.2
Zulässigkeit der Einmeldung in das HIS

Der Hinweis des Eingebers, die Einmeldung in das HIS beruhe nicht auf seiner Einwilligung, ist zutreffend. Darin liegt allerdings kein Rechtsverstoß.

Eine Datenübermittlung ist nämlich nicht nur dann zulässig, wenn sie sich auf eine Einwilligung stützen kann (§§ 4, 4a BDSG). Rechtsgrundlage kann

auch eine gesetzliche Befugnisnorm sein, in vorliegendem Kontext § 28 Abs. 1 Nr. 2 BDSG.

§ 28 Abs. 1 Nr. 2 BDSG

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

…

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, …

Vor diesem rechtlichen Hintergrund ist zwischen dem Gesamtverband der Deutschen Versicherungswirtschaft e. V. in Berlin (GDV) und den Datenschutzaufsichtsbehörden abgestimmt worden, dass Versicherungsunternehmen bei Vorliegen bestimmter Einmeldekriterien Daten an den Betreiber des HIS zu melden befugt sind. Diese Konstellation liegt dann vor, wenn es um erhöhte Risiken geht oder Auffälligkeiten, die auf Versicherungsmissbrauch hindeuten könnten. In das HIS melden Versicherungen unter anderem Auffälligkeiten aus Versicherungsfällen und personenbezogene Informationen zu Risikoprüfungen im Antragsbereich. Vor einer Einmeldung von personenbezogenen Daten sind die Interessen der Versicherungsbranche und der Betroffenen abzuwägen. Bei Vorliegen der festgelegten Meldekriterien ist allerdings regelmäßig von einem überwiegend berechtigten Interesse des Unternehmens an der Einmeldung auszugehen. Beispielsweise wird bei Kraftfahrzeugen dann in das HIS eingemeldet, wenn ein Totaldiebstahl, Totalschaden oder eine fiktive Abrechnung (über 2.500 EUR) vorliegen.

Bei der Eingabe ging es um die Meldung eines Totalschadens. Ich habe den Eingeber über die Zulässigkeit dieser Einmeldung informiert.

4.14.3
Ausblick

Das Thema HIS ist auch in den neuen Verhaltensregeln der Versicherungswirtschaft, Code of Conduct (coc) nach der Vorschrift des § 38a BDSG, ein Regelungsgegenstand.

§ 38a BDSG

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Mittlerweile ist die Überprüfung durch die Berliner Datenschutzaufsichtsbehörde abgeschlossen und die Vereinbarkeit des ihr unterbreiteten Entwurfs mit dem geltenden Datenschutzrecht festgestellt worden.

Art. 14 coc

(1) Die Unternehmen der deutschen Versicherungswirtschaft – mit Ausnahme der privaten Krankenversicherer – nutzen ein Hinweis- und Informationssystem (HIS) zur Unterstützung der Risikobeurteilung im Antragsfall, zur Sachverhaltsaufklärung bei der Leistungsprüfung sowie bei der Bekämpfung von Versicherungsmissbrauch. Der Betrieb und die Nutzung des HIS erfolgen nach den Regelungen des Bundesdatenschutzgesetzes zur geschäftsmäßigen Datenerhebung und -speicherung zum Zweck der Übermittlung (Auskunftei).

(2) Das HIS wird getrennt nach Versicherungssparten betrieben. In allen Sparten wird der Datenbestand in jeweils zwei Datenpools getrennt verarbeitet: in einem Datenpool für die Abfrage zur Risikoprüfung im Antragsfall (A-Pool) und in einem Pool für die Abfrage zur Leistungsprüfung (L-Pool). Die Unternehmen richten die Zugriffsberechtigungen für ihre Mitarbeiter entsprechend nach Sparten und Aufgaben getrennt ein.

(3) Die Unternehmen melden bei Vorliegen festgelegter Einmeldekriterien Daten zu Personen, Fahrzeugen oder Immobilien an den Betreiber des HIS, wenn ein erhöhtes Risiko vorliegt oder eine Auffälligkeit, die auf Versicherungsmissbrauch hindeuten könnte. Vor einer Einmeldung von Daten zu Personen erfolgt eine Abwägung der Interessen der Unternehmen und des Betroffenen. Bei Vorliegen der festgelegten Meldekriterien ist regelmäßig von einem überwiegenden berechtigten Interesse des Unternehmens an der Einmeldung auszugehen. Besondere Arten personenbezogener Daten, wie z. B. Gesundheitsdaten, werden nicht an das HIS gemeldet.

(4) Die Unternehmen informieren die Versicherungsnehmer bereits bei Vertragsabschluss in allgemeiner Form über das HIS unter Angabe der verantwortlichen Stelle mit deren Kontaktdaten. Sie benachrichtigen anlässlich der Einmeldung die Betroffenen über die Art der gemeldeten Daten, den Zweck der Meldung, den Datenempfänger und den möglichen Abruf der Daten.

(5) Ein Abruf von Daten aus dem HIS kann bei Antragstellung und im Leistungsfall erfolgen, nicht jedoch bei Auszahlung einer Kapitallebensversicherung im Erlebensfall. Der Datenabruf ist nicht die alleinige Grundlage für eine Entscheidung im Einzelfall. Die Informationen werden lediglich als Hinweis dafür gewertet, dass der Sachverhalt einer näheren Prüfung bedarf. Alle Datenabrufe erfolgen im automatisierten Abrufverfahren und werden protokolliert für Revisionszwecke und den Zweck, stichprobenartig deren Berechtigung prüfen zu können.

(6) Soweit zur weiteren Sachverhaltsaufklärung erforderlich, können im Leistungsfall auch Daten zwischen dem einmeldenden und dem abrufenden Unternehmen ausgetauscht werden, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Der Datenaustausch wird dokumentiert. Soweit der Datenaustausch nicht gemäß Artikel 15 erfolgt, werden die Betroffenen über den Datenaustausch informiert. Eine Information ist nicht erforderlich, solange die Aufklä-

rung des Sachverhalts dadurch gefährdet würde oder wenn die Betroffenen auf andere Weise Kenntnis vom Datenaustausch erlangt haben.

(7) Die im HIS gespeicherten Daten werden spätestens am Ende des 4. Jahres nach dem Vorliegen der Voraussetzung für die Einmeldung gelöscht. Zu einer Verlängerung der Speicherdauer auf maximal 10 Jahre kommt es in der Lebensversicherung im Leistungsbereich oder bei erneuter Einmeldung innerhalb der regulären Speicherzeit gemäß Satz 1. Daten zu Anträgen, bei denen kein Vertrag zustande gekommen ist, werden im HIS spätestens am Ende des 3. Jahres nach dem Jahr der Antragstellung gelöscht.

(8) Der Gesamtverband der Deutschen Versicherungswirtschaft gibt unter Beachtung datenschutzrechtlicher Vorgaben einen detaillierten Leitfaden zur Nutzung des HIS an die Unternehmen heraus.

Der GDV hat bereits Anwendungshinweise zum HIS an die Versicherungswirtschaft herausgegeben.

4.15
Löschung von Gesundheitsdaten bei Versicherungen

Es ist nicht erforderlich, vom Versicherungsnehmer eingereichte medizinische Unterlagen zu speichern, wenn ein Versicherungsvertrag letztlich nicht zustande kommt.

4.15.1
Der Anlass

Ein Bürger bat mich mit seiner Eingabe, folgenden Sachverhalt datenschutzrechtlich zu überprüfen:

Er habe zur Prüfung der Voraussetzungen für eine private Berufsunfähigkeitsversicherung bei einem Versicherungsunternehmen medizinische Unterlagen eingereicht. Nachdem ein Vertragsschluss nicht zustande gekommen sei, habe er die Löschung dieser medizinischen Daten verlangt. Der Versicherer habe dies mit Blick auf § 257 HGB abgelehnt. Der Petent bat um Auskunft, ob diese Vorgehensweise datenschutzrechtlich zulässig ist.

4.15.2
Datenschutzrechtliche Bewertung

Datenschutzrechtlich sind personenbezogene Daten u. a. dann nicht zu löschen, wenn gesetzliche Aufbewahrungsfristen entgegen stehen (§ 4 Abs. 1 BDSG).

Eine solche Vorschrift könnte § 257 HGB sein.

§ 257 HBG

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

...

2. die empfangenen Handelsbriefe

...

(4) Die in Abs. 1 Nr. 1 und 4 aufgeführten Unterlagen sind 10 Jahre, die sonstigen in Abs. 1 aufgeführten Unterlagen 6 Jahre aufzubewahren.

Die entscheidende Frage ist demnach, ob auch eingereichte medizinische Unterlagen als empfangene Handelsbriefe mit einer sechsjährigen Aufbewahrungsfrist anzusehen sind, wenn ein Versicherungsvertrag letztlich nicht zustande kommt. Handelsbriefe sind nur Schriftstücke, die ein Handelsgeschäft betreffen (§ 257 Abs. 2 HGB).

Zu dieser Thematik hat das Bundesministerium der Justiz in einem Antwortschreiben auf eine Anfrage des Bayerischen Landesamtes für Datenschutz darauf hingewiesen, dass Unterlagen, die im Verlaufe von Verhandlungen zwischen Versicherungsnehmer und Versicherungsunternehmen anfallen, grundsätzlich Handelsbriefe im Sinne von § 257 HGB sein können. Komme es aber nicht zu einem Vertragsschluss, seien medizinische Informationen nicht dem § 257 HGB zuzuordnen. Dies ergebe sich daraus, dass die Korrespondenz, die nicht zu einem Abschluss eines Handelsgeschäfts geführt habe, nicht als Handelsbrief einzuordnen sei. Medizinische Unterlagen unterlägen insoweit keiner handelsrechtlichen Aufbewahrungspflicht. Dieser Position des Bundesministeriums der Justiz habe ich mich angeschlossen.

Dies hat zur Konsequenz, dass im vorliegenden Kontext § 257 HGB einer Löschung von Gesundheitsdaten nicht entgegen steht. Dieses Ergebnis harmoniert insbesondere auch mit § 213 des Versicherungsvertragsgesetzes vom 22. November 2007 (VVG). Diese Norm ist zwar nur in den Schlussvorschriften des VVG platziert, signalisiert aber dennoch deutlich, dass der Gesetzgeber personenbezogenen Gesundheitsdaten gerade auch im Versicherungsvertragsrecht besondere Beachtung schenkt. Auch wenn die Regelung die Erhebung dieser Daten bei Dritten betrifft, so wird doch exemplarisch deutlich, dass gerade auch im Versicherungsvertragsrecht Gesundheitsdaten datenschutzrechtlich einem besonderen Schutz unterliegen.

Vor diesem Hintergrund habe ich die Versicherung um Stellungnahme gebeten, ob sie an ihrer Rechtsansicht festhalte, § 257 HGB stehe der vom Eingeber begehrten Löschung seiner Gesundheitsdaten entgegen.

§ 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 Absatz 1 erforderliche Einwilligung kann vor Abgabe der Vertragserklärung erteilt werden. Die betroffene Person ist vor einer Erhebung nach Absatz 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 Absatz 2 bei der Unterrichtung.

Daraufhin hat die Versicherung sich nochmals mit der Angelegenheit befasst und mir als Ergebnis mitgeteilt, dass sie die vom Eingeber angestrebte Löschung seiner medizinischen Daten vorgenommen habe. Den Eingeber habe ich hierüber informiert.

4.16
Datenübermittlungen zwischen Versicherungen

Versicherungen sind u. a. dann befugt, Daten eines Versicherten einem anderen Versicherer zu übermitteln, wenn dies zur Wahrung der berechtigten Interessen dieses Versicherers erforderlich ist und kein Grund zu der Annahme besteht, dass der Versicherte ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

4.16.1
Der Anlass

Mit ihrer Eingabe kritisierte eine Versicherte folgenden Verfahrensablauf: Sie befinde sich zurzeit mit der Versicherung K. in einem Rechtsstreit wegen eines Verkehrsunfalls. Auf Grund einer missverständlichen Angabe im Impressum dieser Versicherung K. habe sie zuvor fehlerhaft die Versicherung R. verklagt. Die Versicherung R. habe gegenüber dem Gericht Klageabweisung beantragt, u. a. weil die Klage gegen den falschen Beklagten, nämlich die Versicherung R. statt Versicherung K. gerichtet sei. Der Datenschutzverstoß bestehe darin, so die Eingeberin, dass die Versicherung K. der Versicherung R. für diesen Prozess Versichertendaten betreffend den Verkehrsunfall übermittelt habe. Beide Versicherungen gehören zum selben Versicherungskonzern.

4.16.2
Datenschutzrechtliche Bewertung

Eine Versicherung ist befugt, einer anderen Versicherung personenbezogene Daten einer Versicherten zu übermitteln, wenn dies zur Rechtsverteidigung gegenüber der von der Versicherten erhobenen Klage geschieht. Die Berechtigung einer Versicherung, personenbezogene Daten einer anderen Versicherung zur Wahrung deren berechtigen Interessen zu übermitteln, ergibt sich aus § 28 Abs. 2 Nr. 2a BDSG.

§ 28 Abs. 2 Nr. 2a BDSG

Die Übermittlung … ist zulässig
2. soweit es erforderlich ist,

a) zur Wahrung berechtigter Interessen eines Dritten

...

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung … hat.

Im vorliegenden Fall war es so, dass sich die Versicherung R., an die Daten übermittelt wurden, zusätzlich zu dem Hinweis, dass sie die falsche Beklagte sei, versicherungsrechtlich (also in der Sache betreffend den Verkehrsunfall) verteidigen wollte. Die Übermittlung war also erforderlich, um die Versicherung R. in die Lage zu versetzen, vollständig auf die Klagebegründung erwidern zu können. Es bestand kein Grund zu der Annahme, dass die Versicherte ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung personenbezogener Daten an die Versicherung R. hatte, weil sie gegen diese Versicherung ja Klage erhoben hatte und es insoweit kein schutzwürdiges Interesse gab, dass die beklagte Versicherung R. nicht umfassend der Klage entgegentreten konnte.

Ich habe die Eingeberin über diese datenschutzrechtliche Bewertung informiert.

4.17
Telefonische Spendenwerbung

Telefonische Spendenwerbung durch nichtstaatliche Organisationen, die gemeinnützig oder auch als Interessenverbände tätig werden (sog. Spendensammelorganisationen), ist nur mit Einwilligung des Betroffenen zulässig.

In einem Beschwerdefall wurde die Petentin, die in unregelmäßigen Abständen an eine Spendenorganisation spendete, von deren Mitarbeiter te-

lefonisch kontaktiert und um eine regelmäßige halbjährige Spende gebeten. Dies lehnte die Petentin mit dem Hinweis ab, sie könne eine solche Verpflichtung nicht eingehen, da sie immer nur dann spende, wenn sie Geld übrig habe. Kurz nach diesem Telefonat erhielt die Petentin dennoch ein Schreiben der Organisation, in dem ihr für ihre Spendenbereitschaft gedankt und gleichzeitig mitgeteilt wird, dass ab einem bestimmten Zeitpunkt regelmäßig halbjährlich 10 EUR von ihrem Konto abgebucht werde. Die Petentin teilte der Organisation mit, dass sie der Abbuchung einer regelmäßigen Spende von ihrem Konto am Telefon nicht zugestimmt habe und bat um Löschung ihrer personenbezogenen Daten, weil sie künftig keinen Kontakt mehr zu der Organisation wünsche.

Nachdem die Organisation sich bei ihr entschuldigt hatte und versicherte, dass keine Abbuchungen erfolgen würden, aber nicht auf die Löschung ihrer Daten eingegangen war, bat mich die Petentin um Unterstützung, die Löschung ihrer Daten gemäß § 35 BDSG durchzusetzen.

Die betroffene Organisation gehört zu den sog. NGOs (non governmental organisations), also nichtstaatliche Organisationen, die gemeinnützig oder auch als Interessenverbände tätig werden (Spendensammelorganisationen).

Nach herrschender Meinung fallen NGOs, die gemeinnützig tätig sind, nicht unter die Bestimmungen des § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG), wonach eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, unzulässig wäre.

Das bedeutet aber nicht, dass diesen Organisationen Telefonwerbung grundsätzlich erlaubt ist. Auch die Telefonnummer einer natürlichen Person stellt bereits ein personenbezogenes Datum dar, deren Speicherung und Nutzung zu geschäftlichen Zwecken einer datenschutzrechtlichen Grundlage oder der Erlaubnis des Betroffenen bedarf.

Soweit es für Zwecke der Werbung für Spenden, die nach § 10b Abs. 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind, erforderlich ist, dürfen nach § 28 Abs. 3 Satz 2 Ziff. 3 BDSG personenbezogene Daten in bestimmtem Umfang verarbeitet oder genutzt werden. Erlaubt ist dies bei listenmäßig oder sonst zusammengefassten Daten über Angehörige einer Personengruppe, die sich auf die Zugehörigkeit der Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbeziehungen, seinen Namen, Titel, akademischen Grad, seine Anschrift, sein Geburtsjahr beschränken.

Demnach dürfen NGOs zur Spendenwerbung (nur) diese sog. „Listendaten“ verarbeiten und nutzen.

Das BDSG erlaubt in diesem Bereich (§ 28 Abs. 3 Satz 2 Nr. 3 BDSG) darüber hinaus keine Hinzuspeicherung oder gar werbliche Nutzung von weiteren Datenarten wie z. B. Telefonnummern oder E-Mail-Adressen durch die verantwortliche Stelle. Daraus ergibt sich, dass eine Speicherung und Nutzung der Telefonnummer nur mit Einwilligung des Spenders möglich wäre.

Im konkreten Beschwerdefall lag allerdings eine Einwilligung der Petentin nach § 4a Abs. 1 Satz 3 i. V. m. § 28 Abs. 3a BDSG zur telefonischen werblichen Ansprache nicht vor.

Das Verhalten der NGO habe ich als Verstoß gegen die datenschutzrechtlichen Bestimmungen beanstandet. Gleichzeitig habe ich die Spendenorganisation aufgefordert, künftig Telefonwerbung ohne vorliegende datenschutzrechtliche Einwilligung der Spender zu unterlassen.

Die personenbezogenen Daten der Petentin hat die NGO nach meiner Intervention, wie von dieser gewünscht, gelöscht.

4.18
Internetgestütztes Kampfrichter-Administrationssystem

Auch Sportverbände nutzen zur Verwaltungsoptimierung immer stärker das Internet. Ein Bundesverband hat mit meiner Hilfe ein Kampfrichter-Administrationssystem datenschutzkonform umgesetzt.

Ein großer bundesdeutscher Sportverband trat an mich heran und bat um datenschutzrechtliche Prüfung und Beratung zu einem für die speziellen Bedürfnisse des Verbandes entwickelten internetgestützten Kampfrichteradministrationssystem, das bundesweit eingesetzt werden sollte. Die Vertreter des Verbandes legten mir dazu die Beschreibungen der einzelnen Module, die Regelung der Zugriffsrechte, die Datenschutzerklärung der Nutzer (Einwilligungserklärung gem. § 4a BDSG), die Hinweise zum Datenschutz sowie die Nutzungsbedingungen des Verbandes vor.

Die wesentlichen Module der Automatisierung sind die Pflege der Kontaktdaten der Nutzer, die Einteilung der Kampfrichter, die Bewertung der Kampfrichter und die Nachrichten- und Informationsverwaltung. Die Zugriffsrechte der einzelnen Nutzer beruhen auf einem Rollensystem, wonach nur die Administratoren den Zugang zum Gesamtsystem erhalten. Für die einzelnen Nutzer sind ihrer Funktion angepasste (eingeschränkte) Zugriffsrechte vorgesehen. Sind die entsprechenden Grunddaten durch die Berechtigten der jeweiligen Ebene eingegeben, kann sich ein Kampfrichter u. a. zu Turnieren anmelden und seine Einteilung sowie das weitere Procedere (z. B. Bildung einer Fahrgemeinschaft) über das System abwickeln.

Auch hat er die Möglichkeit, seine Bewertungen einzusehen. Die Daten sind allerdings nur solange verfügbar, wie der Nutzer im System als „aktiv“ gekennzeichnet ist.

Die Überprüfung der Module und Zugriffsrechte ergab keine Beanstandungen. Die Zugriffsrechte waren nach dem Erforderlichkeitsgrundsatz ausgerichtet, d. h. jeder Zugriffsberechtigte kann das System nur im Rahmen seines Aufgabenbereichs nutzen. Insbesondere wurde nur die Verarbeitung der erforderlichen Daten vorgesehen. Auch wurde die Eingabe freiwilliger Daten hinreichend gekennzeichnet.

Allerdings habe ich darauf Wert gelegt, dass die Verpflichtung der Zugriffsberechtigten auf das Datengeheimnis (§ 5 BDSG) nicht online erfolgt, wie es ursprünglich vorgesehen war.

§ 5 BDSG

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Zwar hat der Gesetzgeber die Verpflichtung auf das Datengeheimnis an keine besonderen Formvorschriften gebunden. Bereits aus Nachweisgründen ist jedoch eine schriftliche Vorgehensweise anzuraten. Da die jeweilige Person verpflichtet werden muss, ist sie auch entsprechend zu informieren und über die Folgen einer Verletzung der Verpflichtung aufzuklären. Die Verpflichtung sollte daher aktenkundig gemacht und ihr Vollzug – ebenfalls zu Beweiszwecken – vom Betroffenen durch Unterschrift bestätigt werden. Der Verband sah von einer Online-Verpflichtung ab und verpflichtete die Zugriffsberechtigten in der empfohlenen Schriftform.

Bezüglich der Datenschutzerklärung und den Hinweisen zum Datenschutz sowie den Nutzungsbedingungen habe ich einige kleinere, zumeist redaktionelle Änderungen empfohlen, die zu einem besseren Verständnis und zu mehr Transparenz für die Nutzer führen sollen. Dies bezog sich z. B. auf Hinweise zur nur eingeschränkten Protokollierung von IP-Adressen. Eine vollständige Speicherung der aufrufenden IP-Adresse eines Seitenabrufs im Protokoll des Webservers ist nach derzeitiger Rechtsprechung nicht zulässig. Die Protokolleinträge sind zu anonymisieren (Löschen der letzten oder der letzten und vorletzten Stelle der IP-Adresse), sodass Auswertungen nach Herkunft der Aufrufe damit nicht mehr möglich sind. Ein entsprechender Hinweis über die Anonymisierung sollte im Internetangebot

vermerkt werden. Der Verband setzte diese Anregungen bei seinen Hinweisen um.

Schließlich bestellte der Verband im Zuge der Einführung des Systems einen Datenschutzbeauftragten nach § 4f BDSG und ist damit seinen gesetzlichen Verpflichtungen nachgekommen.

Nach Abschluss meiner Beratung wurde das Administrationssystem datenschutzkonform in Betrieb genommen.

5. Bilanz

5.1
Elektronische Aufenthaltsüberwachung ehemaliger Straftäter (40. Tätigkeitsbericht, Ziff. 3.3.3)

Mit Beginn des Jahres nahm in Bad Vilbel die Gemeinsame Überwachungsstelle der Länder (GÜL) ihre Tätigkeit auf. Ich hatte im 40. Tätigkeitsbericht über die Rahmenbedingungen berichtet.

In diesem Jahr lag der Schwerpunkt der Begleitung des Projekts auf der technischen Umsetzung, insbesondere der Entwicklung des Berechtigungs- und des IT-Sicherheitskonzepts. Dabei waren alle Beteiligten vor neue Herausforderungen gestellt – nicht nur die Technik muss rund um die Uhr funktionieren, sondern gleichzeitig muss auch jederzeit qualifiziertes Personal vor Ort sein, sowohl bei der GÜL als auch im Rechenzentrum der HZD in Hünfeld. Für die Polizei in den Ländern musste zudem technische Infrastruktur aufgebaut werden, um ggf. in einem Alarmfall sofort einen Zugriff auf die Daten zum Aufenthaltsort eines Probanden bekommen zu können, ohne dass abzusehen ist, ob dieser Fall je eintritt.

Nach Anlaufschwierigkeiten sind nunmehr im Wesentlichen die Voraussetzungen für eine so komplexe IT-Anwendung erfüllt.

Ein erster Fall in einem anderen Bundesland zeigte gleichzeitig die Grenzen der elektronischen Aufenthaltsüberwachung. Ein Proband hat in der Wohnung einer Bekannten erneut ein Kind missbraucht. Mithilfe der GPS-Daten konnte man nachweisen, dass er am Tatort war. Wie schon im letzen Jahr dargestellt, ist es dem System nicht möglich, im Vorhinein sicher zu stellen, dass es nicht zu einem Kontakt mit einem Kind und einer solchen Tat kommen kann. Dies zeigt, dass die hohen Erwartungen an dieses Projekt nicht erfüllbar sind. Mit der Aufenthaltsüberwachung lässt es sich eben nicht vollständig verhindern, dass ein Proband erneut Straftaten begeht.

5.2
Visawarndatei und Abgleich am Visumsverfahren beteiligter Personen mit der Antiterrordatei (40. Tätigkeitsbericht, Ziff. 3.4.2)

Im 40. Tätigkeitsbericht hatte ich mich kritisch zu dem geplanten Abgleich von Daten aller am Visumsverfahren beteiligter Personen mit der Antiterrordatei geäußert. Als datenschutzrechtlich problematisch hatte ich insbesondere die durch die Änderung des Aufenthaltsgesetztes vorgesehene Regelung gesehen, nach der alle am Visumsverfahren beteiligten Personen mit

den Daten der Antiterrordatei abgeglichen werden können. Meine Kritik bezog sich vor allem darauf, dass auch Personen wie Einlader oder Personen, die durch Abgabe einer Verpflichtungserklärung oder in anderer Weise die Sicherung des Lebensunterhalts des Eingeladenen gewähren wollen, einbezogen werden. Diese Regelung ist ohne Änderung in Kraft getreten. Ob sie gerichtlich Bestand haben wird, erscheint fraglich.

6. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

6.1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Februar 2012

Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen

stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

Aus Sicht des Datenschutzes ist eine Anzeige von Schuldnerdaten, die nicht vom legitimen Abfragezweck erfasst werden, zu vermeiden. Deshalb halten es die Datenschutzbeauftragten des Bundes und der Länder für notwendig, bei der Regelung der Einsicht in das Schuldnerverzeichnis die zwingende Angabe weiterer Identifizierungsmerkmale vorzusehen.

6.2
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21./22. März 2012

Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer **Datenschutz-Grundverordnung** enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst

hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,
- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,
- die Förderung des Selbstdatenschutzes,
- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,

– das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und
– die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Art. 8 der EU-Grundrechte-Charta und Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im **Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

6.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21./22. März 2012

Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

6.4
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21./22. März 2012

Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik – ins-

besondere der Videoüberwachung und dem Instrument der Mustererkennung – menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder“ frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT“ (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

6.5
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23. Mai 2012

Patientenrechte müssen umfassend gestärkt werden

Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken. Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.
- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.
- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.
- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.
- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.

– Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z. B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

6.6
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 2012

Orientierungshilfe zum datenschutzgerechten Smart Metering

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d. h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

– Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
– Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.
– Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
– Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
– Die Daten sollen an möglichst wenige Stellen übermittelt werden.
– Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
– Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.

- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.
- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

6.7
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012

Melderecht datenschutzkonform gestalten!

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht

insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

– Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage.

  Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.
– Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.
– Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.
– Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.
– Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.
– Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.
– Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt

werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

6.8
Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. November 2012

Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

– Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der **Datenschutz-Grundverordnung** an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.
– Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht be-

reits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

– Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.
– Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.
– Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.
– Mit Blick auf die **Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

6.9
Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. November 2012

Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene“ Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

6.10
Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. November 2012

Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale

(GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u. a. Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

6.11
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. November 2012

Einführung von IPv6
Hinweise für Provider im Privatkundengeschäft und Hersteller

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.
- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.
- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.
- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.
- Interface Identifier und Präfix sollten synchron gewechselt werden.
- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.
- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.

- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.
- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.
- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfix.
- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.
- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

7. Beschlüsse des Düsseldorfer Kreises

7.1
Beschluss der obersten Aufsichtsbehörden im nicht-öffentlichen Bereich vom 17. Januar 2012

Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung*

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY[1] daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z. B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung *(Krankenversicherung)*[2] benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache, dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. …[3] weiterleiten zu dürfen.

---

* Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.

[1] Hier und im Folgenden kann anstelle von „die Versicherung XY“ der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY“) jeweils „wir“ eingefügt werden.

[2] Hier kann die konkrete Sparte genannt werden.

[3] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[4] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.[5]

Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY [Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird] selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[6]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

[4] Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

[5] Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4a Abs. 1 Satz 2 BDSG.

[6] Werden bei einem Versicherungsprodukt generell keine Kinder und/oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen (siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1 Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht[7]

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesundheitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

☐ Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist – meine Gesundheitsdaten bei Ärzten, Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden[8] erhebt und für diese Zwecke verwendet.

Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen sowie Versicherungsanträgen und -verträgen

[7] Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

[8] Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.

aus einem Zeitraum von bis zu zehn Jahren[9] vor Antragstellung an die Versicherung XY übermittelt werden.

Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang – soweit erforderlich – meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von ihrer Schweigepflicht.

Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.[10]

Möglichkeit II:

☐ Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich

- in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
- oder die erforderlichen Unterlagen selbst beibringe.

  Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren[11] nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte[12] dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärungen bis zu zehn Jahre nach Vertragsschluss.

---

[9] Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

[10] Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 S. 2 i. V. m. Abs. 4 VVG.

[11] Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahres-Frist.

[12] Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

2.2 Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:[13]

Möglichkeit I:

☐ Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I).

Möglichkeit II:

☐ Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn diese abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

[13] Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z.B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.[14]

3.1 Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet.[15]

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2 Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XYGruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weiterge-

[14] Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

[15] Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.

geben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[16] soweit erforderlich für die anderen Stellen.[17]

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[18] über die Stellen[19] und Kategorien von Stellen[20], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.[21] Eine aktuelle Liste kann auch im Internet unter *(Internetadresse)* eingesehen oder bei *(Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mail-Adresse)* angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,[22] dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY

[16] Der Satzteil „für sich und“ ist nur für die Kranken-, Lebens- und Unfallversicherung zu verwenden.

[17] Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.

[18] In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.

[19] Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.

[20] Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z. B. Krankentransporte.

[21] Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.

[22] Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.

Unternehmensgruppe und sonstiger Stellen[23] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3 Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[24] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt.

Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt.

Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.

Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.[25] Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.

Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet.

Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung Ihrer Ge-

[23] „und sonstige Stellen“ – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.

[24] Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.

[25] Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.

sundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet.[26]

Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheitsdaten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4 Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[27]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.[28] Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweigepflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[29] melden.

---

[26] Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.

[27] Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht. Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

[28] Ein berechtigtes Interesse für die Abfrage zum Zweck der Risikound Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.

[29] Durch die Formulierung „an den jeweiligen Betreiber“ sowie die Aufnahme von „derzeit“ im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5 Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Informationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten, wenn der Vertrag nicht zustande kommt[30]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es

möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragen weiterer Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[31] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.[32]

Ort, Datum	Unterschrift Antragsteller/in oder mitzuversichernde Person
Ort, Datum	Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres)
Ort, Datum	Unterschrift des gesetzlichen Vertreters

[30] Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt. Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.

[31] Es zählt das Datum der Unterschrift im Antrag.

[32] Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz/Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung/Einzelfalleinwilligung) angeboten werden. Erfolgt keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z.B. in der Rei-

segepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.

7.2
Beschluss der obersten Aufsichtsbehörden im nicht-öffentlichen Bereich vom 18./19. September 2012

Near Field Communikation (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Aus-

lesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

8. Materialien

8.1

Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutz-Grundverordnung

Angesichts des rasanten technologischen Fortschritts, zunehmender Vernetzung und Globalisierung ist der grundrechtsorientierte Ansatz des europäischen Datenschutzrechts mit vielfältigen Herausforderungen konfrontiert. Das durch Art. 8 der Europäischen Grundrechtecharta garantierte Grundrecht auf den Schutz personenbezogener Daten ist seit dem Inkrafttreten des Vertrags von Lissabon unmittelbar anwendbares Recht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) begrüßt deshalb das von der Kommission verfolgte Ziel eines hohen gemeinsamen Datenschutzniveaus in der gesamten Europäischen Union.

Mit der Datenschutz-Grundverordnung (Verordnung) strebt die Kommission eine Harmonisierung des Datenschutzrechts an. Die Konferenz hält es für sinnvoll und erforderlich, einen effektiven Datenschutz für alle Bürgerinnen und Bürger in Europa zu gewährleisten. Ungeachtet der Frage, ob sich die Kompetenz der EU zum Erlass einer Verordnung auf Basis von Art. 16 Abs. 2 Satz 1 AEUV im Hinblick auf das Prinzip der begrenzten Einzelermächtigung und das Subsidiaritätsprinzip auch auf rein innerstaatliche Datenverarbeitungen im öffentlichen Bereich erstreckt, ist die Konferenz der Auffassung, dass auch insoweit ein möglichst hoher Mindeststandard gewährleistet werden muss. Es darf insgesamt zu keiner Absenkung des in den Mitgliedsstaaten bereits erreichten Schutzniveaus kommen. Die Mitgliedsstaaten sollten daher auch in Zukunft – vor allem bei besonders sensiblen Datenverarbeitungen – gesetzliche Regelungen mit einem möglichst hohen Schutzniveau erlassen dürfen. Die Verordnung muss in jedem Fall den Verfassungs- und Rechtstraditionen der Mitgliedsstaaten Rechnung tragen.

Der Entwurf ermächtigt die Kommission in einer Vielzahl von Vorschriften zu einer näheren Regelung durch delegierte Rechtsakte. Die Konferenz appelliert an das Europäische Parlament und den Rat, die Notwendigkeit jeder einzelnen Delegationsermächtigung kritisch zu überprüfen. Im Hinblick auf den Wesentlichkeitsgrundsatz müssen entsprechend Art. 290 AEUV die entscheidenden Regelungen in der Verordnung selbst getroffen oder aber im Hinblick auf fachspezifische Regelungen dem nationalen Gesetzgeber überlassen werden. Auch wenn das Parlament bei einer Ausübung der Delegationsrechte durch die Kommission auf den Erlass dieser Rechtsakte einwirken kann, ist deren demokratische Legitimation deutlich geringer, als

bei einer Regelung der wesentlichen Punkte in der Verordnung selbst. Die Konferenz lehnt daher insbesondere solche delegierten Rechtsakte ab, bei denen grundlegende materiell- und verfahrensrechtliche Regelungen (wie z. B. in Art. 6 bei der Rechtmäßigkeit der Verarbeitung) konkret ausgestaltet werden sollen.

Die Konferenz weist auch darauf hin, dass der Entwurf in zahlreichen Regelungen unbestimmte Rechtsbegriffe sowie Interessenabwägungen enthält, deren hoher Abstraktionsgrad einen großen Spielraum bei der Auslegung und Anwendung zulässt. Sie empfiehlt dringend, die notwendigen Klarstellungen in den Regelungen selbst vorzunehmen.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf vorgesehene Kohärenzverfahren, welches in der gegenwärtigen Ausgestaltung die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb stark vereinfacht und praktikabler gestaltet werden. Die durch Art. 8 der Grundrechtecharta und Art. 16 AEUV gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Die Konferenz hält es für erforderlich, die in den Art. 8 (3), 12 (6), 14 (7) und 22 (4) vorgesehenen Ausnahmen für die Datenverarbeitung kleiner und mittlerer Unternehmen (KMU) zu überprüfen. Ausnahmen sollten sich generell weniger an der Größe eines Unternehmens, sondern vielmehr an den Gefahren und Risiken für die Rechte und Freiheiten des Einzelnen orientieren. Auch von sehr kleinen Unternehmen können erhebliche Gefährdungen für den Datenschutz ausgehen.

Der Entwurf der Verordnung führt in erheblichem Umfang zu Abgrenzungsschwierigkeiten mit der RL 2002/58/EG. Art. 89 (1) ist insoweit zu abstrakt und unklar formuliert. Welche besonderen Pflichten gibt es konkret, die in der Richtlinie 2002/58/EG festgelegt sind? Weder Art. 89 noch die einschlägige Erwägung 135 geben hierüber Aufschluss.

Die Konferenz schlägt vor, eine Regelung „Erziehung und Bildung“ aufzunehmen. Der Datenschutz dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden,

die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

„Art. Xx – Erziehung und Bildung

Um sich in der Informationsgesellschaft behaupten zu können, ist den Bürgerinnen und Bürgern durch geeignete Maßnahmen Datenschutzkompetenz zu vermitteln. Sie ist Teil der übergreifenden Medienkompetenz; ihre Vermittlung ist eine gesamtgesellschaftliche Aufgabe in den Mitgliedstaaten, die hierbei von der Union unterstützt werden.“

Zu den einzelnen Regelungen nimmt die Konferenz wie folgt Stellung:

Kapitel I – Allgemeine Bestimmungen

Zu Art. 2:
Die Konferenz spricht sich dafür aus, dass auch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union entweder in den Geltungsbereich der Verordnung einbezogen werden (Art. 2 (2) lit. b)) oder die Verordnung 45/2001 zeitgleich angepasst wird. Es wäre nicht vertretbar, wenn sich die EU selbst von der angestrebten Modernisierung des Datenschutzrechts ausnehmen würde. Zudem spricht auch das Ziel der Harmonisierung für eine Einbeziehung der Organe der Union, da zunehmend auch zwischen diesen und den Mitgliedstaaten ein Austausch personenbezogener Daten stattfindet.

Die Beibehaltung der Ausnahme der Datenverarbeitung durch natürliche Personen zu ausschließlichen persönlichen oder familiären Zwecken in Art. 2 (2) lit. d) wird grundsätzlich begrüßt. Allerdings wäre eine Klarstellung wünschenswert, die in einer differenzierten Regelung die datenschutzrechtlichen Pflichten von natürlichen Personen angemessen ausgestaltet. Dies könnte beispielsweise in einer eigenständigen Regelung zur Veröffentlichung personenbezogener Daten an einen unbestimmten Personenkreis geschehen.

Zu Art. 3:
Die Konferenz begrüßt die Einführung des Marktortprinzips in der Verordnung.

Zum räumlichen Anwendungsbereich für Verarbeitungen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen weist sie darauf hin, dass Ermittlungs- und Rechtsdurchsetzungsbefugnisse im EU-Ausland nur nach Maßgabe bislang nicht existierender zwischenstaatlicher Verträge bestehen. In Vorentwürfen der Verordnung war deshalb bereits vorgesehen, dass der innerhalb der EU zu bestellende Vertreter (Art. 25) umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten solle. Dessen zusätzliche Einbeziehung in die Rechte und Pflichten wäre aus Sicht der Konferenz zu begrüßen.

Der Begriff der „Beobachtung" sollte konkretisiert werden (Art. 3 (2) lit. b)), weil nicht hinreichend klar ist, welche Anwendungsfälle hierdurch erfasst werden sollen.

Zu Art. 4:
Die Definition der „betroffenen Person" sollte ohne die Formulierung „nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde", die damit eine subjektive Komponente impliziert, wie folgt gefasst werden: „eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt von der für die Verarbeitung verantwortlichen oder jeder sonstigen natürlichen oder juristischen Person bestimmt werden kann" (Art. 4 (1)).

Es sollte auch klargestellt werden, dass Kennnummern, Standortdaten usw. zu den personenbezogenen Daten zählen (siehe Erwägungsgrund 23 der bekannt gewordenen Entwurfsfassung 56; Art. 4 (1) und (2)).

Es sollte definiert werden, was „automatisiert" bedeutet (Art. 4 (3)).

In der Definition der „Datei" sollte klargestellt werden, dass die Zugänglichkeit nach mindestens einem bestimmten Kriterium ausreicht (Art. 4 (4)).

Die Definition der „biometrischen Daten" sollte nicht nur auf die eindeutige Identifizierbarkeit abstellen, sondern auch das harmonisierte biometrische Vokabular verwenden: „Daten zu den physischen, physiologischen oder verhaltenstypischen Charakteristika eines Menschen wie Gesichtsbilder oder daktyloskopische Daten" (Art. 4 (11)).

Für Betroffene und Aufsichtsbehörden fehlt es an Transparenz und Verlässlichkeit, wenn die Hauptniederlassung über unternehmensinterne Regelungen („Ort (...), an dem die Grundsatzentscheidungen (...) getroffen werden") bzw. über den Schwerpunkt der Verarbeitung („Ort, an dem die Verarbeitungstätigkeiten (...) hauptsächlich stattfinden") definiert wird. Eine Präzisierung wird dringend für erforderlich gehalten, insbesondere im Hinblick auf die Regelungen des „One-Stop-Shops" in Art. 51 (2) sowie die Regelungen des gerichtlichen Rechtschutzes in Kapitel VIII.

Die Definition des „Dritten“ sollte in Art. 4 aufgenommen werden, um insbesondere die Figur des Auftragsdatenverarbeiters entsprechend Art. 2 lit. f) der RL 95/46/EG klarer zu fassen.

Die Begriffe „Anonymisierung“ und „Pseudonymisierung“ sollten ebenfalls definiert werden, da beiden Vorgängen materiell-rechtlich eine größere Bedeutung eingeräumt wird und aus Sicht der Konferenz auch eingeräumt werden sollte.

Kapitel II – Grundsätze

Zu Art. 5:
Als weiterer Grundsatz sollte in Art. 5 die Verpflichtung aufgenommen werden, dass bei der Verarbeitung personenbezogener Daten die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind, um die hohe Bedeutung des technologischen Datenschutzes zu unterstreichen.

Die Zweckbindung ist bei der Verarbeitung personenbezogener Daten eines der wichtigsten Grundprinzipien zur Gewährleistung des Datenschutzes. Im Hinblick auf Art. 5 lit. b) sollte die Zweckbindung deshalb strikter gefasst werden. Zumindest erwartet die Konferenz die Klarstellung, dass der in der Verordnung gewählte Begriff der Zweckvereinbarkeit der Zweckbindung im Sinne des deutschen Datenschutzrechts entspricht.

In Art. 5 lit. e) sollte zusätzlich die anonyme und pseudonyme Nutzung der Daten als Gestaltungsauftrag mit aufgenommen werden. Dies sollte im Weiteren mit Regelungen zu einer Privilegierung der pseudonymen Datenverarbeitung flankiert werden.

Zu Art. 6:
Die Abwägungsklausel des Art. 6 (1) lit. f) wird in der Praxis eine herausragende Bedeutung erlangen. Die Vorgaben und Maßstäbe, anhand derer die Interessenabwägung innerhalb dieser Auffangregelung vorzunehmen ist, müssen daher hinreichend klar sein. In Art. 6 (1) lit. f) sollte eine Regelungsstruktur gefunden werden, die branchen- und situationsspezifischen Konkretisierungen Rechnung trägt. Die Verordnung sollte dabei beispielsweise auf die spezifischen Datenschutzaspekte der Auskunfteien und des Scorings eingehen. Im Hinblick auf die Verarbeitung von personenbezogenen Daten zu Direktmarketingzwecken sollte – wie in der bekannt gewordenen Entwurfsfassung 56 – grundsätzlich ein Einwilligungserfordernis (opt-in) vorgesehen werden.

Zudem erscheint es – wie Art. 20 des Vorschlags zeigt – auch denkbar, abschließende Fallgruppen zu definieren, die einer Interessenabwägung auf-

grund des hohen Gefährdungspotentials der Datenverarbeitung von vornherein nicht zugänglich sind.

Vor dem Hintergrund des in Art. 290 AEUV niedergelegten Wesentlichkeitsgrundsatzes sollten die hier geforderten Konkretisierungen in der Verordnung selbst formuliert werden, da es sich um wesentliche Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten handelt. Art. 6 (5) wäre daher zu streichen.

Ausgehend von Art. 6 (3) lit. b) ist sicherzustellen, dass durch den Verweis auf das mitgliedstaatliche Recht im öffentlichen Bereich ein über die Anforderungen der Verordnung hinausgehendes Datenschutzrecht erhalten bleiben kann, wie dies in verschiedenen bundes- und landesrechtlichen Regelungen bereits jetzt verwirklicht ist. Es muss auch weiterhin ohne Zweifel gewährleistet sein, dass in einem ausdifferenzierten bereichsspezifischen Datenschutzrecht dem erhöhten Schutzbedarf staatlicher Datenverarbeitung auch in Zukunft Rechnung getragen wird. Dies muss sich eindeutig und ausdrücklich aus dem Wortlaut von Art. 6 (3) lit. b) ergeben. Anderenfalls wäre der derzeit bestehende besondere Schutz, beispielsweise der in der Bundesrepublik Deutschland bestehende Schutz von Sozialdaten, durch die Verordnung gefährdet.

Zu Art. 7:
Die Konferenz unterstützt die Absicht der Kommission, in Art 7 (4) die Freiwilligkeit von Einwilligungen zu konkretisieren. Sie weist allerdings darauf hin, dass ein erhebliches Ungleichgewicht nur ein Indiz für Unfreiwilligkeit sein kann.

Zu Art. 8:
Der besondere Schutz von Kindern und Jugendlichen bei der Verarbeitung der auf sie bezogenen Daten ist der Konferenz ein besonderes Anliegen. Insofern begrüßt sie, dass sich der Verordnungsentwurf dieser Thematik annimmt und sie in einer spezifischen Regelung verankern will. Die Vorschrift sollte sich jedoch stärker an den konkreten, für diese Altersgruppe spezifischen Gefährdungen orientieren. Aus diesem Grunde sollte bei Einwilligungen auch stärker auf die Einsichtsfähigkeit des Kindes und weniger auf starre Altersgrenzen abgestellt werden.

In Art. 8 (1) sollte das Regelungsziel der Norm präzisiert werden. Es ist zu klären, ob eine Beschränkung auf Dienste der Informationsgesellschaft ausreichend ist, da es sich gemäß der Begriffsbestimmung aus der Richtlinie 98/34/EG hierbei in der Regel um gegen Entgelt erbrachte Dienste handelt,

obwohl offensichtlich auch entgeltfreie Dienste erfasst werden sollen. Einer Klarstellung bedarf auch, wann einem Kind solche Dienste „direkt“ angeboten werden. Es ist ebenfalls zu klären, ob sich Art. 8 (1) ausschließlich auf solche Datenverarbeitungen bezieht, bei denen die Rechtmäßigkeit nach Art. 6 (1) lit. a) auf die Einwilligung gestützt wird oder ob bei jeder Datenverarbeitung der Einwilligungsvorbehalt der Eltern bzw. gesetzlichen Vertreter gelten soll.

Zudem ist das Verhältnis zwischen den Absätzen 1 und 2 des Art. 8 klärungsbedürftig.

Die Profilbildung (Art. 20) sollte bei Minderjährigen generell verboten sein.

Zu Art. 9:
Art. 9 soll den bedeutsamen Bereich der Zulässigkeit der Verarbeitung von besonderen Kategorien personenbezogener Daten regeln. Die Konferenz sieht hier den aus Art. 8 der RL 95/46/EG übernommenen Ansatz eines abschließenden Katalogs sensitiver Daten kritisch. Vorzugswürdig wäre es, auf den tatsächlichen Verarbeitungskontext abzustellen und den Katalog der sensitiven Daten als Regelbeispiele auszugestalten.

Die Vorgaben sind im Sinne des Wesentlichkeitsgrundsatzes in der Verordnung selbst zu treffen, die entsprechend zu ergänzen ist. Die in Art. 9 (3) enthaltene Delegationsermächtigung wird deshalb abgelehnt.

Zu Art. 10:
Das von der Verordnung hier offenbar verfolgte Regelungsziel wird in Erwägungsgrund 45 deutlich. Dort wird ausführt, dass der für die Verarbeitung Verantwortliche nicht verpflichtet sein sollte, zusätzliche Daten einzuholen, um eine betroffene Person zu bestimmen. Er sollte das Recht haben, bei der betroffenen Person, falls diese von ihrem Auskunftsrecht Gebrauch macht, weitere Informationen einzuholen, um die zu dieser Person gesuchten personenbezogenen Daten zu lokalisieren. Dies spiegelt sich im Wortlaut des Art. 10 jedoch nicht wider. Dieser sollte deshalb so gefasst werden, dass sich der Erwägungsgrund 45 im Regelungstext selbst niederschlägt.

Kapitel III Rechte der betroffenen Person

Zu Art. 11:
Der Vorschlag wird grundsätzlich begrüßt. Es sollte jedoch in Abs. 1 klargestellt werden, was der für die Verarbeitung Verantwortliche (konkret) leisten muss.

Zu Art. 12:
Aus Gründen der Bestimmtheit und wegen der Erheblichkeit der hier zu treffenden Konkretisierungen sollte unmittelbar in der Verordnung selbst dargelegt werden, unter welchen Voraussetzungen ein Antrag offenkundig unverhältnismäßig ist, insbesondere auch, wann eine missbräuchliche Häufung von Betroffenenrechten vorliegt (vgl. Art. 12 (4)). Die Befugnis der Kommission zu delegierten Rechtsakten in Art. 12 (5) sollte daher entfallen.

Die Konferenz spricht sich gegen eine Missbrauchsgebühr aus. Aus ihrer Sicht reicht es aus, dass in Missbrauchsfällen das jeweilige Betroffenenrecht nicht in Anspruch genommen werden kann. Sofern an der Missbrauchsgebühr festgehalten wird, muss vermieden werden, dass sich Betroffene völlig unerwartet Gebührenforderungen gegenübersehen. Deshalb sollte der für die Verarbeitung Verantwortliche die betroffene Person im konkreten Einzelfall darüber informieren müssen, wenn er die Ausübung der Betroffenenrechte für offenkundig unverhältnismäßig erachtet und aus diesem Grund ein Entgelt verlangen will. Die Höhe des Entgelts muss verhältnismäßig sein und sich an dem tatsächlichen Aufwand bemessen.

Art. 12 sollte um das Erfordernis sicherer Übertragungswege für personenbezogene Daten nach dem Stand der Technik ergänzt werden.

Zu Art. 13:
Die Regelung wird grundsätzlich begrüßt. Die Nachberichtspflicht gemäß Art. 13 sollte sich jedoch auch auf Widersprüche nach Art. 19 erstrecken.

Zu Art. 14:
In der Verordnung ist unter Art. 14 (4) lit. b) klarzustellen, was unter einer „angemessenen“ Frist zu verstehen ist. Ferner ist zu prüfen, ob anstatt dieser nicht ein „unverzügliches Handeln“ geboten ist. Benachrichtigungen erst bei Datenübermittlungen dürfen nur bei Datenverarbeitern möglich sein, die geschäftsmäßig Daten zur Übermittlung vorhalten (u. a. Auskunfteien, Adresshandel, Detekteien).

Zu Art. 15:
In Art. 15 (1) lit. g) sollte die Einschränkung auf die (lediglich) „verfügbaren“ Herkunftsdaten gestrichen werden, da eine Angabe über die Herkunft personenbezogener Daten stets geboten ist und diese nicht verschleiert werden darf.

Die Aufklärungspflicht nach Art. 15 (1) lit. h) sollte auf die „Bedeutung und Tragweite“ der Verarbeitung erstreckt werden. Ein (ausdrücklicher) Hinweis

auf besondere Risiken bei der Profilbildung, Auskunfteien oder dem Scoring ist aufzunehmen.

Es muss zudem sichergestellt werden, dass für eine Mitteilung in elektronischer Form gemäß Art. 15 (2) nur sichere Übertragungswege nach dem Stand der Technik in Betracht kommen.

Zu Art. 16:
Es ist klarzustellen, ob unter einem Korrigendum eine Richtigstellung zu verstehen ist. Zudem regelt die Vorschrift nicht, wie zu verfahren ist, wenn sich die Unrichtigkeit oder Richtigkeit der Daten nicht beweisen lässt, bzw. wer die Beweislast trägt. Dieser Punkt sollte ergänzt werden. Denkbar wäre z. B. eine Verpflichtung, diese Daten im Sinne von Art. 17 (4) zu beschränken.

Zu Art. 17:
In Art. 17 (2) sollte eine Pflicht der Dritten zur Löschung der Daten analog Art. 17 (1) geregelt werden. Insbesondere sollte klargestellt werden, ob die Regelung auf den Bereich des Internets beschränkt ist und ob sie nach Maßgabe des Lindqvist-Urteils auch für Privatpersonen gilt.

Das Verhältnis der „umgehenden“ Löschungspflicht in Art. 17 (3) zu der in Art. 12 (2) geregelten Monatsfrist ist klärungsbedürftig. Es erscheint jedenfalls nicht sinnvoll, wenn der für die Verarbeitung Verantwortliche zwar einerseits die personenbezogenen Daten umgehend löschen müsste, andererseits aber für die Benachrichtigung des Betroffenen über die Löschung einen Monat Zeit hätte.

Die Formulierung in Art. 17 (2) „alle vertretbaren Schritte“ bedarf insbesondere aus technischer Sicht der Präzisierung.

Die Beschränkung nach Art. 17 (4) sollte verpflichtend vorgegeben werden.

Zu Art. 18:
Die Konferenz unterstützt die Einführung eines Rechts auf Datenportabilität in Art. 18 (1). Dieses Recht sollte aber nicht davon abhängen, ob der für die Verarbeitung Verantwortliche seine Verarbeitungen in einem gängigen Format tätigt. Vielmehr sollte durch die Streichung des Wortes „gängige“ eine allgemeine Konvertierungspflicht geregelt werden. Es ist klärungsbedürftig, ob Art. 18 (1) auch den öffentlichen Bereich erfasst.

Die in Art. 18 (2) verwandten Begriffe des Zur-Verfügung-Stellens und des Entziehens von Daten sollten in der Verordnung definiert werden, falls auf diese Begriffe nicht in Gänze verzichtet werden kann.

Zu Art. 19:
In Art. 19 (1) sollte der Begriff „schutzwürdige Gründe“ durch „berechtigte Interessen“ ersetzt werden. Es sollte zudem geprüft werden, ab wann und wie der Nachweis für das überwiegende Verarbeitungsinteresse des für die Verarbeitung Verantwortlichen als erbracht gelten soll.

Kommerzielle Werbung sollte, wie bereits zu Art. 6 angemerkt, grundsätzlich nur mit Einwilligung des Betroffenen gestattet sein. Art. 19 (2) sollte deshalb entsprechend angepasst werden. Die Konferenz empfiehlt zudem, den Begriff „unentgeltlich“ in Art. 19 (2) zu streichen, da sich die Unentgeltlichkeit bereits aus Art. 12 (4) Satz 1 ergibt. Andernfalls wäre im Einzelnen darzulegen, weshalb welche Maßnahmen nach Kapitel III jeweils entgeltfrei sein sollen oder nicht.

Unter Hinweis zu den Anmerkungen zu Art. 13 sollte auch Art. 19 entsprechend angepasst werden.

Zu Art. 20:
Die Konferenz unterstützt grundsätzlich die Aufnahme einer speziellen Regelung zur Profilbildung. Allerdings hält sie den Vorschlag für stark ergänzungsbedürftig.

Schon die Profilbildung selbst (z. B. in sozialen Netzwerken, beim Scoring und bei Auskunfteien) greift in erheblicher Weise in das Grundrecht auf Datenschutz ein und ist deshalb regelungsbedürftig.

Art. 20 (1) sollte zudem auf jede – auch nur teilweise automatisierte – systematische Verarbeitung zur Profilbildung Anwendung finden und daher das Wort „rein“ gestrichen werden.

Bei Minderjährigen (Art. 8) sollte die Profilbildung generell verboten sein.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wird wegen ihrer besonderen Sensitivität äußerst kritisch gesehen. Dort, wo sensitive Daten für eine Prognose unerlässlich sind, wie z. B. bei der Risikobeurteilung im Krankenversicherungsbereich, müssen enge, branchenspezifische Ausnahmetatbestände eingeführt werden, die an dem Grundsatz der Erforderlichkeit auszurichten sind. In Art. 20 (3) ist zudem klarzustellen, ob die Voraussetzungen des Art. 9 kumulativ gelten sollen. Dies würde sicherstellen, dass die Verwendung besonderer Kategorien personenbezogener Daten materiell-rechtlichen Beschränkungen unterliegt und sie nicht beliebig in Profilbildungen einfließen können.

Im Hinblick auf die besonderen Risiken der Bildung von Profilen, die auf einzelne Personen bezogen werden können, ist die Wiederherstellung eines

Personenbezugs bei unter Pseudonym oder einem technischen Identifikationsmerkmal geführten Profilen grundsätzlich zu untersagen.

Wegen der Erheblichkeit der in Art. 20 (5) zu treffenden Konkretisierungen und aus Gründen der Bestimmtheit sollte eine entsprechende Reglung in die Verordnung aufgenommen und die Befugnis der Kommission zu delegierten Rechtsakten gestrichen werden.

Zu Art. 21:
Statt einer Öffnungsklausel für den nationalen Gesetzgeber nur zur Beschränkung der Rechte Betroffener (Art. 21) sollten weiter reichende Betroffenenrechte gewährt werden dürfen. Dies gilt ungeachtet der bereits zu Art. 6 geforderten generellen Öffnungsklausel für den öffentlichen Bereich.

Art. 21 (1) lit. c) sollte gestrichen werden. Es ist nicht nachvollziehbar, weshalb die bisher in der RL 95/46/EG nicht vorgesehene Beschränkung in Bezug auf den Schutz sonstiger öffentlicher Interessen geboten sein soll. Zumindest sollten die Anforderungen an die Beschränkung strikter formuliert werden, damit die Betroffenenrechte nicht leerlaufen.

Kapitel IV – Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Ein zukunftsfähiger Datenschutz umfasst technische und organisatorische Maßnahmen, die Datenschutz und Datensicherheit angemessen berücksichtigen. Um dies zu gewährleisten, sind die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit als Zielvorgaben für technische und organisatorische Maßnahmen in die Bestimmungen der Art. 23 ff. aufzunehmen.

Zu Art. 22:
Um sicherzustellen, dass eine Verarbeitung personenbezogener Daten erst dann erfolgt, wenn die geeigneten Strategien und Maßnahmen auch umgesetzt sind, sollte Art. 22 (1) wie folgt formuliert werden: „Der für die Verarbeitung Verantwortliche stellt durch *die Umsetzung* geeigneter Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann.“

Art. 22 (3) sollte dahingehend ergänzt werden, dass die Entscheidung über Konsequenzen aus der Überprüfung der in den Absätzen 1 und 2 genannten Maßnahmen nicht dem Prüfer, sondern weiterhin dem für die Verarbeitung Verantwortlichen obliegt.

Zu Art. 23:
In Art. 23 (1) könnte die ausdrückliche Bezugnahme auf die Berücksichtigung der Implementierungskosten zu einem Einfallstor für das Unterlassen von Maßnahmen zur datenschutzfreundlichen Technikgestaltung werden. Zumindest müssen – wie in Art. 30 (1) – die Implementierungskosten technisch-organisatorischer Maßnahmen in ein angemessenes Verhältnis zum konkreten Gefahrenpotential der Datenverarbeitung gesetzt werden, um eine Relation zwischen Kosten und Eingriffstiefe in das Recht auf informationelle Selbstbestimmung herzustellen.

Art. 23 (2) sollte präzisiert und um Kriterien und Anforderungen in Bezug auf die zu treffenden Maßnahmen und Verfahren ergänzt werden. Hierbei sind insbesondere Anonymisierung und Pseudonymisierung nach dem Stand der Technik zu fordern, sofern dies nicht bereits in Art. 5 geregelt wird.

Es sollte klargestellt werden, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft.

Die Grundeinstellungen von Produkten und Diensten sind so zu gestalten, dass so wenig personenbezogene Daten wie möglich erhoben oder verarbeitet werden und bereits ohne Zutun der Nutzer eine datenschutzfreundliche Nutzung sichergestellt wird.

Die Regelung sollte ausdrücklich auch für Verhaltensbeobachtungen ("Trakking") im Internet durch den für die Verarbeitung Verantwortlichen oder durch Dritte gelten.

Satz 2 des Art. 23 (2) sollte wie folgt lauten: „Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich *nur den von der betroffenen Person zu bestimmenden Personen* zugänglich gemacht werden.“ Damit soll erreicht werden, dass die betroffene Person den Personenkreis selbst bestimmt, dem ihre personenbezogenen Daten zugänglich gemacht werden dürfen, und der für die Verarbeitung Verantwortliche hierfür die entsprechenden Vorkehrungen zu treffen hat.

Zu Art. 24:
In Art. 24 sollte im Text ausdrücklich ergänzt werden, dass sich die betroffene Person zur Wahrnehmung ihrer Rechte an jeden der für die gemeinsame Verarbeitung Verantwortlichen wenden kann.

Zu Art. 25:
Die Konferenz schlägt vor, auch in den Fällen des Art. 25 (2) lit. a) einen Vertreter zu bestellen. Art. 25 (2) lit. a) sollte daher gestrichen werden.

Der in Art. 25 (2) lit. b) geplante Verzicht bei Unternehmen mit weniger als 250 Mitarbeitern auf die Benennung eines Vertreters, der umfassend in die Rechtsstellung des Verantwortlichen und dessen Pflichten eintreten sollte, stellt eine Ausnahme dar, die nicht nachvollziehbar ist. Die Konferenz schlägt daher vor, diese Ausnahmeregelung ebenfalls zu streichen. Diese Klausel eröffnet weitgehende Umgehungsmöglichkeiten, da nicht geprüft werden kann, wie viele Beschäftigte bei einem nicht in der Union niedergelassenen Unternehmen tatsächlich tätig sind.

Zu Art. 26:
Der in Art. 26 (2) geregelte Mindestinhalt eines Vertrages oder Rechtsaktes zur Auftragsdatenverarbeitung sollte die wesentlichen Aspekte enthalten und daher um die Angabe von Gegenstand und Dauer des Auftrags sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung, der Art der Daten und den Kreis der Betroffenen ergänzt werden. In lit. a) sollte durch Streichung des 2. Halbsatzes sichergestellt werden, dass der Auftragsverarbeiter in jedem Fall ausschließlich auf Weisung des für die Verarbeitung Verantwortlichen tätig wird und nicht nur in besonderen Fällen, in denen die Übermittlung der Daten nicht zulässig ist.

Der Schutz der betroffenen Person erfordert die Klarstellung, dass sie sich bei gemeinsam für die Verarbeitung Verantwortlichen gemäß Art. 24 sowohl an den für die Verarbeitung Verantwortlichen als auch an den Auftragsverarbeiter wenden kann.

Eine wirksame Kontrolle des Auftragsverarbeiters kann nur umfassend erfolgen, wenn dem für die Verarbeitung Verantwortlichen in Art. 26 (2) auch ein Kontrollrecht, beispielsweise durch einen Treuhänder, eingeräumt wird und den Auftragsverarbeiter entsprechende Mitwirkungspflichten treffen. Dies gilt auch für etwaige Unterauftragsverhältnisse.

Die Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des Auftragsverarbeiters sind wesentliche Fragen, die letztlich auch die Zulässigkeit der Auftragsdatenverarbeitung insgesamt berühren. Insbesondere wäre etwa die Einführung und nähere Ausgestaltung eines Konzernprivilegs eine wesentliche Frage, die im Sinne von Art. 290 AEUV – soweit in den Absätzen 1 bis 4 nicht ohnehin bereits geschehen – in der Verordnung selbst geregelt werden sollte. Die Konferenz sieht daher die in Art. 26 (5) vorgesehene Ermächtigung zu delegierten Rechtsakten kritisch.

Zu Art. 28:
In Art. 28 sollte geregelt werden, dass die Dokumentation grundsätzlich vor Aufnahme der Verarbeitung personenbezogener Daten zu erstellen ist. Zu-

dem sollte der für die Verarbeitung Verantwortliche verpflichtet werden, die Dokumentation dem Datenschutzbeauftragten (soweit vorhanden) zur Verfügung zu stellen.

Die zeitliche Befristung einer Verarbeitung personenbezogener Daten ist im Sinne des Erforderlichkeitsprinzips ein wesentlicher Grundsatz. Art. 28 (2) lit. g) sollte daher in „eine *konkrete* Angabe der Fristen für die Löschung der verschiedenen Datenkategorien“ geändert werden.

Zu Art. 30 bis 32 allgemein:
Verfahren mit Personenbezug müssen durch technische und organisatorische Maßnahmen, ausgerichtet an den Datenschutzzielen, geschützt werden. Dieser Grundsatz ist in der Verordnung selbst zu verankern. Die Konferenz verweist in diesem Zusammenhang auf Vorbemerkungen zu Kapitel IV. Im Übrigen sollten Aufzählungen technischer und organisatorischer Maßnahmen durch entsprechende Verweise ersetzt werden.

Zu Art. 30:
Die in Art. 30 (1) geforderten angemessenen technischen und organisatorischen Maßnahmen können nur durch eine vorab und kontinuierlich durchgeführte Risikobewertung bzw. Risikoanalyse gewährleistet werden. IT-Sicherheit erfordert in diesem Sinne ein konzeptionelles Herangehen sowie die Etablierung von IT-Sicherheits- und Datenschutzmanagementsystemen. Art. 30 (1) sollte daher durch die Forderung nach einem Sicherheitskonzept ergänzt werden, welches Teil der Verfahrensdokumentation gemäß Art. 28 (2) lit. h) werden muss.

Wie in Art. 23 (1) sollte auch in Art. 30 (1) die Bezugnahme auf Implementierungskosten gestrichen werden.

Zu Art. 32:
Die in Art. 32 (3) geforderte Verschlüsselung personenbezogener Daten muss dahingehend präzisiert werden, dass sie durch Verfahren nach dem Stand der Technik erfolgen muss.

Zu Art. 33:
Eine Regelung der Datenschutz-Folgenabschätzung (Art. 33), die nachhaltig dem Schutz personenbezogener Daten dienen soll, muss die elementaren Datenschutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit umsetzen, um vollumfänglich Risiken und dafür angemessene Maßnahmen identifizieren zu können.

Die Ergebnisse sind in einem regelmäßigen Monitoring zu überprüfen.

Die Begriffe der Datenschutz-Folgenabschätzung und der Vorab-Genehmigung bzw. -Zurateziehung sollten voneinander abgegrenzt werden, da sich diese wechselseitig nicht ersetzen können.

Da jede der in Art. 33 (2) lit. a) genannten Auswertungen bereits erhebliche Risiken mit sich bringt, sollten die Worte „systematische und umfassende“ entfallen.

Die Konferenz schlägt vor, in Art. 33 (2) lit. c) das Wort „weiträumig“ zu streichen, da der Begriff zu unbestimmt ist und aus Sicht der betroffenen Person kein Unterschied besteht, ob die Überwachung weiträumig oder kleinräumig stattfindet.

In Art. 33 (2) lit. d) sollte die Durchführung einer Datenschutz-Folgenabschätzung für die Verarbeitung personenbezogener Daten aus Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten, nicht vom Umfang der Datei abhängen, sondern in jedem Fall erfolgen. Das Wort „umfangreich“ sollte daher gestrichen werden.

Für die Datenschutz-Folgenabschätzung muss auch zwingend in Art. 33 (3) eine Dokumentationspflicht aufgenommen werden.

Schließlich sollte Art. 33 um einen zusätzlichen Absatz ergänzt werden, der das Verbot der Datenverarbeitung bei unangemessen hohen Eingriffen in die Rechte der Betroffenen fordert. Grundsätzlich sollten Verfahren ausgewählt werden, die den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung mit sich bringen.

Zu Art. 34:
Die Konferenz hält den Vorschlag, dass der interne Datenschutzbeauftragte die Beantragung einer vorherigen Genehmigung bzw. Zurateziehung nach Art. 37 (1) lit. f) nur überwachen soll, für nicht ausreichend. Zur Entlastung der Aufsichtsbehörden und zur Stärkung des betrieblichen Datenschutzes sollte ihm diese Aufgabe komplett übertragen werden können. Deutschland hat mit der Durchführung der Vorabkontrolle durch die internen Datenschutzbeauftragten gute Erfahrungen gemacht.

Zu Art. 35:
Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv.

Es sollte eine Frist geregelt werden, innerhalb derer der Datenschutzbeauftragte nach Aufnahme der Daten verarbeitenden Tätigkeit zu bestellen ist. Die Konferenz schlägt hierfür eine Frist von einem Monat vor.

Die Konferenz bedauert, dass in Art. 35 (1) lit. b) eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten vorgesehen ist. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Art. 35 (1) lit. c) sollte dahingehend geändert werden, dass bei jeder risikobehafteten Datenverarbeitung (z. B. Auskunfteien, Detekteien, Callcenter, Lettershops etc.) unabhängig von der Mitarbeiterzahl eine Bestellungspflicht für einen Datenschutzbeauftragten besteht. Das Gleiche gilt für Unternehmen, bei denen eine Datenschutzfolgenabschätzung erforderlich ist. Die Anknüpfung an die „regelmäßige und systematische Beobachtung von betroffenen Personen“ ist insoweit nicht ausreichend.

Durch die in Art. 35 (7) geregelte Möglichkeit der Befristung der Amtszeit des Datenschutzbeauftragten kann die Unabhängigkeit beeinträchtigt werden. Die Amtszeit des internen Datenschutzbeauftragten sollte daher nicht befristet werden und das dem Amt zugrunde liegende Arbeitsverhältnis nur aus wichtigem Grund kündbar sein. Die Amtszeit von externen Datenschutzbeauftragten sollte mindestens 4 Jahre betragen.

Art. 35 (11) ist zu streichen. Die Fälle, in denen unabhängig von der Mitarbeiterzahl ein Datenschutzbeauftragter zu bestellen ist, betreffen eine wesentliche Frage und sind deshalb in der Verordnung selbst zu regeln.

Zu Art. 36:

Der Datenschutzbeauftragte sollte nicht nur ein unmittelbares Vorspracherecht gegenüber der Leitung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters haben, sondern dieser – als Ausdruck seiner Unabhängigkeit – unmittelbar unterstellt sein. Außerdem sollte für interne Datenschutzbeauftragte ein wirksamer arbeitsrechtlicher Kündigungsschutz sowie die Aufnahme eines Benachteiligungsverbots vorgesehen werden, um seine Unabhängigkeit besser zu sichern.

In Art. 36 (3) ist das Recht des Datenschutzbeauftragten auf Fort- und Weiterbildung sowie die Kostenübernahme hierfür zu normieren. Zudem sind Regelungen zur Verschwiegenheit des Datenschutzbeauftragten sowie zum Zeugnisverweigerungsrecht aufzunehmen.

Zu Art. 37:

Die Aufgaben des Datenschutzbeauftragten sind in der deutschen Sprachfassung missverständlich formuliert. So wird sprachlich nicht hinreichend deutlich, ob der Datenschutzbeauftragte beispielsweise selbst die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 31 vornehmen muss oder diese Meldung nur zu überwachen hat (Art. 37 (1) lit. e)).

In diesem Zusammenhang sollte auch klargestellt werden, dass die Aufgaben des Datenschutzbeauftragten den für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter nicht von seinen Pflichten entbinden bzw., dass keine Möglichkeit zur Exkulpation bei Nicht- oder Schlechterfüllung seitens des Datenschutzbeauftragten besteht.

Zu Art. 38 und Art. 39:

In Art. 39 (2) sollten die wesentlichen Regelungstatbestände einer Zertifizierung und der Vergabe eines Siegels und Zeichens direkt aufgenommen und nicht an die Kommission delegiert werden. Die Zertifizierungs- und Vergabekriterien sind insbesondere an den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5, der Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6, der Betroffenenrechte und an den Datenschutzzielen in Art. 30 nach Maßgabe der Verordnung auszurichten.

Zertifizierungs-, Vergabe- und Widerrufsverfahren müssen den Anforderungen des Grundsatzes der Transparenz hinsichtlich der Kriterien, des Verfahrens und der wesentlichen Evaluierungsergebnisse genügen. Die Unabhängigkeit und Fachkunde der Zertifizierungs- und Vergabestellen und der Evaluatoren sind zu gewährleisten.

Eine datenschutzspezifische Zertifizierung gemäß Art. 39 (1) beinhaltet stets auch eine Bewertung der IT-Sicherheit. Diese sollte sich an europäischen und internationalen Standards orientieren und die Datenschutzziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit aus Betroffenensicht einbeziehen. Ein entsprechender Zusatz unter Einbeziehung des Ergänzungsvorschlags der Konferenz zu Kapitel IV (elementare Datenschutzziele) ist daher vorzusehen.

Zertifizierungen sind zeitlich zu befristen. Eine Rücknahme eines Zertifikates bei gravierenden Mängeln muss auch vor Fristablauf möglich sein.

Bei der Ausgestaltung der Verhaltensregeln und Zertifizierungsverfahren ist der Europäische Datenschutzausschuss zu beteiligen.

Kapitel V – Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Zu Art. 41:
Die Kommission sollte bei der Angemessenheitsprüfung nach Art. 41 (2) stets auch die Stellungnahme des Europäischen Datenschutzausschusses einholen und berücksichtigen müssen. Im Zusammenhang mit Art. 41 (6) muss klargestellt werden, dass in den Fällen, in denen die Kommission durch Beschluss feststellt, dass kein angemessenes Datenschutz-Niveau gegeben ist, die Datenübermittlung automatisch verboten ist, so dass es keines weiteren Umsetzungsaktes durch die Aufsichtsbehörde bedarf.

Ferner muss klargestellt werden, ob die Formulierung „unbeschadet der Art. 42–44“ bedeutet, dass bei einem Negativ-Beschluss gleichwohl Datenübermittlungen nach allen diesen Vorschriften vorgenommen werden können. Insbesondere die Vorschriften des Art. 41 (6) und des Art. 42 (1) erscheinen in dieser Frage widersprüchlich.

Zu Art. 42:
Da die Genehmigungsfähigkeit der Datenflüsse von vornherein fraglich ist, wenn keine geeigneten Garantien vorliegen, ist der Anwendungsbereich der Regelung des Art. 42 (5) unklar (Auffangtatbestand?). Deshalb sollte der Absatz 5 (bis auf den letzten Satz) entweder gestrichen oder um die genehmigungspflichtigen Fälle präzisiert werden.

Zu Art. 43:
In Art. 43 (1) sollte die Rechtsfolge der Genehmigung der BCR durch die Aufsichtsbehörde explizit aufgenommen werden, z. B. durch folgenden Satz 2: „In diesem Fall gilt die Genehmigung in der gesamten EU.“

Die in Art. 43 (3) genannten Kriterien und Anforderungen an BCR sollten nicht von der Kommission, sondern ausschließlich von dem Europäischen Datenschutzausschuss festgelegt werden.

Zu Art. 44:
Es sollte eine Klausel zum Umgang mit Aufforderungen zur Datenübermittlung durch Gerichte oder Behörden aus Drittstaaten eingefügt werden. Eine (interne) Vorversion des Vorschlags der Kommission beinhaltete eine solche explizite Klausel. Derartige Aufforderungen sollten hiernach grundsätzlich unbeachtlich sein und unter Genehmigungsvorbehalt durch zuständige nationale Behörden stehen. Die Konferenz fordert, dass Datentransfers grund-

sätzlich nur auf der Basis gegenseitiger Rechtshilfeabkommen (Mutual Legal Assistance Treaties, MLATs) zulässig sind.

In Art. 44 (1) müssen bei sensitiven Daten zusätzlich zur informierten Einwilligung geeignete Garantien vorgesehen werden, weil sonst zwar die Datenübermittlung nach Art. 44 (1) lit. a) legitimiert ist, die Datenverarbeitung im Drittland aber keinen besonderen Anforderungen unterliegt. Das Wort „zugestimmt“ sollte durch „eingewilligt“ (entsprechend Art. 7) ersetzt werden.

Art. 44 (1) lit. d) darf nicht für den Datenaustausch „zwischen für die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten zuständigen Behörden“ gelten, wie Erwägungsgrund 87 es vorsieht. Dies würde im Widerspruch zum sachlichen Anwendungsbereich der Verordnung nach Art. 2 (2) lit. e) stehen. Deshalb sollten diese Fälle in Erwägungsgrund 87 gestrichen werden.

Der Anwendungsbereich des Art. 44 (1) lit. h) ist unklar. Insbesondere ist fraglich, ob es sich um einen Auffangtatbestand handeln soll. Die Regelung muss konkretisiert werden. In jedem Fall muss eine Abwägung der berechtigten Interessen des für die Verarbeitung Verantwortlichen mit den schutzwürdigen Interessen der betroffenen Person vorgesehen werden.

Die Anwendungsbereiche der Art. 44 (3), (4), (6) und (7) sind unklar und müssen konkretisiert werden.

Zu Art. 45:
Art. 45 (2) sollte dahingehend ergänzt werden, dass neben der Kommission auch die Aufsichtsbehörden die Förderung der Beziehungen zu Drittländern betreiben können, und zwar auch – und gerade – zu Drittländern ohne angemessenen Datenschutz.

Kapitel VI – Unabhängige Aufsichtsbehörden

Zu Art. 47 und 48:
Die Regelung zur völligen Unabhängigkeit der Aufsichtsbehörden in Art. 47 (1) ist grundsätzlich positiv zu werten. Es sollte allerdings überdacht werden, wie die Unabhängigkeit der Aufsichtsbehörden auch bei der Zusammenarbeit mit den anderen Aufsichtsbehörden, insbesondere im Rahmen des Kohärenzverfahrens, garantiert werden kann (Art. 46 (1) Satz 2).

Zu Art. 51:
Die Regelung des „One-Stop-Shops“ gemäß Art. 51 (2) ist nur praktikabel, wenn sie nicht im Sinne einer ausschließlichen Zuständigkeit, sondern im

Sinne einer „Federführung“ der Aufsichtsbehörde des Mitgliedstaates der Hauptniederlassung zu verstehen ist, falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter über mehrere Niederlassungen innerhalb der EU verfügt.

Der One-Stop-Shop-Grundsatz sollte dann nicht gelten, wenn es sich um einen Sachverhalt handelt, der im Schwerpunkt die Anwendung nationalen Datenschutzrechts eines Mitgliedstaats im Sinne des Kapitels IX betrifft, so dass es hier bei der allgemeinen Zuständigkeit nach Art. 51 (1) bleiben sollte.

Mangels eines einheitlichen Verwaltungsverfahrens-, Verwaltungsprozess- und Verwaltungsvollstreckungsrechts kann die Aufsichtsbehörde in anderen Mitgliedsstaaten grundsätzlich nicht selbst tätig werden. Derartige hoheitliche Maßnahmen sollten daher nur im Wege der Amtshilfe möglich sein. Diese Klarstellung ist auch im Hinblick auf Art. 55 (1) und (2) sowie Art. 63 notwendig.

Es sollte überprüft werden, ob die sich aus Erwägungsgrund 19 ergebende Einbeziehung rechtlich selbständiger Tochtergesellschaften in die One-Stop-Shop-Regelung tatsächlich erforderlich ist. Diese könnten aufgrund ihrer rechtlich selbständigen Handlungsfähigkeit auch getrennt betrachtet werden. Sofern eine Einbeziehung für erforderlich gehalten wird, sollte dies einschließlich einer Definition des Begriffs Tochtergesellschaft unmittelbar im Verordnungstext und nicht nur in einem Erwägungsgrund geregelt werden.

Zu Art. 52:
Ausgehend von dem Vorschlag, eine Regelung zu „Erziehung und Bildung“ aufzunehmen (s.o.), sollten auch die Aufgaben der Aufsichtsbehörden entsprechend erweitert werden. Die Konferenz schlägt für Art. 52 (2) daher folgenden Wortlaut vor:

„Jede Aufsichtsbehörde fördert die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten und über geeignete Maßnahmen zum eigenen Schutz. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder.“

Die in Art. 52 (6) vorgesehene Missbrauchsgebühr sollte gestrichen werden, da nach den Erfahrungen der deutschen Aufsichtsbehörden derartige Beschwerden äußerst selten vorkommen, so dass – auch im Hinblick auf den Verwaltungsaufwand – eine Erhebung von Gebühren unverhältnismäßig wäre.

Zu Art. 53:
Die Konferenz weist darauf hin, dass auch die EU-rechtlich gebotene Unabhängigkeit der Aufsichtsbehörden nur im Rahmen der jeweiligen verfassungsrechtlichen Staatsstrukturprinzipien bestehen kann (Art. 4 Abs. 2 EUV). Dies gilt insbesondere für deren Sanktionsbefugnisse und Sanktionspflichten.

Art. 53 (2) sollte auch den anlasslosen Zugang zu Geschäfts- und Diensträumen umfassen. Unklar ist, was in Art. 53 (3) mit der Formulierung, dass Verstöße gegen die Verordnung den Justizbehörden zur Kenntnis zu bringen sind, gemeint ist.

Zu Art. 54:
Art. 54 sollte gestrichen werden. Hilfsweise wird angeregt, die Aufsichtsbehörden lediglich zur Erstellung eines regelmäßigen Jahresberichts zu verpflichten, der der Öffentlichkeit (und damit automatisch dem nationalen Parlament, der Kommission, dem Europäischem Datenschutzausschuss u. a.) zugänglich gemacht werden muss.

Kapitel VII – Zusammenarbeit und Kohärenz

Zu Art. 55 und Art. 56:
In dem in Art. 55, 56 geregelten Verfahren der Amtshilfe und der Zusammenarbeit sollten die betroffenen Behörden grundsätzlich sowohl im Hinblick auf die rechtliche Bewertung eines Sachverhalts als auch hinsichtlich erforderlicher aufsichtsbehördlicher Maßnahmen einvernehmlich zusammenwirken. Dies gilt insbesondere dann, wenn es sich um eine Maßnahme der federführenden Behörde i.S.d. Art. 51 (2) handelt, die von der Aufsichtsbehörde eines anderen Mitgliedstaates durchzuführen ist. Bei Divergenzen im Hinblick auf die Bewertung eines Sachverhalts oder die Vornahme aufsichtsbehördlicher Maßnahmen sollte der Europäische Datenschutzausschuss von den beteiligten Behörden angerufen werden können.

Die Gründe, aus denen Amtshilfeersuchen nach Art. 55 (4) abgelehnt werden können, sind zu eng. Sie sollten auch zwingende Hinderungsgründe nach nationalem Recht (z. B. im Falle des Sozialgeheimnisses) umfassen.

In Fällen, in denen der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter zwar über mehrere Niederlassungen innerhalb der EU verfügt, es sich aber um einen rein nationalen Sachverhalt handelt, sollte es aus Gründen der Verfahrensökonomie ebenfalls bei der allgemeine Zuständigkeitsregelung des Art. 51 (1) bleiben. Anderenfalls würde die Abstimmung

mit der Hauptniederlassungsbehörde einen unverhältnismäßigen Verfahrensaufwand bedeuten. In diesen Fällen sind die Voraussetzungen der Art. 55, 56 (Betroffenheit von Personen in mehreren Mitgliedstaaten) nicht erfüllt.

Unbestimmt ist, was unter „Vorkehrungen für eine wirksame Zusammenarbeit“ in Art. 55 (1) und „praktische Aspekte spezifischer Kooperationsmaßnahmen“ in Art. 56 (4) zu verstehen ist. Die verfahrenstechnischen Aspekte der Amtshilfe und der Zusammenarbeit sollten in Art. 55, 56 klar formuliert werden.

Es muss sichergestellt sein, dass hinreichende Mittel bereitstehen, um die praktische Arbeit im Rahmen der Amtshilfeleistungen zu erleichtern (insbesondere im Hinblick auf Übersetzungsleistungen, ggfs. durch das Sekretariat des Datenschutzausschusses).

Die Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten betreffend „Form und Verfahren der Amtshilfe (...)“ in Art. 55 (10) sollte präzisiert und beschränkt werden. Das Verfahren der Amtshilfe sollte in der Verordnung, die Form der Amtshilfe und die Ausgestaltung des elektronischen Informationsaustausches im Sinne einer Standardisierung hingegen in einem Durchführungsrechtsakt geregelt werden.

Zu Art. 58:
Im Hinblick auf Art. 58 (2) lit. a) sollte klargestellt werden, ob hiervon ausschließlich der Fall des Art. 3 (2) lit. a), b) umfasst ist, oder ob auch Fälle ohne Drittlandbezug dem Kohärenzverfahren unterfallen sollen. Ansonsten würden unübersehbar viele Fälle der Kohärenz unterfallen (z. B. Versandhandel innerhalb der EU).

Zu Art. 59 – Art. 63:
Die Kompetenzen der Kommission im Verhältnis zum unabhängigen Datenschutzausschuss sowie in Bezug auf das Kohärenzverfahren (Art. 59–63) sind abzulehnen. Dies gilt insbesondere im Hinblick auf die umfassenden Informationspflichten des Ausschusses gegenüber der Kommission und die Befugnis der Kommission zur Aufforderung der Aussetzung aufsichtsbehördlicher Maßnahmen. Gleiches gilt hinsichtlich der Ermächtigung der Kommission zum Erlass von Durchführungsrechtsakten über die „ordnungsgemäße Anwendung“ der Verordnung aus Anlass eines aufsichtsbehördlichen Einzelfalles und von „sofort geltenden Durchführungsrechtsakten“ in Fällen „äußerster Dringlichkeit“. Diese Kompetenzen der Kommission sind mit Art. 8 (3) Grundrechtecharta und 16 (2) Satz 2 AEUV nicht vereinbar, weil die Einhaltung des EU-Datenschutzes unabhängigen Auf-

sichtsbehörden übertragen ist. Auf der Ebene der Mitgliedstaaten soll die Datenschutzkontrolle völlig unabhängig von jeglichem Einfluss erfolgen. Daher ist es widersprüchlich, wenn für die Kommission mit ihren unterschiedlichsten Aufgaben, auch solchen, die in einem Spannungsverhältnis zum Datenschutz stehen, jene Maßstäbe keine Geltung haben sollen.

Über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, sollte als Folge der Unabhängigkeit der Aufsichtsbehörden – statt der Kommission – ausschließlich der Datenschutzausschuss entscheiden. Im Hinblick auf den personellen, sächlichen und zeitlichen mit dem Kohärenzverfahren verbundenen Aufwand sollte dessen Anwendungsbereich beschränkt werden. Es wird wesentlich im Interesse der Funktionsfähigkeit des Kohärenzverfahrens und eines europaweit wirksamen Datenschutzes darauf ankommen, entsprechende Fallgruppen zu definieren. Nicht alle datenschutzrechtlichen Fragen, die auch in anderen Mitgliedstaaten der EU auftauchen können, bedürfen einer Behandlung im Kohärenzverfahren. Für dieses eignen sich insbesondere:

- Fragen des Drittstaatentransfers
- BCR mit mitgliedstaatenübergreifendem Bezug
- Konstellationen, in denen unterschiedliche Auffassungen zwischen einer nach dem One-Stop-Shop-Prinzip zuständigen Aufsichtsbehörde und einer anderen Aufsichtsbehörde nicht zu einem einvernehmlichen Ergebnis führen
- Fälle von grundsätzlicher Bedeutung für den Datenschutz in der EU, insbesondere bei einer Datenverarbeitung außerhalb der EU, falls alle Mitgliedstaaten betroffen sind und es nicht allein einer unternehmens- oder konzerninternen Verteilung von Verantwortlichkeiten überlassen bleiben kann, die verantwortliche Behörde in Europa festzulegen.

Es sollte darüber hinaus den Aufsichtsbehörden möglich sein, Fragen von sich aus an den Europäischen Datenschutzausschuss heranzutragen. Es ist zu erwägen, ob der Ausschuss in Fällen, in denen eine Aufsichtsbehörde von der Stellungnahme des Ausschusses abzuweichen beabsichtigt, eine verbindliche Stellungnahme annehmen kann, für die ein höheres Abstimmungsquorum als die einfache Mehrheit der Mitglieder zu fordern wäre.

Die Vollstreckbarkeit von Entscheidungen anderer Aufsichtsbehörden nach Art. 63 sollte unter dem Vorbehalt stehen, dass es sich hierbei um rechtmäßige Entscheidungen der nach Art. 51 zuständigen Aufsichtsbehörde handelt, die unter Beachtung der Vorschriften des Kapitel VII (Amtshilfe, Zusammenarbeit, Kohärenz) getroffen wurden.

Zu Art. 64:
Die umfassende Informationspflicht über alle Tätigkeiten des unabhängigen Ausschusses gegenüber der Kommission nach Art. 64 (4) ist unangemessen.

Zu Art. 66:
Die Streichung der in Art. 30 (1) lit. d) RL 95/46 ausdrücklich enthaltenen Befugnis zur Abgabe von Stellungnahmen zu Verhaltensregeln auf EU-Ebene wird abgelehnt. Der Ausschuss sollte ebenfalls bei der Entwicklung von Zertifizierungsverfahren mitwirken und auch, entsprechend dem jetzigen Art. 30 (1) lit. b) RL 95/46, Stellung nehmen können zum Schutzniveau in der EU und in Drittstaaten.

Es ist abzulehnen, dass die bisherige Kompetenz der Art. 29-Gruppe gemäß Art. 30 (3) RL 95/46/EG, „von sich aus Empfehlungen zu allen Fragen" abzugeben, „die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen", nach Art. 66 (1) lit. a) unter der einschränkenden Zweckbestimmung der Beratung der Kommission stehen soll.

Über die in Art. 66 genannten Kompetenzen hinaus sollte dem Ausschuss ein Stellungnahmerecht insbesondere zu Entwürfen der Kommission für delegierte Rechtsakte zukommen. Auf diesem Wege könnten die Expertise und die Kompetenz der Datenschutzbehörden in diesen Bereich eingebracht und gewahrt werden. Zudem würde hierdurch die Transparenz des Delegations- und Komitologieverfahrens erhöht.

Zu Art. 69:
Art. 69 (1) Satz 2 sollte gestrichen werden. Vorsitz- und Stellvertreterposten des Ausschusses sollten ausschließlich durch eine Wahl besetzt werden. Weshalb dem Europäischen Datenschutzbeauftragten zumindest die Funktion eines Stellvertreters zustehen soll, erscheint nicht nachvollziehbar, zumal die Verordnung in der derzeitigen Entwurfsfassung nicht für Organe und Ämter der EU gilt.

Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen

Zu Art. 73 bis Art. 79:
Es ist sicherzustellen, dass durch den neuen Rechtsrahmen auch ein EU-weit wirksamer Rechtsschutz für die Betroffenen gewährleistet wird. Die in Kapitel VIII vorgesehenen Regelungen sind unklar gefasst und erfüllen diese Voraussetzungen nicht.

Länderübergreifende Klagen durch Aufsichtsbehörden im Namen Betroffener nach Art. 74 (4) gegen Aufsichtsbehörden anderer Mitgliedsstaaten können zu gegenseitigen Kontrollen der Aufsichtsbehörden führen, die im Gegensatz zum sonst geregelten Zusammenarbeitsgebot stehen würden. Es wären Klagen möglich, die der eigenen Rechtsauffassung der Aufsichtsbehörden zuwiderliefen.

Kapitel IX – Vorschriften für besondere Datenverarbeitungssituationen

Zu Art. 80 bis Art. 85:
Die Art. 81, 82 und 84 eröffnen den Mitgliedsstaaten die Befugnis, eigene Regelungen „in den Grenzen dieser Verordnung“ zu treffen. Entscheidend ist, dass damit nicht nur Konkretisierungen auf der Ebene des durch die Verordnung geregelten Datenschutzniveaus möglich sind, sondern dass durch nationalstaatliche Regelungen im Interesse des Datenschutzes weitergehende Anforderungen normiert werden können. Es sollte eine ausdrückliche Klarstellung im Verordnungstext in diesem Sinne erfolgen. Eine solche Regelung müsste mit den unter Art. 6 und Art. 21 vorgeschlagenen Öffnungsklauseln für mitgliedsstaatliches Recht abgestimmt werden.

Soweit in den Art. 81 (3) und 82 (3) auf die Möglichkeit für die Kommission verwiesen wird, delegierte Rechtsakte zu erlassen, ist deren Geltung auf die Mitgliedstaaten zu beschränken, die keinen Gebrauch von der Möglichkeit gemacht haben, die betreffenden Sachbereiche selbst zu regeln. Anderenfalls würde sich der Rechtsakt selbst in Widerspruch setzen. Wenn die Mitgliedstaaten die Ermächtigung bekommen, diese Bereiche selbst zu regeln, ist nicht nachvollziehbar, warum der Kommission dennoch weitreichende Regelungskompetenzen zur Konkretisierung eingeräumt werden sollen. Diese Konkretisierungen sollten dann konsequenterweise unmittelbar von den Mitgliedstaaten selbst vorgenommen werden können.

Gesundheitsdaten dürfen nach Art. 81 (2) unter den gleichen Voraussetzungen zu historischen oder statistischen Zwecken sowie zu wissenschaftlichen Zwecken verarbeitet werden wie sonstige personenbezogene Daten. Gesundheitsdaten sollten aber auch in diesem Zusammenhang stärker geschützt werden.

Anders als die Art. 80 bis 82 sieht der Art. 83 keine Ermächtigung für die Mitgliedsstaaten vor. Die Vorschrift würde also unmittelbar geltendes Recht werden. Die Konferenz erwartet hier – ebenso wie bereits bei Art. 6 (3) ausgeführt – dass das ausdifferenzierte nationale Statistikrecht und dessen vielfach strengere Vorgaben (im Vergleich zum allgemeinen Datenschutzrecht) weiterhin bestehen bleiben können. Dies sollte in Art. 83 klargestellt werden.

In Art. 85 sollte klargestellt werden, dass sich der Vorbehalt zugunsten kirchlicher Regelungen auf die Bereiche beschränkt, die von Art. 17 AEUV erfasst werden (vgl. Erwägungsgrund 128).

Kapitel X – Delegierte Rechtsakte und Durchführungsrechtsakte

Zu Art. 86 und Art. 87:
Im Hinblick auf die Rechtssicherheit sollten die Delegationsermächtigungen nach Art. 86 auf ein Mindestmaß reduziert werden. Nach Auffassung der Konferenz sind, wie bereits ausgeführt, alle wesentlichen materiellen Fragen in der Verordnung selbst bzw. durch Gesetze der Mitgliedstaaten zu regeln.

Hinsichtlich der verbleibenden Delegationsermächtigungen sollte in die Verordnung eine Verpflichtung der Kommission zur Konsultation des Europäischen Datenschutzausschusses vor dem Erlass delegierter Rechtsakte aufgenommen werden.

Anhang: Fehler und Übersetzungsfehler

In Art. 6 (1) lit. c) sollte in der deutschen Übersetzung das Wort „gesetzlichen“ durch das Wort „rechtlichen“ ersetzt werden, um auch – wie bisher in Art. 7 lit. c) der RL 95/46/EG – untergesetzliche Normen mit einzubeziehen. Der englische Wortlaut („legal obligation“) ist in beiden Vorschriften identisch.

In Art. 26 (1) sollte „...dass die betreffenden technischen und organisatorischen Maßnahmen... “ durch „...dass geeignete technische und organisatorische Maßnahmen...“ ersetzt werden.

In Art. 26 (2) lit. f) sollte „... den Auftragsverarbeiter ...“ durch „... den für die Verarbeitung Verantwortlichen...“ ersetzt werden.

In Art. 30 (3) muss es im letzten Satz anstatt „Art. 4“ „Abs. 4“ heißen.

In den Art. 11 (1), Art. 22 (1), Art. 37 (1) lit. b) und Art. 79 (6) lit. e) sollte anstatt „Strategie“ eine zutreffendere Übersetzung für „policy” gefunden werden.

8.2
Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdekkung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

Ungeachtet der Frage, ob sich die Kompetenz der EU zum Erlass einer Richtlinie auf Basis von Art. 16 Abs. 2 Satz 1 AEUV im Hinblick auf das Prinzip der begrenzten Einzelermächtigung und das Subsidiaritätsprinzip auch auf rein innerstaatliche Datenverarbeitungsvorgänge im Bereich der Gefahrenabwehr, der Strafverfolgung und des Strafvollzugs erstreckt, bewertet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Konferenz) den Richtlinienentwurf wie folgt:

Zielsetzung der Richtlinie

Die Richtlinie sollte durch Mindeststandards für die Mitgliedstaaten ein möglichst hohes Datenschutzniveau festschreiben. Den Mitgliedstaaten sollte die Möglichkeit verbleiben, in ihrem nationalen Recht über die Richtlinie hinausgehende datenschutzfreundlichere Regelungen zu treffen. Diese grundsätzliche Weichenstellung sollte in der Richtlinie selbst vorgenommen werden.

Eine solche Klarstellung würde nicht nur die durch die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) entwickelten Datenschutzgrundsätze wahren (z. B. Rechtsprechung zum Kernbereich der privaten Lebensgestaltung), sondern es darüber hinaus den nationalen Verfassungsgerichten ermöglichen, den Grundrechtsschutz in Zusammenarbeit mit dem Europäischen Gerichtshof weiterzuentwickeln.

Ohne entsprechende Festlegungen in der Richtlinie bestünde die Gefahr, dass grundrechtswahrende nationale Regelungen angesichts der Vorgaben der Richtlinie (die Gewährleistung des Datenschutzes und Sicherstellung des Datenaustauschs zwischen den Mitgliedstaaten gemäß Art. 1 (2) lit. b)) im Sinne einer Vollharmonisierung als richtlinienwidrig ausgelegt werden. Eine entsprechende Auslegung wäre vor dem Hintergrund der Rechtsprechung des Europäischen Gerichtshofs für den Bereich der geltenden Datenschutzrichtlinie 95/46/EG keineswegs ausgeschlossen und hätte unvertretbare Konsequenzen, etwa im Hinblick auf die im Strafprozessund im Polizeirecht enthaltenen Schutzvorkehrungen für die Rechte der Betroffenen.

Zu den einzelnen Bestimmungen wird folgendermaßen Stellung genommen:

Kapitel I – Allgemeine Bestimmungen

Anwendungsbereich (Art. 1–2)

Die Richtlinie ist gemäß Art. 2 (1) sachlich nur anwendbar, wenn eine „zuständige Behörde“ zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung personenbezogene Daten verarbeitet. Nicht erfasst sind damit Aufgaben im Bereich der Abwehr von Gefahren, die nicht der Abwehr von Straftaten dient (Beispiel: Fahndung nach Vermissten ohne Bezug auf das Vorliegen einer Straftat oder nach Strafunmündigen). Inwieweit andere Aufgaben im Bereich der Grenzkontrolle, des Zolls oder des Aufenthaltsrechts, die je nach der Tradition des Mitgliedstaates als eine polizeiliche Aufgabe verstanden werden, ebenfalls in den Anwendungsbereich der Richtlinie fallen, dürfte innerhalb der Mitgliedstaaten der EU durchaus unterschiedlich beurteilt werden. Nach Auffassung der Konferenz sollte vermieden werden, dass dieselbe polizeiliche Tätigkeit in einem Mitgliedstaat der Verordnung und in einem anderen Mitgliedstaat der Richtlinie unterfällt. Für die deutschen Polizeibehörden dürfte aus der vorgesehenen Bestimmung der Anwendungsbereiche von Datenschutz-Grundverordnung und Richtlinie folgen, dass sie in ihrem heutigen Aufgabenbereich sowohl die Datenschutz-Grundverordnung als auch die Richtlinie anzuwenden hätte. Zwar sind Abgrenzungsprobleme für Behörden mit polizeilichen Aufgaben nicht neu, wie etwa im Bereich von Zollverwaltung und Zollfahndung schon heute deutlich wird. Dennoch sollte der daraus folgenden Schwierigkeit der Abgrenzung nach Auffassung der Konferenz in erster Linie dadurch abgeholfen werden, weitest gehende Konsis-tenz zwischen der Datenschutz-Grundverordnung und der Richtlinie herzustellen.

Soweit der vorgeschlagene Rechtsakt Mindestanforderungen auch für die innerstaatliche Datenverarbeitung bei Polizeiund Strafverfolgungsbehörden umfasst, entspricht dies der schon vor einigen Jahren geäußerten Forderung der Konferenz. Angesichts der zunehmenden Verwirklichung des sog. Grundsatzes der Verfügbarkeit (Schwedische Initiative, Prümer Vertrag etc.), wonach ein in einem Mitgliedstaat erhobenes und verarbeitetes Datum auch den Polizeiund Strafverfolgungsbehörden eines anderen Mitgliedstaats zur Verfügung stehen soll, ist die Gewährleistung eines hohen Datenschutzniveaus in allen Mitgliedsstaaten erforderlich.

In Art. 2 (2) wird der Anwendungsbereich im Hinblick auf die Umstände der Verarbeitung bestimmt (automatisiert/nicht-automatisiert). Die Konferenz weist insofern darauf hin, dass der Wortlaut insbesondere auf der Grundlage der deutschen Fassung im Unklaren lässt, ob auch Akten von dem Anwendungsbereich umfasst sind. Im Ergebnis sollte die Richtlinie auf die Erhebung und die Verarbeitung personenbezogener Daten unabhängig von

dem Verarbeitungsmedium Anwendung finden. Eine Unterscheidung zwischen automatisierter bzw. nicht-automatisierter Verarbeitung einerseits und Verarbeitung in Akten anderseits ist nicht sachgerecht. Dies sollte klargestellt werden.

Nach Art. 2 (3) lit. a) soll die Richtlinie keine Anwendung finden, sofern personenbezogene Daten im Rahmen einer Tätigkeit verarbeitet werden, die nicht in den Anwendungsbereich des Unionsrechts fällt, etwa im Bereich der „nationalen Sicherheit". Die Konferenz hält es für erforderlich, den Begriff der „nationalen Sicherheit" zu präzisieren.

Der Richtlinienvorschlag nimmt auch die Organe und Einrichtungen der EU (u. a. Europol) vom Anwendungsbereich aus. Ungeachtet der Frage, durch welches Rechtsinstrument die Einrichtungen der EU erfasst werden sollten, wäre es aus Sicht der Konferenz nicht sachgerecht, sie von den Reformbemühungen um ein erhöhtes Datenschutzniveau auszunehmen. Wenn das Ziel der Datenschutzreform ist, einen umfassenden Rechtsrahmen auf einem hohen Datenschutzniveau in Europa zu schaffen, sollte dieser auch für die Einrichtungen der EU gelten. Zwar ist nachvollziehbar, dass die komplexen Regelungen der ehemaligen 3. Säule nur schwer in einem einzigen Gesetzespaket überarbeitet werden können. Es muss jedoch vermieden werden, dass für die Einrichtungen der EU andere Maßstäbe gelten als für die Polizei- und Justizbehörden der Mitgliedstaaten. Die Konferenz regt daher eine zügigere als in Art. 60 vorgesehene Anpassung der bestehenden Vorschriften an. Es ist zumindest zu prüfen, ob das mit der Richtlinie zu setzende Mindestniveau für alle Mitgliedstaaten auch für alle bestehenden Einrichtungen der EU zum Mindestniveau erklärt werden könnte.

Begriffsbestimmungen (Art. 3)

Zu den Begriffsbestimmungen ist im Rahmen der Richtlinie auf folgende Besonderheiten hinzuweisen:

Die Definition eines Kindes in Art. 3 (13) sollte gestrichen werden, da hieran im Entwurf einer Richtlinie keine spezifischen Verarbeitungsregeln bzw. Schutzgarantien geknüpft sind.

Im Hinblick auf die Regelung in Art. 7 lit. d) sollte eine Definition für den Begriff der „Gefahr für die öffentliche Sicherheit" aufgenommen werden.

Im Hinblick auf die Regelung in Art. 16 (3) sollte die Definition der „Einschränkung der Verarbeitung" in Art. 3 (4) überarbeitet werden.

Kapitel II – Grundsätze

Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten (Art. 4)

Wesentliche Grundlagen für den effektiven Schutz personenbezogener Daten sind u. a. enge Vorgaben für die Anforderungen an die Erforderlichkeit, die Zweckbindung und die Datensparsamkeit. Die Prinzipien der Datenverarbeitung gemäß Art. 4 bedürfen nach Auffassung der Konferenz insgesamt der Ergänzung und Präzisierung. Sie sollten grundsätzlich mehr Konsistenz zu den Prinzipien aufweisen, die in Art. 5 für die Datenschutz-Grundverordnung vorgeschlagen sind.

Die Regelung zur Zweckbindung in Art. 4 lit. b) enthält eine sehr offene Formulierung zur zweckändernden Weiterverarbeitung („nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise"). Sie sollte nach Auffassung der Konferenz strikter gefasst werden, insbesondere vor dem Hintergrund der unklaren und offenen Regelung des Art. 7 zur Rechtmäßigkeit der Verarbeitung. Es sollte klargestellt werden, dass Art. 4 und 7 im Zusammenwirken nicht so verstanden werden dürfen, dass ein einmal im Anwendungsbereich der Richtlinie für einen bestimmten Zweck erhobenes Datum ohne weitere gesetzliche Voraussetzungen für jeden anderen von der Richtlinie erfassten Zweck weiterverarbeitet werden darf.

Es sollte zudem eine engere Bestimmung des Grundsatzes der Erforderlichkeit in Art. 4 lit. c) formuliert werden. Die Bestimmungen „angemessen, sachlich relevant und nicht exzessiv" stellen nach Auffassung der Konferenz nur eine schwache Begrenzung für die Zulässigkeit der Datenverarbeitung dar. Dies gilt insbesondere deshalb, weil eine Beschränkung auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß, wie sie in Art. 5 lit. c) der Datenschutz-Grundverordnung vorgesehen ist, in dem Entwurf für die Richtlinie fehlt. Zudem wird die Datensparsamkeit nicht als Grundsatz aufgeführt. Es entsteht vielmehr der Eindruck, dass der Grundsatz der Erforderlichkeit kaum mehr beinhaltet als das Verbot exzessiver Datenverarbeitung.

Als weiterer Grundsatz sollte die Verpflichtung aufgenommen werden, dass bei der Verarbeitung personenbezogener Daten immer die technischen und organisatorischen Maßnahmen zum Datenschutz einzuhalten sind.

In sprachlicher Hinsicht sollte es in Art. 4 lit. a) auch in der deutschen Fassung „Fairness" bzw. „faires Verfahren" anstelle von „nach Treu und Glauben" heißen.

Unterscheidungen nach Kategorien von Betroffenen, Richtigkeit und Betroffenheit (Art. 5 und Art. 6)

Der Entwurf sieht vor, dass die Mitgliedstaaten bei der Verarbeitung personenbezogener Daten sowohl im Hinblick auf verschiedene Personenkategorien (Verdächtige, verurteilte Straftäter, Zeugen, Opfer etc., Art. 5) als auch im Hinblick auf die Richtigkeit und Zuverlässigkeit der Daten (Art. 6) – so weit wie möglich – Unterscheidungen vorzunehmen haben. Unterscheidungen nach anderen Kriterien, die für das deutsche Recht maßgeblich sind, sieht der Entwurf nicht vor. Dabei geht es beispielsweise um die Frage, ob der Eingriff den Kernbereich der persönlichen Lebensgestaltung berührt oder die Daten aus besonders einschneidenden Grundrechtseingriffen (Telekommunikationsgeheimnis, Unverletzlichkeit der Wohnung) herrühren. Damit das erreichte und nach deutschem Verfassungsrecht unabdingbare Schutzniveau erhalten bleiben kann, sollte die Richtlinie Mindeststandards und keine Obergrenzen für mitgliedstaatliche Regelungen regeln.

Sowohl in Art. 5 als auch in Art. 6 bleibt offen, was aus den vorzunehmenden Unterscheidungen bzw. was aus dem Unterlassen der Unterscheidung folgen soll. Die Konferenz befürwortet insbesondere engere Grenzen für die Verarbeitung von Daten zu bestimmten Personengruppen (z. B. Opfer oder Zeugen von Straftaten).

Rechtmäßigkeit der Verarbeitung (Art. 7)

Artikel 7 enthält die zentrale Vorschrift zur Bestimmung der Rechtmäßigkeit von Datenverarbeitungen. Dabei bedarf die in Art. 7 getroffene Unterscheidung zwischen lit. a), b), c) und d) nach Auffassung der Konferenz der weiteren Erläuterung.

Ebenfalls erläuterungsbedürftig ist das Zusammenwirken dieser Vorschrift mit den in Art. 4 aufgeführten Prinzipien der Datenverarbeitung, insbesondere im Hinblick auf den Grundsatz der Zweckbindung.

Die Konferenz begrüßt, dass eine Einwilligung als Legitimation für die Datenverarbeitung im Bereich der Richtlinie ausgeschlossen ist. Ihre Anwendung ist von der Konferenz wiederholt infrage gestellt worden, insbesondere dann, wenn dadurch die Grenzen der gesetzlichen Befugnisse erweitert werden sollen.

Kapitel III – Rechte der betroffenen Personen

Rechte der Betroffenen (Art. 10–17)

Umfangreiche Rechte der Betroffenen sind wesentlich für ein hohes Datenschutzniveau. Um den Richtlinienentwurf zu einer geeigneten Grundlage für

die Erweiterung der Betroffenenrechte in den Mitgliedstaaten zu machen, bedarf es einzelner Klarstellungen und Änderungen.

Besonderer Klärungsbedarf besteht im Hinblick auf Art. 17 i. V. m. Erwägungsgrund 82. Der Konferenz ist weder klar, in welchen Fällen Art. 17 anwendbar ist, noch, welche Folgen die Anwendbarkeit von Art. 17 hat. Die Auslegung wird zudem dadurch erschwert, dass die deutsche und die englische Fassung („Gerichtsbeschluss“ oder „Gerichtsdokument“/„judicial decision or record“) unterschiedliche Interpretationen nahe legen. Eine Klarstellung ist in dieser Frage von besonderer Bedeutung, weil davon letztlich abhängt, ob und inwieweit die Betroffenenrechte während des gesamten staatsanwaltlichen Ermittlungsverfahrens gelten.

Nach Auffassung der Konferenz sollten die in den Art. 11–16 gewährten Rechte grundsätzlich auch im Bereich des staatsanwaltlichen Ermittlungsverfahrens Anwendung finden. Mindeststandards bezüglich der Ausgestaltung der Betroffenenrechte zählen zu den zentralen Elementen eines hohen Datenschutzniveaus und müssen auch bei der Verarbeitung personenbezogener Daten durch Staatsanwaltschaften gelten.

Darüber hinaus sind die Möglichkeiten der Mitgliedstaaten, die Betroffenenrechte einzuschränken, zu weitgehend. Als nicht vertretbar sieht die Konferenz die Regelungen in Art. 11 (5) und Art. 13 (2) der Richtlinie an. Sie eröffnen dem Gesetzgeber die Möglichkeit, bei bestimmten Datenkategorien die Information bzw. die Auskunftserteilung an den Betroffenen per se auszuschließen, ohne dass eine Abwägung im Einzelfall erfolgen muss. Es sollte vielmehr in Art. 11 und 13 klargestellt werden, dass Einschränkungen stets nur nach Prüfung des Einzelfalls zulässig sind.

Es ist nachvollziehbar, dass die Information des Betroffenen bzw. sein Auskunftsrecht in bestimmten Fällen (zunächst) beschränkt werden muss. Die Beschränkungen müssen allerdings in der Richtlinie hinreichend konkret bestimmt werden. Insofern werfen die Art. 11 (4) und Art. 13 (1) erneut Fragen auf. Sie eröffnen einen zu weiten Spielraum für den nationalen Gesetzgeber, die Rechte der Betroffenen einzuschränken.

Die Information der betroffenen Person über die Erhebung personenbezogener Daten sollte zudem unverzüglich (d. h. ohne schuldhaftes Zögern) erfolgen. Die Angabe „innerhalb einer angemessenen Frist“ in Art. 11 (3) lit. b) ist insoweit zu unbestimmt.

In Art. 15 sollte klargestellt werden, ob unter einem „Korrigendum“ eine Richtigstellung zu verstehen ist.

Zudem sollte der Richtlinienentwurf dahingehend ergänzt werden, dass den Betroffenen in geeigneten Fällen neben dem Auskunftsrecht auch ein Akteneinsichtsrecht zu gewähren ist.

Kapitel IV – Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Vorschriften über die Verarbeitung Verantwortlicher und Auftragsverarbeiter (Art. 18–32)

Die Konferenz bedauert, dass die Vorschrift zu „Datenschutz durch Technik“ („privacy by design“) in Art. 19 keine konkreten Vorgaben macht und so zu einem reinen Programmsatz ohne praktische Auswirkungen werden könnte. Zudem könnte die ausdrückliche Bezugnahme auf die Berücksichtigung der entstehenden Kosten in der vorliegenden Formulierung zu einem Einfallstor für das Unterlassen von Maßnahmen zur datenschutzfreundlichen Technikgestaltung werden.

Bei verschiedenen Vorschriften des Kapitels IV sieht die Konferenz einen weiteren Klarstellungsbedarf. Dazu gehört das Verhältnis der „unabhängigen internen oder externen Prüfer“ zum Datenschutzbeauftragten und zu den Aufsichtsbehörden nach Art. 18 (3). Dazu gehören ebenso die Regelungsgehalte der Art. 20 und 22 (z. B. hinsichtlich der Kontrollpflichten des Auftragnehmers) und das Verhältnis der Art. 20 und 21 zueinander.

Die in Art. 23 (2) formulierten Dokumentationspflichten sollten ergänzt werden durch eine Beschreibung der betroffenen Personengruppen, der diesbezüglichen Daten oder Datenkategorien und durch eine Festlegung von Regelfristen zur Datenlöschung.

Die Vorschriften über die Datensicherheit (Art. 27-29) sollten um Datenschutzzielbestimmungen ergänzt werden.

Die nach Art. 27 (2) erforderliche Risikobewertung ist nur als angemessene Sicherheitsmaßnahme zu bewerten, wenn eine kontinuierlich durchgeführte Risikobewertung bzw. Risikoanalyse gewährleistet ist. IT-Sicherheit erfordert in diesem Sinne ein konzeptionelles Herangehen sowie die Etablierung von IT-Sicherheits- und Datenschutzmanagementsystemen. Artikel 27 sollte daher durch die Forderung nach einem Sicherheitskonzept, welches Teil der Verfahrensdokumentation gemäß Art. 23 (2) werden muss, ergänzt werden.

Die in Art. 28 (5) enthaltene Delegation an die Kommission bedarf der Überprüfung. Die Kriterien und Anforderungen für die Feststellung einer Verletzung des Schutzes personenbezogener Daten sind so wesentlich, dass sie im Rechtsakt selbst bestimmt werden sollten.

Die in Art. 29 (3) geregelte Pflicht zur Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten sollte nicht davon abhängig gemacht werden, ob die verantwortliche Stelle ausreichende technische Schutzmaßnahmen getroffen hat.

Bei den Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters sollten in der Richtlinie entsprechend den Vorgaben der Datenschutz-Grundverordnung nicht nur die „vorherige Zurateziehung“ („prior consultation“) der Datenschutzbehörden, sondern auch eine Folgenabschätzung („privacy impact assessment“) durch die jeweilige Stelle vorgesehen werden.

Bei den Anforderungen an den Datenschutzbeauftragten ist der Begriff der „Zuverlässigkeit“ aufzunehmen (Art. 30 (2)). Darüber hinaus sollte eine Verschwiegenheitspflicht des Datenschutzbeauftragten festgelegt werden sowie die Aufnahme eines Benachteiligungsverbots, eines Kündigungsschutzes und die Möglichkeit der Teilnahme an Fort- und Weiterbildungsveranstaltungen.

In Art. 32 der Richtlinie sollte zudem klargestellt werden, dass die Aufgaben des Datenschutzbeauftragten die verantwortliche Stelle nicht von ihren eigenen Pflichten entbindet, d. h., dass sie sich nicht unter Verweis auf die Nicht- oder Schlechterfüllung durch den Datenschutzbeauftragten exkulpieren kann. Insbesondere Art. 32 lit. a), lit. d) und lit. h) sind insoweit missverständlich.

Kapitel V – Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Die Vorschriften zu den Übermittlungen von personenbezogenen Daten in Drittstaaten sind in einem wichtigen Punkt widersprüchlich und sind insgesamt zu weit gefasst.

Im Hinblick auf die Übermittlung von personenbezogenen Daten an internationale Organisationen sollte in Art. 33 klargestellt werden, dass nur solche internationale Organisationen gemeint sind, die einen Bezug zu Fragen der inneren Sicherheit aufweisen. Dies gilt ebenso für die sog. Weiterübermittlungen („onward transfers“), die in einer spezifischen Vorschrift geregelt werden sollten.

Es fehlt eine Klarstellung, dass bestehende Angemessenheitsbeschlüsse, die auf der Grundlage der RL 95/46/EG ergangen sind, für den JI-Bereich nicht gelten.

Entsprechend den bisherigen Regelungen in der Richtlinie 95/46/EG enthält der Vorschlag die Einführung von Angemessenheitsbeschlüssen zum Datenschutzniveau von Drittstaaten. Sofern die Kommission einen solchen Beschluss gefasst hat, ist die Angemessenheit des Datenschutzniveaus verbindlich festgestellt. Es bedarf allerdings der Klarstellung, dass bei Negativbeschlüssen der Kommission nach Art. 34 (5) Datenübermittlungen nur

auf der Grundlage der Ausnahmen nach Art. 36, nicht aber auf der Grundlage des Art. 35 (1) vorgenommen werden dürfen. Die Vorschriften der Art. 34 (5) und Art. 35 (1) sind in dieser Frage widersprüchlich.

Die Möglichkeit der Mitgliedstaaten, personenbezogene Daten auf der Grundlage einer eigenen Einschätzung in Drittstaaten zu übermitteln, ist im Hinblick auf Art. 35 (1) lit. b) zu unbestimmt gefasst. Jedenfalls ist eine Bezugnahme auf Art. 34 (2) lit. a) vorzunehmen, der die bei der Angemessenheitsentscheidung zu berücksichtigenden Faktoren aufführt. Darüber hinaus sollte die Einbeziehung des Auftragsverarbeiters in Art. 35 gestrichen werden.

Die Konferenz hält die Ausnahmevorschrift des Art. 36 für zu weit gefasst. Dies gilt insbesondere für lit. d) und lit. e), nach denen kaum noch eine Übermittlung denkbar ist, die nicht auf eine der Ausnahmeklauseln gestützt werden könnte. Die Konferenz regt daher im Hinblick auf die in den lit. a) bis e) enthaltenen Ausnahmevorschriften die Streichung der lit. d) und e) an. Zudem sollte in Art. 36 eine Dokumentationspflicht entsprechend des Art. 35 (2) aufgenommen werden.

Artikel 37 bezieht sich auf die Übermittlung von Daten in Drittstaaten, für die auf nationaler Ebene besondere Verwendungsbeschränkungen gelten. Insofern seien alle „vertretbaren Vorkehrungen“ zu treffen, um diese Beschränkungen einzuhalten. Dies ist nach Auffassung der Konferenz zu unbestimmt und sollte daher, insbesondere auch bezüglich der zu ergreifenden technischen und organisatorischen Maßnahmen, konkretisiert werden. Die Vorschrift sollte zudem um die Verpflichtung ergänzt werden, den Empfänger der übermittelten Daten über Berichtigungs- und Löschungsansprüche zu informieren.

Artikel 37 ist nicht auf Übermittlungen zwischen den Mitgliedstaaten anwendbar. Daher muss die Richtlinie an geeigneter Stelle klarstellen, dass die in den nationalen Vorschriften der Mitgliedstaaten enthaltenen Verwendungsbeschränkungen und Mitteilungspflichten auch für Datentransfers innerhalb der Europäischen Union gelten. Die Richtlinie sollte die Daten empfangenden Mitgliedstaaten verpflichten, die Verwendungsbeschränkungen des übermittelnden Mitgliedstaates umzusetzen.

Schließlich sollte die Regelung des Art. 38 dahingehend ergänzt werden, dass neben der Kommission auch die Aufsichtsbehörden die Förderung der Beziehungen zu Drittländern betreiben können, und zwar auch – und gerade – zu Drittländern ohne angemessenen Schutz.

Kapitel VI und VII – Unabhängige Aufsichtsbehörden und Zusammenarbeit

Die Regelungen zur Unabhängigkeit sind grundsätzlich positiv zu werten. In Art. 39 (1) Satz 2 sollte allerdings klargestellt werden, dass die Unabhängigkeit der Aufsichtsbehörden auch bei der Zusammenarbeit mit der Kommission sowie den anderen Aufsichtsbehörden garantiert sein muss.

Eine im Bereich von Polizei und Justiz zentrale Frage betrifft die Zuständigkeit von Datenschutzbehörden bei der Datenverarbeitung durch Gerichte im Rahmen ihrer gerichtlichen Tätigkeiten. Im Text von Art. 44 (2) sollte unmissverständlich klargestellt werden, dass der Ausschluss der Zuständigkeit der Aufsichtsbehörden sich nicht auf Akte der Exekutive bezieht, die nach nationalem Recht unter Beteiligung eines Richters zustande gekommen sind (in Deutschland etwa im Hinblick auf Maßnahmen der Strafverfolgungsbehörden, die einem Richtervorbehalt unterlegen haben).

In Art. 45 (4) sollte verdeutlicht werden, dass die Nutzung eines Formulars für Beschwerden nicht verbindlich ist und technische Schutzvorkehrungen im Sinne des Art. 27 zu treffen sind.

Die Konferenz begrüßt, dass Art. 46, insbesondere lit. b), die bisherige Ausgestaltung der aufsichtsbehördlichen Befugnisse im deutschen Recht auch weiterhin zulässt, ohne Änderungen für die Zukunft auszuschließen, wie die Verleihung von Anordnungskompetenzen. Die Frage der Ausgestaltung der Befugnisse für die Aufsichtsbehörden ist von besonderer Bedeutung und steht in engem Zusammenhang mit der Möglichkeit der gerichtlichen Auseinandersetzung zwischen der Aufsichtsbehörde und der beaufsichtigten Stelle und/oder dem Betroffenen (vgl. Art. 51).

Zur Vermeidung jeden Zweifels, der aus dem Vergleich mit der Datenschutz-Grundverordung resultieren könnte, sollte gleichfalls in der Richtlinie ausdrücklich klargestellt werden, dass Art. 46 auch den anlasslosen Zugang zu Diensträumen umfasst.

Zuletzt muss sichergestellt sein, dass hinreichende Mittel bereitstehen, um die praktische Arbeit im Rahmen der Amtshilfeleistungen zu erleichtern (insbesondere im Hinblick auf Übersetzungsleistungen, ggf. durch das Sekretariat des Datenschutzausschusses). Die Amtshilfeverpflichtung nach Art. 48 sollte durch Ausnahmevorschriften, etwa zum Schutz von Geheimhaltungsvorschriften, ergänzt werden.

Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen

Die Erweiterung der Vertretungsbefugnis für Einrichtungen, Organisationen und Verbände gemäß Art. 50 (2) ist grundsätzlich zu begrüßen.

In Art. 51 (1) sollte klargestellt werden, dass gerichtliche Rechtsbehelfe nur gegen Entscheidungen der Aufsichtsbehörde mit Regelungswirkung gegenüber Bürgern und anderen Behörden möglich sind.

In Art. 51 (2) sollte klargestellt werden, dass die vorgesehene Klagemöglichkeit gegen die Aufsichtsbehörde auf die Untätigkeit der Aufsichtsbehörde begrenzt ist. Die unklare Formulierung „wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist“ sollte gestrichen werden.

Die Regelung über gemeinsame Vorschriften zum Gerichtsverfahren (Art. 53) sieht in Absatz 2 vor, dass jede Aufsichtsbehörde das Recht hat (im Englischen: „shall have the right“), Klage zur Durchsetzung der in der Richtlinie enthaltenen Rechte zu erheben. Die Konferenz spricht sich dafür aus, Art. 53 (2) so zu ändern, dass die Mitgliedstaaten eine entsprechende Berechtigung der Aufsichtsbehörden vorsehen können, jedoch nicht hierzu verpflichtet sind.

Die in Art. 54 (2) der Richtlinie vorgesehene Einführung einer gesamtschuldnerischen Haftung aller an der Verarbeitung beteiligten Stellen wird von der Konferenz als sinnvoll angesehen und daher begrüßt.

Kapitel IX und X – Delegierte Rechtsakte und Durchführungsbestimmungen, Schlussbestimmungen

Die Konferenz begrüßt, dass internationale Übereinkommen, die von den Mitgliedstaaten vor Inkrafttreten der Richtlinie geschlossen worden sind, innerhalb von fünf Jahren überarbeitet werden sollen, um sie in Übereinstimmung mit den Vorgaben der Richtlinie zu bringen (Art. 60). Es sollte klargestellt werden, dass die Richtlinie insofern nur als ein Mindestniveau anzusehen ist und in keinem Fall eine Herabstufung bestehender höherer Standards zu erfolgen hat. Die bisher fehlende Anwendbarkeit der Richtlinie auf die Einrichtungen der EU darf nicht dazu führen, dass die zwischen der EU und Drittstaaten vereinbarten Abkommen (wie etwa das TFTP-Abkommen oder das PNR-Abkommen) von dieser Regelung ausgenommen sind.

Entsprechend der allgemeinen Forderung der Konferenz sollte eine substanziellere Vorschrift für die Evaluierung der Richtlinie aufgenommen werden, als dies gegenwärtig in Art. 61 (3) vorgesehen ist. Die Evaluierungsklausel sollte auch die Hinzuziehung von externem Sachverstand enthalten.

8.3
Kurzfassung der Stellungnahme des Hessischen Datenschutzbeauftragten vom 17. August 2012 zum Entwurf der EU VO über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, COM (2012) 238 final

Bei allen positiven Ansätzen des VO-Entwurfes gibt es zwei wesentliche Kritikpunkte:

1. Die eID-Funktion es nPA mit ihren richtungweisenden und datenschutzgerechten Funktionalitäten dürfte nach der VO in Europa nicht weiter genutzt werden.
2. **ArchiSig und ArchiSafe**, die fortschrittlichen deutschen Konzepte zur elektronischen Beweissicherung und Archivierung, die mit erheblichem Aufwand im Auftrag der Bundesregierung entwickelt wurden, würden nach den Vorgaben der EU Verordnung ihre Beweiskraft verlieren.

Die wichtigsten weiteren Forderungen des HDSB im Überblick:

I. Grundsätzliches

– Die Verordnung selbst muss Mindestanforderungen an Datenschutz, Datensicherheit, Interoperabilität und technische Standards festlegen. Eine Regelungskompetenz durch die Kommission allein ist abzulehnen.
– Das hohe deutsche Niveau in Bezug auf Datenschutz und Datensicherheit muss aufrecht erhalten werden.
– Die Schaffung einer zentralen Datenbank für die Online-Authentisierung bzw. Identifizierung muss vermieden werden.
– Es müssen Regelungen getroffen werden, welche Befugnisse die Datenschutzbehörden neben den Aufsichtsbehörden gegenüber den Vertrauensdiensteanbietern im Falle von Rechtsverstößen haben.

II. Elektronische Identifizierungssysteme

– Datenschutzrechtliche Anforderungen (Verwendung von Pseudonymen, Datensparsamkeit, Zweckbindung, Erforderlichkeitsprüfung) sind für elektronische Identifizierungssysteme umzusetzen.
– Die Anforderungen dieses EU VO-Entwurfes an elektronische Identifizierungssysteme sollten so modifiziert werden, dass die eID-Funktion des neuen Personalausweises (nPA) sie erfüllt und notifiziert werden kann.
– Der Begriff Identifikationsdaten sollte so differenziert werden, dass eine datensparsame Verwendung grundsätzlich erfolgt.

III. Vertrauensdienste

- Die Authentifizierung muss eindeutig definiert werden, so dass eine klare, saubere Trennung der jeweiligen Funktionen der verschiedenen Vertrauensdienste erreicht wird.
- Qualifizierte Signaturen, Siegel und Zeitstempel sollten auf allen Ebenen (Zertifikatserstellung und Endanwender) qualifiziert sein. Andernfalls sind die mit Bundesmitteln entwickelten Verfahren ArchiSig und ArchiSafe nicht mehr nutzbar.
- Auch natürliche Personen müssen elektronische Siegel nutzen können. Siegel sind „technische Signaturen“: sie beinhalten weder eine Willenserklärung noch eine inhaltliche Zustimmung oder gar den Ersatz der manuellen Unterschrift.
- Eine Website-Authentifizierung muss auch für natürliche Personen möglich sein.
- Qualifizierte Signaturen, qualifizierte Siegel und qualifizierte Zeitstempel sind für eGovernment ausreichend. Darunterliegende Qualitäts-Niveaus (fortgeschritten, einfach) sind überflüssig; das Niveau „fortgeschritten“ kann weder automatisiert noch manuell geprüft werden. Deshalb ist es auch nicht sinnvoll.
- Signaturen, Siegel und Zeitstempel müssen auf Anwender- und Zertifikats-Ebene auf den Zeitpunkt der Erstellung geprüft werden.

8.4
Stellungnahme des Hessischen Datenschutzbeauftragten zum „Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“, COM (2012) 238 final

Vorbemerkungen

Wie bei der EU Datenschutz-Grundverordnung

- gibt es auch hier zu nahezu jedem Artikel Ermächtigungen der Kommission zu Durchführungsrechtsakten und zu delegierten Rechtsakten anstelle konkreter nachvollziehbarer Regelungen. Die behauptete Interoperabilität für eID, Authentisierung und Signatur ist ohne die im Entwurf fehlenden Konkretisierungen nicht erreicht. Ohne diese bedeutet die Zustimmung der EU-Länder eine Blanko-Unterschrift: die erforderliche Normenklarheit fehlt.

  Vorschlag:

  Analog zu den Anforderungen in den Anhängen I für „qualifizierte Zertifikate für elektronische Signaturen und qualifizierte Siegel“ und II für „qua-

lifizierte Signaturerstellungseinheiten“ sollten auch andere Anforderungen als Anhänge beschrieben werden. Sie können dann erforderlichenfalls – analog zu den Regelungen in Artikel 21 Absatz 4 und Artikel 22 Absatz 2 – durch Rechtsakte der Kommission präzisiert werden. Die Erforderlichkeit ist jeweils zu begründen.
– stellt sich auch hier die rechtliche Frage, ob sie nur für den zwischenstaatlichen Bereich oder auch innerstaatlich und hier insbesondere im behördlichen Bereich gelten soll
– gibt es eine Menge handwerklicher Fehler und wesentliche Übersetzungsfehler.

Diese VO soll die EU Signaturrichtlinie 1999/93/EG ersetzen. Damit gilt dann auch das deutsche Signaturgesetz in der vorliegenden Form nicht mehr.

Zusammenfassung wesentlicher Punkte:
Die Vorgaben, die zur Erreichung der Interoperabilität erforderlich sind, sollten direkt in die VO, ggf. in einen Anhang aufgenommen werden. Nur so ist die erforderliche Transparenz für die EU-Länder herstellbar.

Definitionen
– Die Identifikationsdaten sind weder konkret noch differenziert genug noch datenschutzgerecht definiert. Besondere Ausprägungen von Personenidentifikationsdaten, wie z. B. für Altersverifikation, Volljährigkeitsnachweis und Wohnortnachweis, sollten in Artikel 3 Absatz 1 definiert werden, um die Datensparsamkeit umzusetzen und die Beschränkung auf die jeweils erforderlichen Daten zu ermöglichen.
– Die verwendeten Begriffe sollten eindeutig sein und es erlauben, die verschiedenen Funktionen eID, Authentisierung und Signatur klar auseinander zu halten. Dies ist hier nicht der Fall. Die Definition der Authentifizierung bekommt hier zwei Bedeutungen, was zu Verwirrung führt. Nur der erste Teil der Definition „ist ein elektronischer Prozess, der die Validierung der elektronischen Identifizierung einer natürlichen oder juristischen Person ermöglicht“ sollte hier erhalten bleiben. Der zweite Teil sollte hier gestrichen werden: Denn „die Validierung des Ursprungs und der Unversehrtheit der Daten“ ist als elektronisches Siegel in Absatz 20 definiert. Sie wird auch von fortgeschrittenen und qualifizierten elektronischen Signaturen erfüllt, mit denen zusätzlich eine Willenserklärung abgegeben werden kann (FES) bzw. die handschriftliche Unterschrift auf einem Dokument ersetzt werden kann(QES).
– Die Definitionen der elektronischen Signatur und des elektronischen Siegels sollten sich – in Übereinstimmung mit den vielen Formulierungen in

der Begründung – ausschließlich auf elektronische Dokumente beziehen und nicht auf andere elektronische Daten.

- In die Definition des elektronischen Dokumentes sollte zusätzlich aufgenommen werden, wie sich das elektronische Dokument von anderen elektronischen Daten unterscheidet – z.B. als eigenständige Datei.
- Die Website- Authentifizierung ist im Entwurf nur für juristische Personen vorgesehen. Dies ist eine wesentliche, nicht nachvollziehbare Einschränkung. Viele Webseiten werden von natürlichen Personen betrieben.
- Auch natürliche Personen sollten siegeln können: also nur Quelle und Unversehrtheit eines Dokuments/einer Datei bestätigen, ohne dem Inhalt im Sinne einer Willenserklärung zuzustimmen.

Elektronische Identifizierung

- In diesem Kapitel fehlt ein Datenschutzartikel. Hier müssen Datenvermeidung und Datensparsamkeit sowie Pseudonymfunktionen verankert werden. Letztere werden in vielen Fällen ausreichen.
- Die eID des nPA erfüllt die Anforderungen dieses EU VO Entwurfes nicht.

Vertrauensdienste

- Datenschutz: Die Beschränkung der Verarbeitung personenbezogener Daten auf das Mindestmaß sollte nicht nur für die Vertrauensdiensteanbieter sondern auch für die akzeptierenden Instanzen und die Datenübermittlung an sie gelten.
- Die Anforderung der „alleinigen Kontrolle“ des Signaturschlüsselinhabers über die Mittel zur Signaturerstellung muss erhalten bleiben.
- Alle Tätigkeiten von qualifizierten Vertrauensdiensteanbietern sollten ausschließlich unter Verwendung von qualifizierten Signaturen und qualifizierten Siegeln erfolgen, die von der staatlichen Root gesiegelt sind. Der zusätzliche Aufwand hierfür ist vernachlässigbar.
- Alle Zertifikatssignaturen der qualifizierten Vertrauensdiensteanbieter müssen qualifiziert (statt fortgeschritten) sein, damit die Beweiskette funktioniert.
- Qualifizierte Zeitstempel sollten – auf allen Ebenen – wirklich qualifiziert sein. Die unzutreffende Bezeichnung im VO-Entwurf – die Zertifikate sind fortgeschritten signiert und der Zeitstempel selbst ist lediglich eine fortgeschrittene Signatur des (qualifizierten) Vertrauensdiensteanbieters – führt dazu, dass die Beweiswerterhaltung mit ArchiSig und ArchiSafe, die im Auftrag der Bundesregierung entwickelt wurden, unbrauchbar werden. Auch eine Beweiswerterhaltung außerhalb dieser Verfahren ist damit nicht machbar.

- Nicht nur qualifizierte elektronische Signaturen und Siegel, sondern alle, insbesondere auch fortgeschrittene Signaturen und Siegel, sollten auf den Zeitpunkt der Erstellung geprüft werden. Das ist sowohl für Willenserklärungen als auch für Dokumentsignaturen im Sinne der Siegel sachgerecht.
- Die Dienste zur Erhaltung des Beweiswertes qualifiziert signierter Dokumente sind nicht zutreffend formuliert. Sie müssen überarbeitet werden.
- Fortgeschrittene Signaturen und fortgeschrittene Siegel sollten generell aus dem Entwurf gestrichen werden:

  Zum einen gibt es keine Prüfverfahren – weder manuell noch automatisiert – für fortgeschrittene Signaturen oder Siegel.

  Zum anderen sind sie – wie die beiden folgenden Spiegelpunkte zeigen – überflüssig, falls (qualifizierte) Siegel auch für natürliche Personen zugelassen werden:
- Unterschiedliche Sicherheitsniveaus für Siegel sind überflüssig. Hier reichen qualifizierte Siegel aus, da es keine unterschiedlichen Rechtsfolgen wie bei der Signatur gibt.
- Auch bei der Signatur reicht die qualifizierte Signatur (mit Willenserklärung/als Unterschrift) aus:

  Das qualifizierte Siegel kann für natürliche und juristische Personen den Nachweis der Quelle und der Unversehrtheit eines Dokumentes/einer Datei übernehmen.

Zu den Artikeln im Einzelnen:
Anmerkung: Besonders wichtige Anmerkungen sind durch Unterstreichung des Artikels und ggf. des Absatzes hervorgehoben.

Kapitel I: Allgemeine Bestimmungen

Artikel 3, Absatz 1:
Die Identifizierungsdaten sind nicht – auch nicht als maximale Liste – festgelegt. Es gibt keine Prüfung bzw. Beschränkung auf die jeweils konkret erforderlichen Daten, wie sie das Bundesverwaltungsamt beim Antrag eines Anbieters zur Nutzung der eID-Funktion des nPA vornimmt.

Auch verschiedene Arten wie Altersverifikation, Volljährigkeitsnachweis, Wohnortnachweis werden nicht begrifflich unterschieden.

Absatz 4:
Im Interesse einer klaren, sauberen Trennung der Funktionen Identifikation und Authentisierung sollten die beiden Teile dieser Definition getrennt wer-

den. Nur der erste Fall sollte weiterhin als Authentifizierung bezeichnet werden. Der zweite Teil sollte hier gestrichen werden: Denn „die Validierung des Ursprungs und der Unversehrtheit der Daten“ ist als elektronisches Siegel in Absatz 20 definiert. Sie wird auch von fortgeschrittenen und qualifizierten elektronischen Signaturen erfüllt, mit denen zusätzlich eine Willenserklärung abgegeben werden kann (FES) bzw. die handschriftliche Unterschrift auf einem Dokument ersetzt werden kann (QES). Eine Vermischung der beiden Fälle führt zu Problemen: Die Bereiche Authentisierung und Siegel sowie fortgeschrittene Signatur und lassen sich dann nicht mehr auseinander halten. Da man nicht „ein bisschen unterschreiben“ kann, sollte die fortgeschrittene Signatur ganz entfallen. Damit wäre dann auch eine klare Abgrenzung aller Vertrauensfunktionen erreicht.

Artikel 3, Absatz 7c):
Diese Aufweichung der „alleinigen Kontrolle“ kann insbesondere für qualifizierte Signaturen wegen der Zurechnung und der Rechtsfolgen nicht akzeptiert werden.

Absatz 9:
Damit sind wohl PIN und privater Signaturschlüssel gemeint. Sollen sie auch entfernt in einem RZ zum Erstellen von Signaturen verwendet werden können (Beispiel: Handy-Signatur in Österreich)? Dann ist der Unterzeichner nach Absatz 5 keine natürliche Person mehr bzw. dieser kann sie nicht mit hoher Wahrscheinlichkeit unter seiner alleinigen Kontrolle halten.

Absatz 27:
Die Definition „elektronisches Dokument“ ist ohne Definition des Begriffs „Dokument“ nicht hilfreich. Hier sollte auch festgelegt werden, was ein Dokument von Daten unterscheidet – unabhängig davon, ob diese/s elektronisch sind/ist oder nicht. Ein elektronisches Dokument könnte als eine Datei mit elektronischen Daten definiert werden.

Absatz 30:
Nach Anhang IV darf ein „qualifiziertes Zertifikat für die Website-Authentifizierung“ nur für juristische Personen ausgestellt werden. Dies ist eine wesentliche, nicht nachvollziehbare Einschränkung.

Kapitel II: Elektronische Identifizierung

Artikel 5:

Hier muss dann jedes andere Identifizierungsmittel eines anderen EU-Staates akzeptiert werden, auch wenn es datenschutzrechtliche Anforderungen nach Datenvermeidung und -sparsamkeit nicht erfüllt. Das senkt ggf. die Qualität der deutschen Verfahren und ihre sichere Nutzbarkeit.

Artikel 6, Absatz 1c):

- Hier muss – über die Anmerkung zu Artikel 3 Absatz 1 hinaus – auf jeden Fall für datenschutzgerechte, pseudonyme Verfahren gesorgt werden, bei denen die Person nicht direkt erkennbar ist. Als Beispiel sei hier die pseudonyme Nutzung der eID-Funktion für Diensteanbieter genannt, die dienste- und kartenspezifische Kennzeichen nutzt. Diese sind immer dann zu nutzen, wenn die Offenlegung der Identifikationsdaten nicht erforderlich ist.
- Auch sollten sich die akzeptierenden Instanzen umgekehrt gegenüber den Bürgern identifizieren bzw. authentifizieren, so dass eine wechselseitige Sicherheit bezüglich des Kommunikationspartners gegeben ist.

Artikel 6, Absatz 1d), Artikel 7, Absatz 1d), e) und diverse andere Stellen:

Hier ist zu prüfen, ob es statt „Authentifizierungsmöglichkeit“ „**Identifi**zierungsverfahren“, „**Identifi**kation“ oder „**Identifi**zierung“ heißen muss. Die Identifikation bzw. Identifizierung wird bei der Registrierung durchgeführt, eine Authentifizierung dann jeweils in Fachverfahren, die auf der Identifizierung aufbauen (vgl. E-Government-Handbuch des BSI). Die eID des nPA bietet lediglich ein reines Identifizierungsverfahren an. Internet-Dienstanbieter können dieses nutzen, um darauf ein eigenes Authentisierungsverfahren für ihre eigene Anwendung aufzubauen, bei der Sie dem Bürger bestimmte Rechte oder bestimmte Datensätze zuordnen.

Artikel 6, Absatz 1d):

Dass dieses Verfahren jederzeit kostenlos online zur Verfügung steht, nach Satz 2 ohne „bestimmte technische Vorgaben“, also ohne zusätzliche Anforderungen an Hard- oder Software, bedeutet, dass die **eID des nPA diese Anforderungen nicht erfüllt**. Denn hier ist ein kostenpflichtiges Zertifikat – also zusätzliche Hard-/Software – des BVA für den Diensteanbieter erforderlich, das auch die benötigten personenbezogenen Daten für den Anbieter und seine Anwendung jeweils konkret festlegt.

Bedeutet diese Regelung, dass der Bürger die Kosten für die Identifizierung tragen muss? Das werden die Bürger kaum akzeptieren. Wer sonst kommt für die Kosten auf? Gibt es einen Topf für Infrastrukturkosten?

Artikel 8, Absatz 1:
Was bedeutet dieser Absatz vor dem Hintergrund der Durchführungsrechtsakte und der delegierten Rechtsakte?

Kapitel III: Vertrauensdienste

Artikel 11, Absatz 2 (Datenschutz):
Die Beschränkung der Verarbeitung personenbezogener Daten auf das Mindestmaß sollte nicht nur für die Vertrauensdiensteanbieter sondern auch für die akzeptierenden Instanzen und die Datenübermittlung an sie gelten.

Artikel 14, Absatz 2:
Diese Regelung kann gegen einzelstaatliche Interessen oder Regelungen verstoßen.

Artikel 15, Absatz 4 bis 6:
Diese Absätze können zu Widersprüchen zwischen den Regelungen der Aufsichtsstelle und denen der Kommission führen. Wie werden diese aufgelöst?

Artikel 17, Absatz 4:
Welcher Aufwand muss für das Verwaltungsverfahren oder von der betroffenen öffentlichen Stelle betrieben werden, um nachzuprüfen, dass der Vertrauensdienst wirklich qualifiziert ist? Hier wird vermeidbarer Aufwand betrieben.

Artikel 19, Absatz 3:
Wann ist ein Widerruf wirksam? Welche Regelungen gibt es hier?

Artikel 19, Absatz 4:
Auch das Vorhandensein oder Nichtvorhandensein eines Zertifikates in der Datenbank muss als Status mitgeteilt werden.

Artikel 25 Absatz 1:
Es ist sachgerecht und deshalb unbedingt zu begrüßen, dass qualifizierte elektronische Signaturen jetzt auf den Zeitpunkt der Erstellung geprüft werden.

Dies ist allerdings auch für fortgeschrittene Signaturen zu fordern:

- Die Zertifikatssignaturen der Vertrauensdienstanbieter sollen nur fortgeschritten sein. In diesem Fall entstehen die bekannten Probleme mit der Gültigkeit der Prüfkette, wenn FES wie bisher auf Gültigkeit zum Zeitpunkt der Prüfung geprüft werden.
- Auch für fortgeschrittene Anwendersignaturen ist die Prüfung auf den Zeitpunkt der Erstellung sachgerecht.
- So käme man endlich zu einem einheitlichen und sachgerechten Prüfverfahren für alle (qualifizierten und fortgeschrittenen) elektronischen Signaturen.

Auch Siegel sind auf den Zeitpunkt der Erstellung zu prüfen.

Artikel 25 Absatz 1, Ziffer c), d), e) und i):

Diese Bedingungen sind zum Zeitpunkt der Unterzeichnung (noch) nicht erfüllbar.

Artikel 27:
Statt „Bewahrung“ sollte „Preservation“ als „Erhaltung des Beweiswertes“ qualifizierter elektronischer Signaturen übersetzt werden.

Artikel 27 Absatz 1:
Statt „Bewahrungdienste für qualifizierte Signaturen“ sollte es „Dienste zur Erhaltung des Beweiswertes qualifizierter Signaturen“ heißen.

Falsch, weil inhaltlich weder zutreffend noch ausreichend, ist es die „Vertrauenswürdigkeit der qualifizierten elektronischen *Signaturvalidierungsdaten* über den Zeitraum ... zu verlängern“. Hier muss es „Signaturen“ statt „Signaturvalidierungsdaten“ heißen. Hier ist bisher eine Übersignatur mit einem aktuellen qualifizierten Zeitstempel bzw. einer aktuellen qualifizierten Signatur üblich. Die Vertrauenswürdigkeit der bisherigen Signaturvalidierungsdaten wird damit nicht beeinflusst; sie läuft mit dem Zertifikat ab und kann nicht verlängert werden. Auch die Formulierungen zu Artikel 27 in Absatz 3.3.3.3 und in Erwägung 49 sind entsprechend anzupassen.

Artikel 28 Absatz 6 und 7:
Wofür sollen über das qualifizierte Siegel hinaus weitere unterschiedliche Sicherheitsniveaus für Siegel festgelegt werden?

Das führt wie bei der elektronischen Signatur dazu, dass dann kein Niveau wirklich genutzt wird und sich durchsetzt.

Artikel 30, Absatz 1:
Warum werden die Anforderungen an qualifizierte Siegelerstellungseinheiten nicht analog Artikel 29 Absatz 1 in einem eigenen Anhang formuliert? (Oder umgekehrt dort auf einen eigenen Anhang verzichtet.) Eine einheitliche Vorgehensweise ist für die Verständlichkeit und Übersichtlichkeit wünschenswert.

Artikel 33 Absatz 1, a) und b):
Welche Daten sind in a) gemeint? Die Daten des Dokuments oder die Daten des Zeitstempels oder die Uhrzeit des Zeitstempels?

Ergibt sich über a) „koordinierte Weltzeit (UTC)“ nicht, dass der Zeitstempel in b) „auf einer korrekten Zeitquelle beruht“?

Artikel 33 Absatz 1d):
- Dieses Verfahren ist technisch und rechtlich nicht brauchbar.
- Wenn hier mit fortgeschrittenen Signaturen bzw. fortgeschrittenen Siegeln der qualifizierten Vertrauensdiensteanbieter gearbeitet wird, entspricht der Beweiswert von vornherein nicht den mit dem Begriff verknüpften Erwartungen. Auch zur Erhaltung des Beweiswertes (Übersignatur) ist dieses Verfahren nicht geeignet, weil zu schwach.
- Dieses Verfahren erweckt einen unzutreffenden Eindruck: es wird qualifizierter Zeitstempel genannt – aber es ist nur eine fortgeschrittene Signatur bzw. Siegel vorhanden.
- Konsequenz für Deutschland: Alle Verfahren die den Beweiswert sichern sollen, wie ArchiSig, ArchiSafe u.a., arbeiten solide mit qualifizierten Zeitstempeln (nach SigG). Sie sind dann von den qualifizierten Zeitstempeln (nach EU eIAS VO) sprachlich und inhaltlich nicht mehr wirklich zu unterscheiden und erfüllen daher ihren Zweck nicht mehr.
- Im Gegenteil: wegen der EU VO müssen dann die „qualifizierten“ Zeitstempel nach EU eIAS VO in Deutschland akzeptiert werden – sicher auch bei Ausschreibungen – so dass ArchiSig, ArchiSafe etc. auch in Deutschland nicht mehr funktionieren.
- Was ist mit „einem gleichwertigen Verfahren“ gemeint? Wozu wird das eingeführt? Ein solches Verfahren ist überflüssig und führt nicht zur erforderlichen Rechtssicherheit.
- Lösung: Diese Definition ist ein fortgeschrittener Zeitstempel.

Qualifiziert ist er nur, wenn alle Zertifikate, Dokumente (und ggf. Hash-Bäume) in der Hierarchie qualifiziert signiert bzw. gesiegelt sind.

Artikel 34 Absatz 3 und 4:

- Absatz 3 kann zu Konflikten mit geltendem Recht im Inland führen.
- Warum werden die Formate in Absatz 4 nicht direkt – zumindest in einem Anhang formuliert?

Artikel 37 Absatz 2:

Für diesen Bereich sind besonders schnelle Sperrungen und Warndienste bei Kompromittierung bzw. Missbrauch erforderlich.

Anhang I, j):

Qualifizierte Zertifikate können jetzt ersichtlich auch für andere als qualifizierte Signaturen verwendet werden. Nämlich dann, wenn keine qualifizierte Signaturerstellungseinheit verwendet wird. Das ist absolut irreführend und nicht hilfreich.

Das Feld im Zertifikat, das die Verwendung – eigentlich nur die Existenz – einer qualifizierten Signaturerstellungseinheit bestätigt, gibt es bisher nicht. Weder in den Normen noch in der Praxis. Das wird zu Verwirrungen mit dem bisherigen qualifizierten Zertifikat nach SigG und EU-Signaturrichtlinie 1999/93/EG führen.

Anhang II, Absatz 1c):

Hier ist statt „verfügbarer“ Technik „nach dem Stand der Technik“ zu fordern.

Anhang III, j):

Analog zur Bemerkung unter Anhang I, j).

Anhang IV:

Warum wird die Website- Authentifizierung nur für juristische Personen realisiert?

Das geht an der Realität des Internet vorbei bzw. lässt alle Websites von natürlichen Personen ohne nachvollziehbaren Grund ohne die erforderliche Sicherheit.

Übersetzungsfehler

Artikel 3:
Absatz 7c): hier geht es nicht um „ein hohes Maß an Vertrauen“, sondern im Gegenteil um ein „hohes Maß an Vertrauens**würdigkeit**“. Alternativ lässt sich „high level of confidence“ auch als „mit hoher Wahrscheinlichkeit“ übersetzen.

Artikel 6, Absatz 1d) und diverse andere Stellen:
„relying party“ sollte mit „akzeptierende Dritte“ oder „akzeptierende Instanzen“ übersetzt werden. Es geht hier darum, sich auf etwas zu berufen, zu verlassen oder zu stützen oder darum, auf etwas zu bauen oder zu beruhen. Nicht um Vertrauen an sich, sondern darum, eine Basis für Vertrauenswürdigkeit zu schaffen.

Artikel 14, Absatz 3:
Hier muss es mehrfach statt „unterstützte Aufsichtsstelle“ „unterstütz**end**e Aufsichtsstelle“ heißen

Artikel 15, Absatz 1:
Im dritten Satz muss übersetzt werden: „..., um Sicherheitsverletzungen zu vermeiden bzw. ihre Auswirkungen so gering wie möglich zu halten ...“

Artikel 15, Absatz 2, Satz 1:
Statt „unverzüglich“ muss wörtlich übersetzt werden „ohne schuldhafte Verzögerung“ und nach Aufsichtsstelle unbedingt ein Komma gesetzt werden. Eine eindeutige und unmissverständliche Übersetzung ist erstrebenswert.

Artikel 18:
„sealed trusted lists“ muss stets mit „**g**esiegelte Vertrauensliste“ statt mit „besiegelte Vertrauensliste“ übersetzt werden.

Artikel 18, Absatz 4:
Statt „auf sichere Weise“ muss es „auf einem sicheren Kanal“ oder „auf einem sicheren Weg“ heißen.

Diverse Stellen:

„Bewahrung“ von Signaturen, Zertifikaten etc.

Hier geht es stets um die Erhaltung des Beweiswertes elektronischer Signaturen.